Nicolae Sfetcu

Épistémologie des services de renseignement

Collection ESSAIS

MultiMedia Publishing

Épistémologie des services de renseignement

Nicolae Sfetcu

15.04.2020

Sfetcu, Nicolae, « Épistémologie des services de renseignement », SetThings (15 avril 2020), MultiMedia Publishing (ISBN : 978-606-033-363-0), DOI: 10.13140/RG.2.2.35970.22729 URL = https://www.telework.ro/fr/e-books/epistemologie-des-services-de-renseignement/

Email: nicolae@sfetcu.com

Une traduction de :
Sfetcu, Nicolae, « Epistemologia serviciilor de informații », SetThings (4 februarie 2019), MultiMedia Publishing (ed.), DOI: 10.13140/RG.2.2.19751.39849, ISBN 978-606-033-160-5, URL = https://www.telework.ro/ro/e-books/epistemologia-serviciilor-de-informatii/

Sommaire

Abstract

Dans cet article, je souligne l'analogie entre les aspects épistémologiques et méthodologiques de l'activité des services de renseignement et certaines disciplines scientifiques, en préconisant une approche plus scientifique du processus de collecte et d'analyse de l'information au sein du cycle du renseignement. J'affirme que les aspects théoriques, ontologiques et épistémologiques de l'activité de nombreux services de renseignement sont sous-estimés, ce qui conduit à une compréhension incomplète des phénomènes actuels et à une confusion dans la collaboration interinstitutionnelle. Après une brève Introduction, qui inclut un historique de l'évolution du concept de service de renseignement après la Seconde Guerre mondiale, Renseignement définit les objectifs et l'organisation des services de renseignement, le modèle de base de ces organisations (le cycle du renseignement) et les aspects pertinents de la collection de l'information et l'analyse du renseignement. Dans la section Ontologie, je souligne les aspects ontologiques et les entités qui menacent et qui sont menacés. La section Épistémologie comprend des aspects spécifiques à l'activité de renseignement, avec l'analyse du modèle traditionnel (Singer) utilisé traditionnellement, et j'expose une approche épistémologique possible à travers le concept de connaissance tacite développé par le scientifique Michael Polanyi. La section Méthodologie contient diverses théories méthodologiques mettant l'accent sur les techniques analytiques structurelles ainsi que certaines analogies avec la science, l'archéologie, les affaires et la médecine. L'article se termine par les Conclusions sur la possibilité d'une approche plus scientifique des méthodes de collecte d'information et d'analyse des services de renseignement.

Mots-clés : services de renseignement, renseignement, ontologie, épistémologie, méthodologie.

1. Introduction

L'information c'est le pouvoir. Cette perception s'est intensifiée au cours de la Seconde Guerre mondiale, lorsque les services de renseignement a été officialisés et leur nombre a été considérablement accru. Dans tous les pays, de nouvelles services et départements ont été créés pour faire face aux menaces. Les gouvernements dépensent actuellement des sommes énormes pour les services de renseignement considérées comme une composante majeure des systèmes de sécurité nationale. Les services de renseignement sont principalement responsables de l'identification et de la prévention des menaces à la sécurité nationale, d'informer rapidement et efficacement les décideurs de ces menaces, ainsi que d'évaluations et de prévisions précises et en temps utile des futurs conflits ou menaces.

Le renseignement comprend une grande variété de significations dans différents contextes, du quotidien au technique. Stewart estime que la transformation du renseignement en connaissance est une étape essentielle, qui constitue le fondement de la création de valeur et d'un avantage concurrentiel pour les entreprises modernes. (Stewart 2001)

Le processus d'obtention, de traitement et d'analyse du renseignement est une préoccupation majeure de la société actuelle, avec l'aide des domaines tels que la technologie de l'information, les systèmes d'information et la science de l'information. À cette fin, des processus et techniques spécifiques sont utilisés pour collecter ou générer des informations, les traiter par analyse et synthèse, générer des prévisions et des stratégies, transmettre et présenter des renseignements aux décideurs, et les stocker. Dans ce contexte, certains concepts majeurs fonctionnent dans ce domaine :

- *Visualisation des renseignements* (InfoVis) dépend du mode de calcul et de représentation des données numériques. Il aide également les utilisateurs à reconnaître les formes et à détecter les anomalies.

- *Sécurité des renseignements* (InfoSec) est le processus en cours de vérification du renseignement et des systèmes d'information contre tout accès, utilisation, divulgation, destruction, modification, dysfonctionnement ou distribution non autorisée.
- *Analyse des renseignements* est le processus d'inspection, de transformation, de modélisation, de synthèse des renseignements et de prévision, de transformation de données brutes en connaissances exploitables à l'appui de la prise de décision.
- *Qualité des renseignements* (InfoQ) est le potentiel d'un ensemble de données et de renseignements pour atteindre un objectif (scientifique ou pratique) en utilisant une méthode d'analyse empirique particulière.

La science de l'information est engagée dans l'analyse, la collecte, la classification, la manipulation, le stockage, la récupération et la diffusion de l'information. (Sfetcu 2016) Il est souvent considéré (à tort) comme une branche de l'informatique. La science de l'information aborde les problèmes systémiques du point de vue des personnes concernées et peut être considérée comme une réponse au déterminisme technologique. La philosophie de l'information étudie les aspects conceptuels spécifiques, y compris l'étude de la nature conceptuelle et les principes de base de l'information, leur dynamique, leur utilisation, ainsi que l'élaboration et l'application d'informations théoriques et de méthodologies spécifiques. (Floridi 2002) Dans les sciences de l'information, une ontologie représente formellement la connaissance comme un ensemble de concepts et la relation entre ces concepts. L'ontologie peut être utilisée pour raisonner sur ces entités et pour décrire le domaine.

La collecte de renseignements est la science de la recherche des documents, des informations sur les documents et des métadonnées des documents, ainsi que de la recherche dans des bases de données relationnelles et sur Internet. Chaque type de recherche a ses propres

caractéristiques, théories, pratiques et technologies. L'accès à l'information est un domaine de recherche visant à automatiser le traitement des grandes quantités d'informations et à en simplifier l'accès par les utilisateurs. L'architecture de l'information met l'accent sur les principes de conception et d'architecture dans le paysage numérique, sur la base d'un modèle ou d'un concept d'information utilisé dans les activités d'analyse du renseignement. La gestion du renseignement implique la collecte et la gestion d'informations provenant d'une ou de plusieurs sources et la distribution de ces informations à un ou plusieurs segments. La représentation des connaissances est un domaine de recherche qui vise à représenter les connaissances sous forme de symboles afin de faciliter les interférences entre ces éléments de connaissance et la création de nouveaux éléments de connaissance. Explorer la représentation de la connaissance implique une analyse du raisonnement. La logique sert à fournir une sémantique formelle sur la manière dont les fonctions de raisonnement devraient être appliquées aux symboles dans le système de représentation des connaissances et à définir la manière dont les opérateurs peuvent traiter et remodeler les connaissances.

Les systèmes d'information sont organisés pour collecter, organiser, stocker et communiquer des informations. Le domaine des systèmes d'information est complémentaire à celui de la collecte, du filtrage, du traitement, de la création et de la distribution des données. (Sfetcu 2016) Tout système d'information spécifique est destiné à soutenir les opérations, la gestion et la prise de décision. Les systèmes d'information interagissent avec les systèmes de données et les systèmes d'activité de l'autre, en tant que système de communication dans lequel les données sont représentées et traitées comme une forme de mémoire sociale. Un système d'information peut également être considéré comme un langage semi-formel qui soutient la prise de décision et l'action humaine. Silver et al ont fourni deux perspectives pour les systèmes

d'information, qui incluent les logiciels, le matériel, les données, les personnes et les procédures. (Silver, Markus, et Beath 1995) Zheng a proposé une autre approche du système d'information, (Zheng 2014) qui ajoute également des processus et des éléments essentiels de système, tels que l'environnement, la limite, le but et les interactions.

Histoire du renseignement

La collecte, l'analyse et l'utilisation d'informations relatives aux adversaires existent depuis l'Antiquité. Sun Tzu, un ancien stratège chinois, dans l'*Art de la guerre*, (Yuen 2014) a insisté sur la nécessité de se comprendre et de comprendre l'ennemi au moyen d'informations, en identifiant différents rôles: l'informateur secret ou l'agent, l'agent de pénétration et l'agent de désinformation. Sun Tzu a souligné le besoin d'une méthodologie et a souligné le rôle de la contre-information, des agents doubles et de la guerre psychologique. Au 4ème siècle avant JC, Chanakya (également appelé Kautilya), en Inde, a écrit *Arthashastra*, un « manuel de gestion de l'État et d'économie politique », qui fournissait une méthodologie détaillée des opérations de collecte, de traitement, de consommation et de l'information comme moyen indispensable pour maintenir et développer la sécurité et le pouvoir de l'État. (Shoham et Liebig 2016) Au début du XIIe siècle, le roi David IV de Géorgie a utilisé des espions pour découvrir les conspiration féodale et les infiltration dans des endroits clés. (Aladashvili 2017) Les Aztèques ont utilisé des commerçants et des diplomates avec immunité diplomatique pour espionnage. (Soustelle 2002, 209)

Francis Walsingham a été le premier Européen à utiliser des méthodes d'espionnage modernes dans l'Angleterre élisabéthaine, en collaborant avec des experts de divers domaines. (Andrew 2018, 242-91) Au dix-huitième siècle, les activités d'espionnage se sont considérablement développées. (Andrew 2018, 242-91) En France, sous le roi Louis XIV (1643-1715) et sous la direction du cardinal Mazarin (1642-1661), un système d'information bien

organisé a été mis en place. Pour faire face aux guerres avec la France, Londres a également mis en place un système destiné à recueillir des informations sur la France et d'autres puissances. Pendant la Révolution américaine de 1775 à 1783, le général américain George Washington a développé avec succès un système d'espionnage destiné à détecter les lieux et les plans britanniques, étant appelé « le premier espion de l'Amérique ». (Nagy 2016, 274)

Pendant la guerre civile américaine (1861-1865), Allan Pinkerton a dirigé pour la première fois une agence de détectives, et il a ensuite servi en tant que chef du Service de renseignement de l'Union dans les premières années. L'Empire autrichien a fondé Evidenzbureau en 1850 en tant que premier service de renseignement militaire permanent. Le département topographique et statistique T&SD a été créé au British War Office en tant qu'organisation embryonnaire de renseignement militaire. Le ministère français de la Guerre a autorisé la création, en 8 juin 1871, du Deuxième Bureau, un service chargé de « mener des recherches sur les plans et les opérations de l'ennemi ». En Allemagne, le maréchal Helmuth von Moltke a mis en place une unité de renseignement militaire, Abteilung (Section IIIb), de l'État-major allemand, en 1889, qui a constamment élargi ses opérations en France et en Russie. L'office d'information du commandement suprême d'Italie a été créé de manière permanente en 1900. Après la défaite de la Russie lors de la guerre russo-japonaise de 1904-1905, le service militaire russe a été réorganisé sous la septième division du deuxième comité exécutif impériale.

Au Royaume-Uni, Secret Service Bureau, créé en 1909 en tant que premier organisme indépendant et interdépartemental ayant le plein contrôle de toutes les activités d'espionnage du gouvernement, a été divisé en 1910 entre un service externe et un service de contre-espionnage. Lors de la guerre mondiale de 1914, toutes les grandes puissances disposaient de structures très sophistiquées pour la formation et la manipulation d'espions, ainsi que pour le traitement des

informations obtenues par espionnage. A cette époque, les techniques modernes d'espionnage étaient recherchées et perfectionnées pour obtenir des renseignements militaires, commettre des actes de sabotage et propagande. Pendant la guerre, deux nouvelles méthodes de collecte de renseignements ont été mises au point : la reconnaissance aérienne, le tournage, et l'interception et le décryptage des signaux radio. (Wheeler 2012)

Au cours de la Seconde Guerre mondiale, à l'ordre de Churchill a été conçu un plan pour former des espions et des saboteurs sous le commandement du SOE (Special Operations Executive) et, à terme, pour impliquer les États-Unis dans leurs facilités de formation. La branche « Recherche et analyse » de l'OSS a réuni de nombreux universitaires et experts qui se sont révélés particulièrement utiles pour donner un aperçu très détaillé des forces et des faiblesses de l'effort de guerre allemand.

MI5 britannique et FBI américain ont identifié tous les espions allemands et les a « transformés » en agents doubles. Leurs rapports à Berlin ont donc été réécrits par des équipes de contre-espionnage. Le FBI a joué un rôle de premier plan dans le contre-espionnage américain et a réuni tous les espions allemands en juin 1941. (Persico 2002) Le contre-espionnage a inclus l'utilisation des agents pour désinformer l'Allemagne nazie des points d'impact lors du blitz et l'isolement des Japonais aux États-Unis contre le programme d'espionnage japonais pendant la guerre.

Pendant la guerre froide, l'Union soviétique a particulièrement bien réussi à introduire des espions au Royaume-Uni et en Allemagne de l'Ouest, mais a échoué aux États-Unis. L'OTAN, d'autre part, a également connu d'importants succès.

L'accent mis sur les intentions et les capacités de l'Union soviétique a dominé la pensée des communautés du renseignement occidentales. En analysant les informations des années 1950,

Walter Laqueur affirme que « les capacités et les intentions militaires soviétiques demeurent le sujet le plus important pour les services secrets américains ». (Laqueur 1993)

Après la guerre froide, les gouvernements et les services de renseignement ont continué à utiliser le modèle conventionnel pour évaluer les menaces pesant sur l'État. Mais les concepts de sécurité se sont éloignés d'une confrontation hautement militarisée entre des adversaires connus et a augmenté l'inquiétude suscitée par les menaces non étatiques plus difficiles à identifier. Les acteurs non étatiques sont devenus des menaces stratégiques, le concept de « terrorisme stratégique » étant développé immédiatement après les attentats de septembre 2001. Bruce Berkowitz affirme qu'il y a eu des actes terroristes dans le passé, mais Ben Laden a été le premier à utiliser le terrorisme stratégique généralisé contre une super-pouvoir. (B. Berkowitz 2002) La mondialisation et la mobilité des personnes et des technologies ont favorisé les acteurs non étatiques. (Waltz 2003) Le directeur de CIA, James Woolsey, a déclaré au Comité de la sécurité nationale de la Chambre des représentants aux États-Unis que « ... c'est comme si nous avions combattu un grand dragon pendant 45 ans, que nous l'avons tué, et nous sommes entrés ensuite dans une jungle pleine de serpents venimeux - et les serpents sont beaucoup plus difficile à surveiller que le dragon n'a jamais été. » (Woolsey 1998) En 2007, Jonathan Evans, le responsable de la sécurité du Royaume-Uni (MI5), a décrit la menace terroriste comme « la menace la plus immédiate et la plus grave pour la paix dans l'histoire de mes 98 années de service ». (Evans 2007)

Les publications gouvernementales dans les pays développés, à la suite de l'attaque du 11 septembre 2001, ont témoigné d'un consensus sur le fait que les services de renseignement étaient essentiels pour prévenir les attaques massives.

Actuellement, aux États-Unis, dix-sept agences fédérales (Intelligence.gov 2013) forment la Communauté du renseignement (IC) des États-Unis. L'Agence centrale de renseignement (CIA)

utilise la Direction des Opérations (NCS) (CIA.gov 2009b) pour collecter des informations et mener des opérations d'infiltration. (CIA.gov 2009a) L'Agence nationale de la sécurité (NSA) recueille des informations à partir des signaux. Initialement, CIA dirigeait la Communauté du renseignement. À la suite des attaques du 11 septembre, le Bureau du Directeur du renseignement national (DNI) a été créé pour promouvoir l'échange d'informations.

2. Renseignement

Michael Goodman estime que "bien que la collecte et l'analyse d'informations ne soient pas un phénomène nouveau, ses études universitaires constituent" un domaine émergent. (Goodman 2007) On considère généralement que le cycle d'information se compose de cinq étapes : planification et direction ; collection ; traitement ; analyse ; et diffusion. (Diane Publishing Company 2000) Le point le plus important du cycle du renseignement est considéré celui de l'analyse. Mike McConnell déclare que "les services de renseignement peuvent aider à informer et à orienter les décisions uniquement si les informations sont traitées par l'esprit d'un analyste". (McConnell 2007)

Ainsi, la Stratégie Nationale de Renseignement des États-Unis souligne la nécessité de "renforcer l'expertise analytique, les méthodes et les pratiques, d'utiliser l'expertise où qu'elle se trouve et d'explorer d'autres points de vue analytiques". (Office of the Director of National Intelligence 2005) Arthur Hulnick écrit que "la communauté du renseignement doit développer une culture analytique du XXIe siècle, différente de l'analyse intuitive conventionnelle du passé". (Hulnick 2006) Noter les efforts de Rob Johnston pour développer une taxonomie de l'analyse du renseignement, affirmant que "les services de renseignement ont besoin de méthodologies pour renforcer le champ de l'analyse". (Johnston 2003)

David Singer indique que la menace est actuellement le principal objectif des services de renseignement. Ken Robertson a également défendu cette idée dans ses efforts pour définir le renseignement :

"Une définition satisfaisante du renseignement devrait faire référence aux éléments suivants : menaces, états, secrets, collecte, analyse et objectif. Le plus important d'entre eux est la menace, car sans menaces, aucun service de renseignement ne serait pas nécessaire" (K. Robertson 1996)

Carl Von Clausewitz, dans *À propos de la guerre* (1832), a défini le renseignement comme "toutes sortes d'informations sur l'ennemi et le pays - la base, en bref, de nos propres plans et opérations." (Clausewitz 1989) Une étude de la culture analytique a établi, par consensus, les définitions suivantes:

- Le *renseignement* est une activité secrète de l'État ou du groupe visant à comprendre ou à influencer des entités étrangères ou nationales.
- L'*analyse du renseignement* consiste à appliquer des méthodes cognitives individuelles et collectives pour peser les données et tester les hypothèses dans un contexte socioculturel secret.
- Les *erreurs de renseignement* sont des inexactitudes factuelles dans l'analyse résultant de données insuffisantes ou manquantes. L'*échec de renseignement* est une prédiction échouant résultant d'hypothèses incorrectes, manquantes, rejetées ou inadéquates.

Stephen Marrin examine deux raisons pour l'échec de l'élaboration de la théorie des services de renseignement : (Marrin 2012b) le fait qu'aucun consensus n'ait encore été atteint concernant les définitions qui sont les précurseurs de la formulation de la théorie et 2) parce que le renseignement est un domaine appliqué, les praticiens étant en principe contre la théorisation.

Le renseignement peut être considérée comme le processus par lequel certains types d'informations sont demandés, collectés, analysés et diffusés, ainsi que la manière dont certains

types d'actions secrètes sont conçues et réalisées. (Shulsky et Schmitt 2002) Berkowitz assimile la communauté du renseignement à celle d'une "bureaucratie classique" de Weber caractérisée par une planification centralisée, des opérations de routine et une chaîne hiérarchique se manifestant dans le cycle traditionnel du renseignement, semblable à une chaîne de montage. (B. D. Berkowitz et Goodman 2000)

> "Le renseignement est plus que de l'information. C'est une connaissance qui a été préparée spécialement pour les circonstances uniques du client. Le mot connaissance souligne la nécessité d'une implication humaine. Les systèmes de collecte du renseignement produisent ... des données, pas de renseignement ; seul l'esprit humain peut offrir ce petit quelque chose qui donne un sens aux données pour les différentes exigences du client. Le traitement spécial qui définit en partie le renseignement est la collecte, la vérification et l'analyse continues des informations qui nous permettent de comprendre le problème ou la situation en agissant puis en adaptant un produit aux circonstances du client. S'il manque l'un de ces attributs essentiels, le produit reste alors des informations brutes plutôt que des informations traitées [renseignement]." (Brei 1996)

Dans l'analyse du renseignement, les spécialistes distinguent trois types de produits de renseignement :

1. *Renseignement opérationnel*, qui assistent et dirigent la collecte ou l'enquête de manière continue et où l'analyste fait généralement partie de l'équipe d'enquête, complétées par des mémorandums, des plans opérationnels et des rapports de situation, ainsi que des supports visuels pour l'analyse, tels que des graphiques, infogrammes, images visuelles, etc.
2. *Renseignement courant*, qui contextualisent les "instantanés" d'un événement ou d'un problème pour le client, sous forme de texte.
3. *Renseignement stratégique*, qui fournissent au client des estimations et/ou des avertissements en présentant des analyses à moyen et long terme sur la nature, la dynamique et l'impact d'un événement ou d'un problème.

2.1. Organisations

Les services secrets sont des agences gouvernementales chargées de la collecte et de l'analyse du renseignement sensible afin de garantir la sécurité et la défense nationales. Les méthodes d'obtenir le renseignement peuvent inclure l'espionnage, l'interception de communications, l'analyse cryptographique, la coopération avec d'autres institutions et l'évaluation des sources publiques. (Sfetcu 2016)

Les services secrets se concentrent actuellement sur la lutte contre le terrorisme, ne laissant que relativement peu de ressources pour surveiller les autres menaces à la sécurité. Pour cette raison, ils ignorent souvent les activités de renseignement externes qui ne représentent pas une menace immédiate pour les intérêts de leur gouvernement. (Ehrman 2011)

Très peu de services externes - CIA, SVR et, dans une moindre mesure, SIS, DGSE de France et Mossad - opèrent dans le monde entier. Presque tous les autres services se concentrent sur les voisins ou les régions immédiates. Ces services dépendent généralement des relations établies avec ces services d'information mondiaux pour des zones situées au-delà de leur voisinage immédiat et commercialisent souvent leur expertise régionale pour répondre à leurs besoins mondiaux.

Les services de renseignement sont des prisonniers de la bureaucratie gouvernementale, soumis aux mêmes forces et tendances politiques que les autres. Les situations politiques des services d'information dans des États autoritaires, totalitaires ou corrompus sont plus difficiles à déterminer. L'absence des cadres juridiques efficaces et l'importance des réseaux personnels en relation avec les relations institutionnelles pour la prise de décision rendent leur étude difficile. Des exemples tirés de l'histoire des services du bloc communiste suggèrent toutefois que la position de leurs services dans ces États peut être paradoxale. La dépendance de ces régimes sur leurs services de répression, l'intégration des services dans l'appareil gouvernemental et l'absence

de tout contrôle externe, offrent aux services une immunité contre les enquêtes externes et la pression des réformes. (Ehrman 2011)

Même lorsqu'ils agissent légalement, les services de renseignement protègent et défendent leurs intérêts. Le résultat est que les services sont presque toujours engagés dans des luttes politiques complexes sur plusieurs fronts. Le plus important de ceux-ci est l'effort constant de rassembler autant de ressources - personnes, fonds et influence sur le processus décisionnel - de leurs supérieurs politiques et de s'opposer aux changements imposés de l'extérieur.

Les services secrets ne sont pas des institutions robotiques, mais plutôt des centaines ou des milliers de personnes qui prennent et exécutent les décisions. Il existe peu d'études sociologiques ou comparatives à source ouverte sur les agents de renseignement. Les responsables des services externes appartiennent généralement à des classes socio-économiques supérieures. La nature de leur travail - vivre et opérer dans d'autres pays, se présenter comme des diplomates ou des hommes d'affaires et interagir avec les dirigeants politiques nationaux et étrangers - nécessite une formation universitaire, une connaissance des langues et de la culture et une confiance dans l'interaction avec les diplomates et les politiciens. Les personnes présentant ces caractéristiques viennent généralement de la classe moyenne supérieure ou supérieure. Les officiers des services internes appartiennent généralement à la classe ouvrière et à la petite bourgeoisie. Leur travail s'apparente au travail de policier et, comme ils s'acquittent de leurs tâches chez eux, le pouls de la rue est plus important que l'élégance sophistiquée. (Richelson 1988, 72) (Shelley 1990, 479-520)

Une caractéristique des services internes et externes est qu'ils se comportent comme une caste. À l'exception du chef, aucune personne nommée de l'extérieur n'a un poste d'autorité ; dans le monde du renseignement n'entrent pas les hommes politiques ambitieux, les avocats, les

analystes des groupes de réflexion et les universitaires, ils occupent généralement des postes gouvernementaux.

John Ehrman déclare que la gestion des services tend à être médiocre. (Ehrman 2011) En général, les agents des dossiers très performants assument des postes de direction. Habituellement, ils ne reçoivent aucune formation en gestion avant d'occuper ces postes, et après cela, ils bénéficient d'une formation systématique insuffisante. En conséquence, les cadres moyens et supérieurs ont souvent peu d'intérêt pour la supervision des détails essentiels de l'administration et de la planification ou pour la prise d'initiatives visant à modifier ou à moderniser les services avant qu'une défaillance ou une crise ne l'oblige à le faire.

L'objectif principal des services de renseignement est de fournir la sécurité, un concept qui évalue le degré de résistance ou de protection à ce qui est considéré comme mauvais. Certains concepts sont communs à plusieurs domaines de sécurité :

- *Assurance* - niveau de garantie qu'un système de sécurité se comportera comme il a été évalué
- *Contre-mesure* - le moyen d'empêcher une menace de déclencher un événement à risque
- *Défense en profondeur* - elle ne repose jamais sur une seule mesure
- *Risque* - un événement possible qui pourrait causer une perte
- *Menace* - une méthode pour déclencher un événement à risque qui est dangereux
- *Vulnérabilité* - une faiblesse d'une cible pouvant être exploitée par une menace pour la sécurité
- *Exploitation* - une vulnérabilité déclenchée par une menace - un risque de 1,0 (100%)

Robert M. Clark considère qu'une organisation est un système qui "peut être visualisé et analysé sous trois perspectives : structure, fonction et processus". (Clark 2003, 277) La *structure*

décrit les différentes parties de l'organisation, en mettant l'accent sur les personnes et leurs relations. La *fonction* décrit le produit de l'organisation en mettant l'accent sur la prise de décision. Et le *processus* décrit les activités et les connaissances qui définissent le produit final.

2.2. Cycle du renseignement

Le cycle du renseignement est un ensemble de processus utilisés pour fournir des informations utiles à la prise de décision. Le cycle comprend plusieurs processus. Le domaine connexe de la contre-information est chargé d'empêcher les efforts du renseignement de tiers.

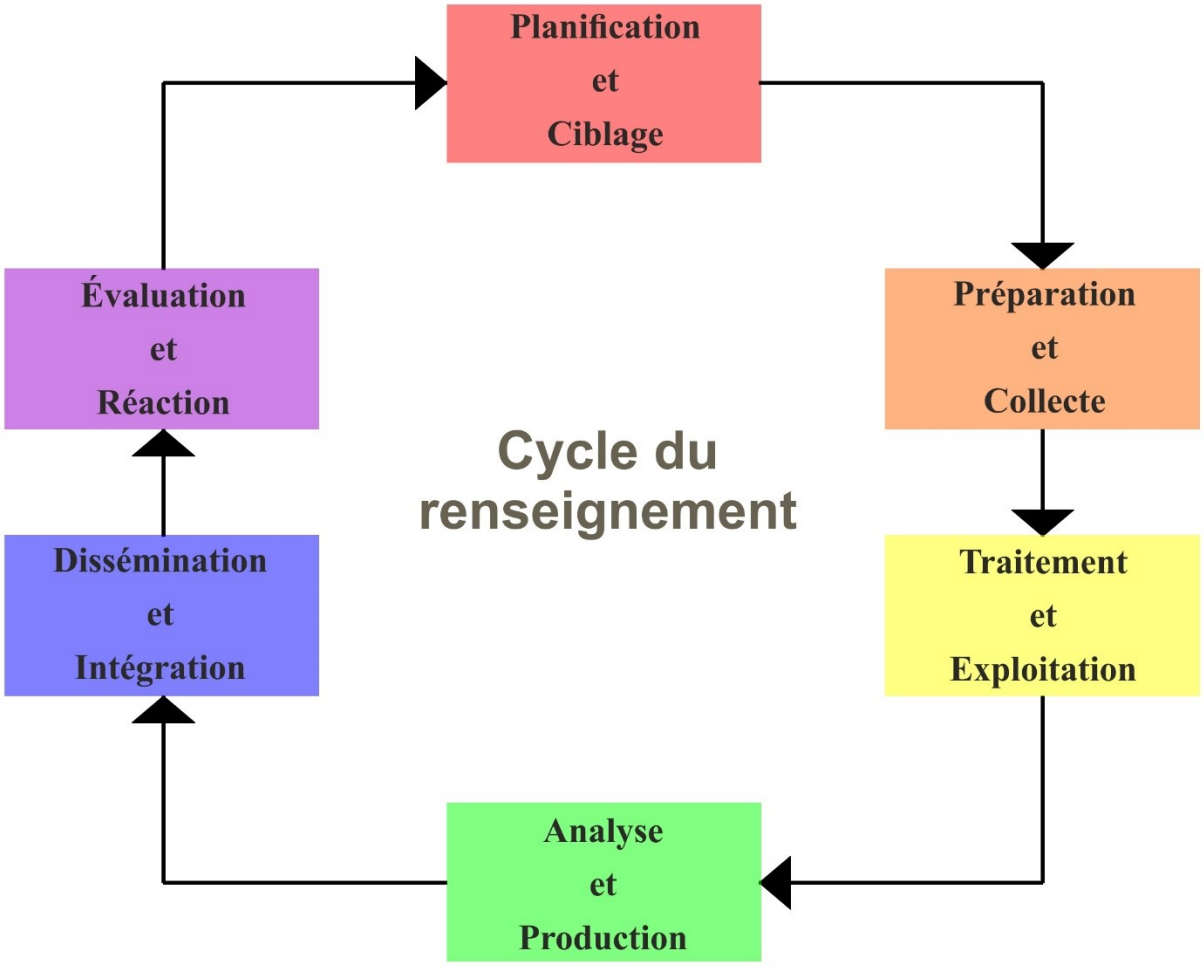

Fig. 1 Processus ou cycle du renseignement

Un modèle de base du processus de collecte et d'analyse du renseignement est appelé « cycle du renseignement ». Ce modèle peut être appliqué et, comme tous les modèles de base, ne reflète pas la plénitude des opérations dans le monde réel. Au cours des activités du cycle du renseignement, les informations sont collectées et assemblées, les informations brutes sont transformées en informations traitées, analysées et mises à la disposition des utilisateurs. Le cycle du renseignement comprend cinq phases :

1. *Planification et Ciblage* : Décide les éléments à surveiller et à analyser. Cela implique de déterminer les besoins en renseignement, de développer une architecture du renseignement appropriée, de préparer un plan de collecte, d'émettre des ordres et de soumettre des demandes aux agences de collecte d'informations.
2. *Préparation et Collecte* : Établir une stratégie pour les responsables du renseignement, obtenir des informations brutes à l'aide de divers types de collecte, tels que sources humaines (HUMINT), sources géospatiales (GEOINT), etc.
3. *Traitement et Exploitation* : Raffinage et utilisation principale du renseignement dans les décisions primaires.
4. *Analyse et Production* : Les données traitées sont traduites en un produit du renseignement finalisé, pouvant inclure des synthèses, des prévisions et des mesures de renseignement spécifiques.
5. *Dissémination et Intégration* : Fourniture de produits de renseignement aux consommateurs (y compris ceux de la communauté de l'information)

En plus de ces phases, une sixième étape est très importante, elle n'est pas réalisée exclusivement dans le service de renseignement, mais en collaboration avec les clients et en observant l'environnement opérationnel pour l'efficacité des informations fournies :

6. *Évaluation et Réaction*

Généralement, ces étapes sont subdivisées au sein d'un service de renseignement. Le nombre d'étapes varie en fonction de la stratégie de chaque service de renseignement ; certaines agences compressent certaines de ces étapes (par exemple, l'analyse et la production sont incluses dans la phase de traitement et d'exploitation) ou ajoutent d'autres étapes en fonction des besoins spécifiques.

La phase initiale de planification et de direction du cycle du renseignement comprend quatre grandes étapes :

1. Identifier et hiérarchiser les *besoins* en renseignement ;
2. Développer une *architecture* de renseignement adéquate ;
3. Préparation d'un *plan de collecte* ; et
4. Emission *d'ordres et de demandes* aux agences de collecte d'informations.

La gestion des besoins en renseignements de la coordination de la collecte (collection coordination intelligence requirements management - CCIRM) est la doctrine de l'OTAN en matière de gestion de la collecte du renseignement, bien qu'elle diffère de la doctrine américaine.

Au stade « analyse et production », les informations sont considérées comme traitées uniquement après avoir été vérifiées auprès de toutes les sources disponibles, leur véracité augmentant en fonction du nombre et de la qualité des contrôles supplémentaires.

L'activité de renseignement étant un processus itératif, en interaction avec de nombreux acteurs, le processus du renseignement peut être qualifié de dialectique, du fait qu'une hypothèse donnée peut être confirmée, révisée ou rejetée sur la base des informations supplémentaires obtenues à partir d'autres disciplines.

Une condition importante pour l'efficacité du renseignement en tant que produit fini est la rapidité et la précision des communications entre les acteurs impliqués.

D'un point de vue épistémologique, il n'est pas encore clair de savoir quand les informations deviennent des connaissances traitées : après la collecte, après une nouvelle vérification par les analystes, après l'approbation de l'agence ou lorsqu'un organisme indépendant a confirmé l'analyse ?

La relation avec le système juridique est un autre aspect à prendre en compte dans le cycle du renseignement, car le rôle des différents acteurs dans le processus du renseignement est moins clair que ceux impliqués dans l'acte juridique. Les sources humaines peuvent être motivées par de nombreux préjugés personnels. Par exemple, un analyste peut bénéficier d'incitations subtiles pour parvenir à une conclusion donnée, ou les collecteurs d'informations peuvent être contraints de ne collecter que certaines informations. (Morgan 2012) Par conséquent, il doit exister un mécanisme institutionnel capable de contester les hypothèses et les conclusions formulées lors de l'analyse des informations. En ce sens, certains services de renseignement utilisent une analyse dite « équipe rouge », une analyse alternative des informations et des conclusions tirées de produits d'informations. (US Department of the Army 1995) Selon un ancien officier de la CIA, Richard Heuer, une telle analyse alternative pourrait potentiellement utiliser des techniques spécifiques pour déterminer si les analyses étaient « fausses ». (Heuer 1999a)

Le stratège militaire John Boyd a créé un modèle de décision et d'action différent (OODA) (Boyd 1976) utile dans de nombreuses zones de conflit. Son modèle comprend quatre phases : 1) l'*observation* d'une menace ou d'une opportunité ; 2) *orientation* dans le contexte d'autres informations ; 3) la *décision* sur le meilleur plan d'action ; 4) l'*action* pour la réalisation du plan. Chaque nouvelle itération du cycle est plus rapide que la précédente, en raison de l'expérience

acquise. En s'assimilant avec le cycle traditionnel du renseignement, l'observation pourrait être un produit de la phase de collecte, alors que l'orientation est un produit de l'analyse.

2.3. La collecte du renseignement

Un processus de collecte d'informations commence lorsqu'un utilisateur introduit une requête dans le système. Plusieurs objets peuvent être associés au résultat d'une requête, avec différents degrés de pertinence. La plupart des systèmes estiment une valeur numérique indiquant dans quelle mesure chaque objet correspond à la requête, et classent les objets en fonction de cette valeur. De nombreuses recherches se sont concentrées sur les pratiques de recherche du renseignement. Une grande partie de ces recherches reposait sur les travaux de Leckie, Pettigrew (maintenant Fisher) et Sylvain, qui, en 1996, ont procédé à un examen approfondi de la littérature scientifique sur la recherche du renseignement par des professionnels. Les auteurs ont proposé un modèle analytique du comportement des professionnels en quête du renseignement, destiné à être généralisable dans l'ensemble de la profession, offrant ainsi une future plate-forme de recherche sur le terrain. Le modèle visait à « découvrir de nouvelles perspectives ... et à donner naissance à des théories plus raffinées et applicables de la recherche du renseignement ». (Leckie, Pettigrew, et Sylvain 1996, 188) Le signe distinctif de l'activité du renseignement est la recherche du type de renseignement que d'autres veulent cacher.

Edward Feigenbaum et Pamela McCorduck ont défini l'ingénierie de la connaissance comme suit : (Feigenbaum et McCorduck 1984)

> « L'ingénierie de la connaissance est la discipline de l'ingénierie qui implique l'intégration des connaissances dans un système informatique afin de résoudre des problèmes complexes qui nécessitent normalement un niveau élevé d'expertise humaine. »

À l'heure actuelle, l'ingénierie de la connaissance fait référence à la construction, à la maintenance et au développement de systèmes basés sur les connaissances. L'ingénierie de la

connaissance est liée à la logique mathématique et fortement impliquée dans les sciences cognitives et l'ingénierie socio-cognitive. La connaissance est produite par des agrégats socio-cognitifs (en particulier humains) et structurée en fonction de notre compréhension du fonctionnement de la rationalité et de la logique humaines.

Dans l'ingénierie de la connaissance, l'extraction des connaissances consiste à établir des connaissances à partir des sources structurées et non structurées d'une manière qui doit représenter les connaissances de manière à faciliter l'inférence. Le résultat de l'extraction va au-delà de l'établissement d'informations structurées ou de leur transformation en un schéma relationnel, nécessitant soit la réutilisation des connaissances formelles existantes (identificateurs ou ontologies), soit la création d'un système basé sur les données source. (Sfetcu 2016)

La collecte traditionnelle du renseignement est une technologie de traitement du langage naturel, qui extrait les informations des textes de langage et de leurs structures typiquement naturelles de manière appropriée. Les types d'informations à identifier doivent être spécifiés dans un modèle avant de démarrer le processus, de sorte que l'ensemble du processus de collecte traditionnelle du renseignement dépend du domaine. La collecte du renseignement est divisée en cinq tâches secondaires suivantes : (Cunningham 2006)

- *Reconnaissance des entités nommées* - reconnaissance et classification de toutes les entités nommées contenues dans un texte, à l'aide de méthodes basées sur des modèles grammaticaux ou statistiques.
- *Résolution de la coréférence* - identifie les entités équivalentes, qui ont été reconnues par la reconnaissance des entités nommées, dans un texte.
- *Construction de l'élément modèle* - les propriétés descriptives des entités, reconnues par la reconnaissance des entités nommées et la résolution de la coréférence, sont identifiées

- *Construction de la relation de modèle* - identifie les relations existantes entre les éléments de modèle.
- *Production du scénario modèle* - sera identifié et structuré en fonction des entités, reconnu par des entités nommées et résolution de la coréférence et des relations identifiées par la construction de la relation de modèle.

Dans la collecte du renseignement basée sur une ontologie, au moins une ontologie est utilisée pour guider le processus de collecte du renseignement à partir de texte en langage naturel. Le système OBIE utilise des méthodes de collecte traditionnelles du renseignement pour identifier les concepts, les cas et les relations des ontologies utilisées dans le texte, qui seront structurés dans une ontologie après le processus. Ainsi, la saisie d'ontologies est le modèle d'information à extraire. (Wimalasuriya et Dejing Dou 2010, 306–23) L'apprentissage d'ontologies automatise le processus de construction d'ontologies en langage naturel.

Les informations publiées dans les médias du monde entier peuvent être classées et traitées comme des secrets lorsqu'elles deviennent un produit d'information. Toutes les sources sont secrètes et l'activité de renseignement est définie de manière à exclure les sources ouvertes. (K. G. Robertson 1987)

Les sources fermées ou secrètes impliquent des « moyens spéciaux » pour accéder à l'information, et la technique peut inclure la manipulation, l'interrogation, l'utilisation des dispositifs techniques et l'utilisation extensive des méthodes criminelles. Ces techniques sont considérées comme coûteuses, fastidieuses et laborieuses par rapport aux méthodes open source. Dans certains cas, les méthodes de collecte cachées sont fortement associées au monde criminel. Noam Chomsky a indiqué qu'il existait de bonnes raisons pour lesquelles les services de renseignement sont si étroitement liés aux activités criminelles.

> « La terreur clandestine », a-t-il déclaré, « nécessite des fonds cachés et des éléments criminels, les agences de renseignement se tournant naturellement vers le quid pro quo ». (Chomsky 1992)

La découverte de la connaissance implique un processus automatique de recherche d'informations dans de grands volumes de données, à l'aide de l'exploration de données, sur la base de méthodologies et de terminologies similaires. (Wimalasuriya et Dejing Dou 2010, 306–23) La collecte du renseignement crée des abstractions des données d'entrée. Les connaissances acquises au cours du processus peuvent devenir des données supplémentaires pouvant être utilisées plus tard. (Cao 2010)

Les enquêtes en cours de collecte du renseignement visent à enrichir le renseignement, à éliminer les doutes ou à résoudre les problèmes.

Le processus de collecte du renseignement auprès de personnes (abrégé HUMINT) se fait par le biais des contacts interpersonnels. L'OTAN définit HUMINT comme « une catégorie de du renseignement tirées de l'informations recueillies et fournies par des sources humaines ». (NATO 2018) Les activités HUMINT typiques consistent en des requêtes et des conversations avec des personnes ayant accès à des informations. La manière dont les opérations HUMINT sont effectuées est dictée à la fois par le protocole officiel et par la nature de la source de l'information.

Les sources peuvent être neutres, amicales ou hostiles et peuvent ne pas être conscientes de leur implication dans la collecte du renseignement.

Le processus de collecte HUMINT consiste à sélectionner les personnes source, à les identifier et à mener des entretiens. L'analyse du renseignement peut aider avec des informations biographiques et culturelles. Lloyd F. Jordan reconnaît deux formes d'étude de la culture, toutes deux pertinentes pour HUMINT. (Jordan 2008)

Les méthodes de couverture sont compliquées et très risquées, mais elles soulèvent également des questions éthiques et morales. Une technique bien connue, par exemple, consiste à

manipuler des agents humains pour obtenir des informations. Le processus, connu sous le nom de « développement de source contrôlé », peut impliquer un recours intensif à la manipulation psychologique, au chantage et à des récompenses financières. (Godfrey 1978) Les collecteurs de renseignement qui appliquent ces techniques opèrent dans des environnements hostiles. Selon Sherman Kent, l'activité de renseignement pourrait s'apparenter à un moyen familier de recherche de la vérité. (Kent 1966) L'activité de renseignement, contrairement à toute autre profession, ne fonctionne pas selon des normes morales ou éthiques connues. Certaines de ces normes ont tendance à être, au mieux, cosmétiques. L'argument est que tout élément vital à la survie nationale est acceptable dans n'importe quelle situation, même lorsque la méthode provoque tout ce qui est démocratique. Les opérations clandestines restent floues en droit international et très peu de recherches scientifiques couvrent ce sujet.

2.4. Analyse du renseignement

Les analystes sont dans le domaine des « connaissances ». L'activité de renseignement fait référence à la connaissance et les types de problèmes abordés sont des problèmes de connaissance. Nous avons donc besoin d'un concept de travail basé sur la connaissance. Nous avons besoin d'une compréhension de base de ce que nous savons et de la manière dont nous le savons, de ce que nous ne savons pas et même de ce qui peut être connu et de ce qui ne peut pas être connu. (Vandepeer 2014) Matthew Herbert fournit un ensemble de principes utiles pour discuter des directives de Colin Powell au directeur américain du renseignement Mike McConnell. Powell aurait conseillé McConnell comme suit :

> « En tant qu'agent de renseignement, votre responsabilité est de me dire ce que vous savez. Dites-moi ce que vous ne savez pas. Ensuite, vous pourrez me dire ce que vous en pensez. Mais gardez toujours ces trois aspects séparés. » (Weiner 2007)

L'analyse du renseignement implique de « transformer des faits disparates en conclusions concentrées ». (Codevilla 1992)

Aucune définition n'est vraiment concluante pour clarifier le sens de l'analyse. En outre, la même personne ou le même groupe de personnes peut jouer divers rôles dans le cycle de processus, parfois même requis par l'analyse.

L'analyse devrait fournir une base utile pour conceptualiser les fonctions de l'activité de renseignement, dont les plus importantes sont l'« estimation » et la « prédiction ». L'activité de renseignement elle-même, dans sa forme de base, a une fonction décisionnelle. Une décision se caractérise par deux fonctions principales : (1) élections ou jugements entre des alternatives concurrentes, et (2) élections et jugements dans des conditions d'incertitude.

John Maynard Keynes déclare que, dans des conditions d'incertitude, « il n'y a aucune base scientifique sur laquelle former une probabilité calculable. Nous n'avons tout simplement aucune connaissance. » (Keynes 1937) Il s'ensuit qu'en l'absence de certitude, le décideur peut être contraint de prendre des mesures aux conséquences incertaines, ou de baser ses choix sur des prédictions futures, un exercice de raisonnement subjectif.

Radner a décrit une décision optimale caractéristique comme suit : « Pour chaque signal, une décision optimale maximise l'utilité conditionnelle attendue de la conséquence, compte tenu du signal. » Ce principe est décrit comme « maximiser l'utilité conditionnelle attendue ». (Radner 1972)

Les chercheurs ont utilisé des concepts tels que « l'information incomplète » et « les décisions dans des conditions d'incertitude » pour étudier les interactions des groupes, sur la base de la nature (subjective) des informations que les acteurs possèdent. (Ekpe 2005) Par exemple, Andrew Kydd a utilisé le modèle d'information incomplète pour expliquer le « modèle d'escalade

en spirale de la course aux armements » de Jervis. (Kydd 1997) La théorie de la décision d'incertitude appartient également à cette famille de comportements de connaissances incomplètes ou d'actions conditionnées par des sentiments subjectifs. Comme le fait remarquer Arrow Kenneth, « « l'incertitude » signifie que l'agent ne connaît pas l'état du monde. » (Arrow 1966)

L'analyse du renseignement applique des méthodes cognitives individuelles et collectives pour évaluer les données et tester des hypothèses dans un contexte socio-culturel secret. (Hayes 2007) L'analyste doit détecter les tromperies et extraire la vérité. L'analyse du renseignement a pour but de réduire l'ambiguïté. Supposer que les ennemis tentent de créer de la confusion n'est pas paranoïaque dans le cas des analystes, mais réaliste. Selon Dick Heuer, dans une expérience dans laquelle le comportement de l'analyste a été étudié, le processus en est un de raffinement incrémental.

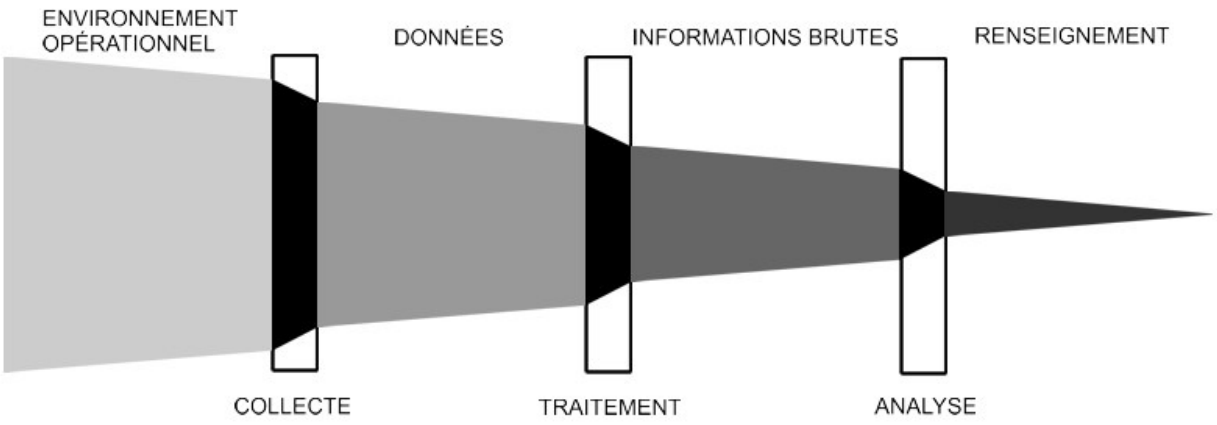

Fig. 2. L'activité de renseignement reflète un affinement progressif des données et des informations

Les disciplines académiques qui examinent l'art et la science de l'analyse du renseignement sont le plus souvent appelées « études de renseignement » et enseignées dans des institutions spécifiques.

L'analyste doit constamment se demander : « Qu'est-ce que les clients veulent / doivent savoir ? Comment préfèrent-ils la présentation ? Est-ce qu'ils essaient de choisir le meilleur plan d'action ou l'ont-ils choisi et maintenant ils doivent connaître les obstacles et les vulnérabilités sur le chemin choisi ? »

Parfois, lorsque l'analyste s'efforce de répondre aux besoins des clients internes et externes, la solution consiste à créer deux types de produits différents, un pour chaque type de client. Un produit interne peut contenir des détails sur les sources, les méthodes de collecte et les techniques d'analyse, tandis qu'un produit externe est plutôt journalistique : Lequel ? Quoi ? Quand ? Où ? Pourquoi ? « Comment » est souvent pertinent pour les journalistes, mais n'est pas indiqué dans l'activité de renseignement. Les actions se trouvent en trois étapes :

1. *Décision* d'agir
2. *Action*
3. *Désengagement* de l'action (Ikle 2005)

Les cartes heuristiques ou sémantiques peuvent aider à structurer les informations, ainsi que les dossiers de fichiers et les fiches. En outre, les bases de données, avec des techniques statistiques telles que la corrélation, l'analyse factorielle et l'analyse des séries chronologiques, peuvent donner une perspective.

L'analyse du renseignement a pour but de révéler à un certain décideur l'importance sous-jacente du renseignement sélectionnée. Les analystes doivent commencer par des faits confirmés, appliquer des connaissances spécialisées pour produire des conclusions plausibles mais moins sûres, et même prévoir, lorsque la prévision est correctement qualifiée. Les analystes ne doivent cependant pas se lancer dans des conjectures qui n'ont en fait aucun fondement.

L'analyse du renseignement implique l'élaboration de prévisions ou de plans d'action recommandés, sur la base d'un large éventail de sources de renseignement disponibles, ouvertes et sous couvert. L'analyse est développée en réponse aux demandes de la direction de l'organisation ou des clients, pour aider à la prise de décision. (Sfetcu 2016)

L'une des techniques utilisées dans l'analyse du renseignement est l'analyse des indicateurs, qui utilise des données historiques pour exposer les tendances et identifier les futurs changements majeurs dans un domaine d'intérêt, aidant à élaborer des prévisions fondées sur des preuves avec un biais cognitif réduit. (Heuer et Pherson 2010)

Les techniques analytiques structurées (TAS) sont devenues plus largement utilisées après les attaques contre World Trade Tower de 11 septembre 2001, lorsque la Commission nationale des États-Unis pour les actes terroristes ou la Commission du 11 septembre ont constaté que la communauté du renseignement « n'avait pas réussi à provoquer des mentalités analytiques, examiner les hypothèses essentielles, envisager des hypothèses alternatives et détecter les rapports trompeurs. » (Pherson 2013) Ces outils analytiques, conçus pour mieux gérer et normaliser la performance de l'analyse, représentent une tentative d'aligner la profession sur des principes scientifiques. D'un point de vue épistémologique, on peut soutenir que les TAS génèrent des connaissances propositionnelles et ne reconnaissent pas suffisamment la valeur des « connaissances tacites » dans le processus de résolution de problèmes dans l'analyse de l'information. (Gentry 2015)

Les indicateurs peuvent être des événements ou des actions uniques d'un facteur qui signifie un changement majeur, affectant les conditions des autres catégories, ou une combinaison d'événements qui remplissent une fonction similaire. Le processus se déroule comme suit :

1. Identifier un ensemble de catégories pertinentes pour l'exigence

2. Identifier un ensemble de facteurs pertinents pour chaque catégorie dans le contexte de l'exigence globale
3. Identifier les scénarios à court terme qui pourraient résulter du transfert immédiat ou de l'amélioration de chaque facteur
4. Identifier une série d'événements ou d'indicateurs qui pourraient signifier une amélioration ou une détérioration de chaque facteur
5. Examen des événements historiques et en cours pour les indicateurs de chaque facteur
6. Identifier des indicateurs uniques et des tendances des indicateurs pour prévoir le scénario à court terme le plus susceptible de se produire. (US Government 2009)

La communauté du renseignement américain standardise ses listes d'indicateurs, au sein d'une agence ou dans toute la communauté. (Artner, Girven, et Bruce 2016)

Une forme courante d'analyse du renseignement est l'utilisation des données des réseaux sociaux, à la fois sur Internet et sur mobile. De nombreux organismes gouvernementaux investissent massivement dans la recherche qui implique l'analyse des réseaux sociaux. Les communautés du renseignement considèrent que la plus grande menace vient de la décentralisation, sans dirigeants, de la dispersion géographique des terroristes, des extrémistes et d'autres personnes subversives et dissidentes. Ces types de menaces sont plus facilement contrés en découvrant des nœuds importants dans le réseau et en les éliminant. Pour cela, une carte détaillée du réseau est nécessaire. (Hogan, Carrasco, et Wellman 2007) L'utilisation des sites de réseautage social est considérée comme une forme de « surveillance participative », où les utilisateurs de ces sites se surveillent pratiquement eux-mêmes, affichant des informations personnelles détaillées sur les sites publics où ils peuvent être consultés par des entreprises et gouvernements.

2.5. Contre-espionnage

Selon la définition de William Johnson, le contre-espionnage (CE) est *une activité conçue pour protéger l'activité de renseignement d'une organisation contre des agents étatiques ou non étatiques*. (Johnson et Hood 2009) Il comprend la collecte et l'analyse d'informations spécifiques, ainsi que des activités préventives et contre-offensives contre les intentions et les actions visant la sécurité nationale, y compris le terrorisme. (Conrad 1985)

Dans la doctrine américaine, CE est désormais considéré principalement comme un contrepoids aux actions des services de renseignement étrangers (FIS HUMINT). Dans le manuel de contre-espionnage de l'armée américaine de 1995, CE avait une portée plus large. Plus récemment, la doctrine américaine de la communauté du renseignement limite l'objectif principal aux activités qui incluent généralement la lutte contre le terrorisme. (Matschulat 2007) La portée de la doctrine de contre-espionnage militaire américaine a été déplacée vers une publication classifiée, Joint Publication (JP) 2-01.2, *Counterintelligence and Human Intelligence Support to Joint Operations*. Pour chaque type d'action étrangère spécifique, des contre-mesures à rôle défensif et offensif sont prévues.

Contre-HUMINT s'occupe de la détection des sources hostiles ou potentiellement hostiles de HUMINT, ayant la responsabilité de surveiller un personnel fiable pour la prévention et la neutralisation des risques. (US Department of the Army 1981)

Les techniques offensives de la doctrine actuelle du contre-espionnage sont principalement dirigées contre les sources humaines, de sorte que le contre-espionnage peut être considéré comme synonyme de contre-renseignement offensive. Le contre-espionnage offensif (et le contre-terrorisme) agit soit en manipulant un adversaire (Foreign Intelligence Services - FIS, ou terroriste), soit en interrompant les opérations de l'opposant.

Le contre-espionnage est considéré principalement comme une discipline analytique, qui se concentre sur l'étude des services d'information. Compte tenu de cela, John Ehrman propose une définition appropriée du CE :

« Le contre-espionnage est l'étude de l'organisation et du comportement des services d'information d'États et d'entités étrangères, et l'application des connaissances qui en résultent ». (Ehrman 2009)

Le fondement de toutes les activités de contre-espionnage est l'étude des services d'information individuels, un processus analytique pour comprendre le comportement des entités étrangères (mission formelle, politique intérieure et étrangère, histoire et mythes au sein de l'entité respective, les personnes qui la composent).

Les opérations CE sont un sous-ensemble spécialisé d'opérations d'information en général, essayant généralement de créer des boucles de rétroaction sans fin. Généralement, il existe trois types d'opérations de contre-espionnage : la pénétration classique, les agents doubles, et l'identification et le suivi des agents du service ciblé.

Le contre-espionnage est un domaine encore sous-théorisé, sans méthodologie clairement définie. John Ehrman identifie plusieurs directions de recherche futures, telles que la politique des services, la sociologie des services et l'économie du contre-espionnage. En outre, les futures études de contre-espionnage dans la construction de la théorie devraient inclure des études comparatives et littéraires. Une solide théorie du contre-espionnage devra placer l'analyse au centre de l'activité de contre-espionnage et permettre une approche multidisciplinaire et intégrée des activités analytiques et opérationnelles.

2.6. Communautés épistémiques

Les communautés épistémiques sont des réseaux informels d'experts basés sur la connaissance, qui influencent les décideurs dans la définition des problèmes auxquels ils sont

confrontés, l'identification de différentes solutions et l'évaluation des résultats. (Hsu et Hasmath 2017) Peter M. Haas a défini le cadre conceptuel d'une communauté épistémique comme

> « ... un réseau de professionnels ayant une expérience et des compétences reconnues dans un domaine particulier et une revendication autoritaire concernant les connaissances pertinentes dans le domaine politique de ce domaine ou zone de problèmes ». (Haas 1992, 3)

Les membres d'une communauté épistémique sont issus de milieux académiques ou professionnels et se caractérisent par un ensemble unifiant de caractéristiques. (Sebenius 1992)

Les communautés épistémiques sont des entités socio-psychologiques qui créent et justifient la connaissance. Michel Foucault qualifie *mathesis* comme une épistème rigoureuse propre à permettre la cohésion d'un discours et donc l'unification d'une communauté. Dans la philosophie de la science et la science des systèmes, le processus de formation d'une communauté épistémique auto-entretenue est parfois appelé une mentalité, semblable à une tendance ou une faction en politique.

Un contre-exemple de ce qui n'est PAS une communauté épistémique est fourni par Mai'a K. Davis Cross en tenant compte de l'Agence européenne de défense (AED) et du Centre de renseignement et de situation de l'Union européenne (IntCen). (Cross 2015) Cross fait valoir que, bien que composées d'experts de haut niveau en matière de sécurité, ces deux organisations ne constituent pas des communautés épistémiques. Les véritables communautés épistémiques, notamment les diplomates, les experts militaires, les chercheurs en sécurité et les experts civils en gestion de crise, ont considérablement influencé la politique de sécurité de l'UE.

Les groupes d'experts qui ne constituent pas des communautés épistémiques ne sont pas seulement des cas faibles ou en croissance. Il peut s'agir fondamentalement de différents types d'acteurs aux caractéristiques divergentes.

Une communauté épistémique comprend rarement tous les membres d'une organisation formelle. Une communauté épistémique forte essaie de transcender son rôle professionnel officiel

en tant que groupe et est souvent en mesure de convaincre les décideurs de changer fondamentalement la nature de leurs objectifs politiques.

Une communauté épistémique peut être considérée comme un groupe de personnes qui n'ont pas ensemble une histoire spécifique, mais qui recherchent une idée d'origine commune comme si elles formaient une communauté intentionnelle. Par exemple, une communauté épistémique peut être trouvée dans un réseau de professionnels d'une grande variété de disciplines et d'environnements, (Keman 1998) y compris les services de renseignement.

Selon Haas, les communautés épistémiques (1) partagent un avis professionnel sur une question de politique, (2) évaluent la validité de leurs objectifs politiques dans leur domaine d'expertise, (3) s'engagent dans un ensemble commun de pratiques concernant le domaine problématique avec le but d'améliorer le bien-être humain et (4) partagent les croyances de principe. (Haas 2001, 11578–79)

Les communautés épistémiques ont également une « composante normative », ce qui signifie que le but ultime est toujours une amélioration de la société, plutôt que le gain propre de la communauté elle-même. (Haas 1992)

Dans les relations internationales et les sciences politiques, une communauté épistémique peut également être considérée comme un réseau mondial de professionnels basé sur des connaissances dans des domaines scientifiques et technologiques qui affectent souvent les décisions politiques. (Morin et Louafi 2017)

Les communautés épistémiques ont la plus grande influence dans des « conditions d'incertitude politique et de visibilité », (Radaelli 1999, 763) généralement après une crise ou un événement déclencheur.

L'Union européenne, avec ses processus d'intégration en cours, ses valeurs démocratiques partagées, ses institutions supranationales et ses interactions transnationales, est très favorable à la formation de communautés épistémiques. (Loik 2013) La politique de sécurité de l'UE est un domaine où plusieurs communautés épistémiques sont basées à Bruxelles.

3. Ontologie

Dans l'activité de renseignement, le problème ontologique est lié à la nature et aux caractéristiques des entités qui menacent et sont menacées. Selon Eric Little et Galina Rogova, « la menace est un objet ontologique très complexe et, par conséquent, une ontologie appropriée doit être construite conformément aux principes métaphysiques formels qui peuvent prendre en compte la complexité des objets, des attributs, des processus, des événements et des relations qui composent ces états de choses". (Eric G. Little et Rogova 2006)

L'argument de Björn Müller-Wille concernant la sécurité et les menaces permet de mettre en évidence l'interdépendance entre les entités menaçantes et menacées. En ce sens, les analystes de l'information doivent définir à la fois ce qu'est une menace et ce qui est menacé. Ainsi, une ontologie significative de la menace doit inclure à la fois les menaces et les entités menacées. (Vandepeer 2011)

Développer une ontologie des menaces nécessite une taxonomie. Buzan, Waever et Wilde fournissent une taxonomie potentiellement utile utilisée pour décrire l'analyse de sécurité. (Buzan et al. 1998) Ils soutiennent que l'analyse de la sécurité implique trois acteurs distincts. De cette taxonomie, adaptée à l'analyse du renseignement, résultent les entités suivantes :

- Un *référent* c'est quoi ou qui est menacé ;
- Un *analyste* agit comme un « déterminant de la menace » ; et
- Un *acteur de la menace* qui est évalué par l'analyste comme menaçant le référent.

Le référent de la menace est généralement l'État, à savoir la survie de l'État et de sa population. (Singer 1958) Le *Quadrennial Homeland Security Review* décrit la sécurité comme l'exigence de « protéger les États-Unis et leur peuple, leurs intérêts vitaux et leur mode de vie ». (Department of Homeland Security 2010) La mondialisation rend de plus en plus difficile d'identifier clairement les intérêts de l'État, même de la population. Selon la Convention de Montevedio, les quatre conditions généralement acceptées pour un État sont : une population permanente ; territoire défini ; un gouvernement ; et la capacité d'entrer en relation avec d'autres États. (Australia Department of Defence 2009) Ces exigences se réfèrent généralement à quatre aspects d'un État qui peuvent être menacés, à savoir : la population, le territoire, le gouvernement et les intérêts. Pour la nature et les caractéristiques des menaces étatiques et non étatiques, la manière dont ces entités peuvent menacer ces quatre facteurs est examinée.

Les intérêts de l'État comprennent la menace de l'influence politique de l'État, limitant ainsi la capacité de l'État à développer des relations favorables ou solides avec d'autres États, la stabilité régionale, (a242) la stabilité économique, le développement et l'infrastructure financière de l'État, (Australia Department of Defence 2009) l'accès aux marchés, les ressources énergétiques, les lignes de communication et la capacité des citoyens à voyager.

Les acteurs non étatiques (en particulier ceux qui menacent) ne sont souvent pas définis. Une définition utile pour les capturer est "... toute personne ou groupe de personnes agissant indépendamment des gouvernements officiels". (Australia Department of Defence 2002)

L'évaluation de la menace (impact) est définie par Steinberg et al comme "le processus d'estimation et d'anticipation des effets sur les situations des actions planifiées ou estimées/anticipées par les participants ; elle comprend les interactions entre les plans d'action de plusieurs acteurs (par ex., en évaluant les susceptibilités et les vulnérabilités aux actions menacées

estimées/prévues, en tenant compte de leurs actions prévues)." (Omand 2009) Il s'ensuit que différentes fonctions et éléments d'évaluation des menaces doivent être pris en compte. (Rudd 2008) La complexité ontologique des éléments de menace nécessite une analyse ontologique basée sur la métaphysique, qui peut classer efficacement les différents types d'objets complexes, de propriétés et d'attributs, d'événements, de processus et de relations qui intéressent divers décideurs.

Le traitement de l'évaluation des situations et des menaces (ESM) fait référence à des informations dépendantes du contexte sur les facettes dynamiques de la réalité, (Eric G. Little et Rogova 2006) de sorte que les ontologies de l'ESM doivent être capables de capturer la structure de la réalité en offrant des capacités pour décrire la multitude de types de relations (par exemple, relations spatio-temporelles, intentionnelles et de dépendance) qui existent entre différentes entités situationnelles (et leurs agrégations) à différents niveaux de granularité. (Bittner et Smith 2003) Pour cette raison, les ontologies à utiliser pour évaluer la situation et les menaces nécessitent une compréhension plus large des types de relations et d'entités relationnelles, trouvées initialement dans les écrits d'Aristote (Aristotle 1991) et formalisées plus tard par Edmund Husserl. (Husserl 1900) Il est important que les ontologies ESM soient structurées dans un cadre métaphysique général plus élevé, afin de pouvoir décomposer les éléments les plus abstraits du domaine d'intérêt, ainsi que les relations entre eux.

Eric G. Little et Galina L. Rogova ont développé une "ontologie des menaces", (Eric G. Little et Rogova 2006) une version modifiée de l'ontologie officielle de base (Grenon et Smith 2004) composée de deux sous-niveaux orthogonaux nommés SNAP et SPAN, qui sont conçus pour capturer les caractéristiques spatiales et temporelles de l'ontologie. Sur la base de la distinction entre le continuant et l'occurrence, des objets spatio-temporels ontologiquement complexes ont été modélisés, avec une bifurcation formelle entre les objets en tant qu'éléments

pouvant exister entièrement à un moment donné dans l'espace et le temps, par rapport aux événements procéduraux, dont les parties et les relations partielles ont lieu constamment au fil du temps et n'existe donc jamais pleinement dans un lieu ou un moment particulier. Cette distinction a permis d'éviter certains problèmes philosophiques traditionnels d'identité.

L'ontologie officielle de base est conçue selon la théorie de la méréotopologie, (B. Smith 1996) une théorie qui combine une logique des parties et des relations partielles (par exemple, la méréologie) avec une logique d'expansion spatiale et de connexion (c'est-à-dire la topologie), langage capable de traiter la multitude d'objets ontologiques requis pour le traitement de fusion de niveau supérieur, par exemple, les objets, les propriétés/attributs, les espaces, les temps et les nombreux types de relations simples et complexes qui existent entre eux.

Les informations utilisées dans l'évaluation des menaces sont extrêmement incertaines, avec un bruit de fond, contradictoire, redondant, d'importance variable et de faible fidélité. Il est donc nécessaire d'incorporer l'incertitude, la fiabilité et l'imprécision dans la caractérisation des relations qualitatives méréotopologiques. (Eric G. Little et Rogova 2006)

Au niveau supérieur, dans son ensemble, les gens existent en tant qu'entités relationnelles, et pas seulement en tant que collections d'éléments indépendants. Le problème est ici d'une importance ontologique, où la modélisation des collections d'éléments n'est pas la même que la modélisation de l'ensemble, car le même élément complexe peut être compris différemment selon qu'il est compris comme une collection ou comme un tout. (B. Smith 1996) La théorie de la méréotopologie fournit un moyen de décrire formellement les types de relations complexes partielles entre eux qui comprennent des éléments tels que les menaces, dans lesquels les trois éléments d'intention, de capacité et d'opportunité sont dans une relation formelle de dépendance fondamentale.

La capture des relations métaphysiques, telles que la dépendance fondamentale, est nécessaire pour concevoir des ontologies de la menace. Compte tenu de la nature complexe des menaces, il est essentiel de concevoir un cadre ontologique pouvant inclure de nombreux types de relations nécessaires à la décomposition correcte des éléments complexes. (E. G. Little et Rogova 2005)

La définition ontologique des certaines caractéristiques essentielles des parties et de leurs relations, ainsi que les métriques et contraintes de proximité, permettront alors une meilleure définition et identification des groupes dispersés.

Une ontologie pour l'analyse et l'action contre les menaces doit être capable de modéliser les distinctions ontologiques entre les menaces potentielles et viables. Cela permet de mieux comprendre comment les éléments de menace (c'est-à-dire les intentions, les capacités et les opportunités) peuvent exister et peuvent évoluer avec le temps. L'escalade des menaces d'un État potentiel à un État viable pourrait être évitée en utilisant des techniques appropriées d'atténuation des menaces.

D'autre part, la stratégie d'amélioration sémantique (AS) (Salmen et al. 2011) est basée sur l'utilisation d'ontologies simples dont les termes sont utilisés pour marquer (ou annoter) les artefacts de données source de manière cohérente. Les termes d'une ontologie AS sont liés ensemble dans une hiérarchie simple par le biais de la relation "is_a" (ou sous-type). Chaque terme n'apparaît qu'une seule fois dans cette hiérarchie et est associé de manière stable aux termes parent et enfant dans la hiérarchie, même si de nouveaux termes sont ajoutés à l'ontologie au fil du temps. Cette stabilité est importante, car le succès de la stratégie nécessite des ontologies qui peuvent être réutilisées à plusieurs reprises pour annoter de nombreux types de données différents de manière à desservir plusieurs communautés autres que les analystes, contribuant ainsi à la création d'une

image opérationnelle commune de plus en plus complète. AS est conçu pour être à la fois plus stable et plus flexible que les approches traditionnelles d'harmonisation et d'intégration, qui, généralement basées sur une cartographie *ad hoc* entre les modèles de données, se détériorent souvent au fil du temps. (B. Smith 2012)

Les ontologies AS sont organisées sur trois niveaux, avec des degrés de flexibilité successifs: 1) Une ontologie unique, petite et neutre du domaine supérieur pour laquelle notre candidat sélectionné est l'ontologie officielle de base; (Volkswagen Foundation 2002) 2) Ontologies de niveau moyen, formées en regroupant des termes qui se réfèrent à des domaines d'action spécifiques ou à des tâches spécifiques, comme l'échange d'informations inter-agences; (B. Smith, Vizenor, et Schoening 2009) 3) Ontologies de bas niveau qui se concentrent sur des domaines spécifiques. L'approche AS est conçue pour être d'une utilité maximale pour les utilisateurs de l'information. Le contenu ontologique est créé uniquement en réponse aux besoins situationnels identifiés des analystes, et les exigences architecturales sont conçues pour assurer une évolution cohérente des ressources de AS sans sacrifier la flexibilité et l'expressivité nécessaires au développement réel sur le terrain. (B. Smith 2012) La stratégie AS peut déterminer le développement ontologique collaboratif et la réutilisation à des fins de collecte de données multiples, à la fois internes et externes.

4. Épistémologie

Dans le renseignement, l'épistémologie est l'étude de la connaissance de la menace et de la manière dont la menace est appréhendée dans le domaine de l'analyse du renseignement.

La plupart des définitions de l’analyse du renseignement ne prennent pas en compte le fait que le statut normatif épistémique de l’analyse du renseignement analysée est une connaissance et non une alternative inférieure. Les contre-arguments au statut épistémologique de l’analyse du

renseignement est sa finalité orientée vers l'action et son contenu tourné vers l'avenir. (Rønn et Høffding 2013)

À la suite des attentats du 11 septembre, une commission du terrorisme a été créée en États-Unis pour identifier les défaillances et les faiblesses des agences de renseignement américaines, pour tirer des enseignements des failles de sécurité et pour empêcher de futures attaques contre la sécurité et la sûreté nationales. L'essentiel était que les institutions de renseignement américaines n'avaient pas l'imagination et la capacité de faire des prédictions pertinentes - c'est-à-dire de relier les « points » pertinents et de tirer des conclusions pertinentes. (Anderson, Schum, et Twining 2009)

Sherman Kent, dans *Strategic Intelligence* (1949), divise le domaine en trois composantes : (Kent 1966) connaissances, organisation et activité. De l'avis de Michael Herman, dans *Intelligence Services in the Information Age* (2001), le domaine de l'activité d'information peut être divisé en : activité, sujets, produit et fonction. (Herman 2001) Scott et Jackson, dans *The Study of Intelligence in Theory and Practice*, article introductif de la revue *Intelligence and National Security* no. 19 de 2010, (Scott et Jackson 2004) complètent les divisions de Kent et Herman en fournissant une analyse de la façon de faire des distinctions significatives dans le domaine du renseignement.

Le renseignement contraste avec les informations et les connaissances et peuvent être placées dans un continuum pyramidal composé de données, d'informations et de connaissances. (Dean et Gottschalk 2007) Le renseignement peut être inséré dans deux positions différentes : soit entre informations et connaissances, soit au sommet de la hiérarchie des connaissances. (Rønn et Høffding 2013)

Dans le premier cas, le renseignement est épistémique par rapport aux informations : Geoff Dean et Petter Gottschalk considèrent que « le renseignement est placé en permanence entre informations et connaissances, car le renseignement représente (...) une forme validée d'informations » (Dean et Gottschalk 2007) La compréhension normative du renseignement peut être considérée comme la «plus plausible information». Le renseignement est souvent appelé « connaissances antérieures » compris comme des informations et une évaluation des activités futures. (Wheaton et Beerbower 2006) L'attribut scientifique du renseignement est caractérisé par des avertissements concernant des événements et des actions potentiellement nuisibles. La question est alors de savoir s'il disqualifie le renseignement en tant que connaissance. (Rønn et Høffding 2013)

Si le renseignement est placé au-dessus de la connaissance, c'est plus qu'une simple connaissance. Jerry Ratcliffe justifie ce classement comme suit :

> « Alors, pourquoi le renseignement serait-il situé au-dessus du continuum des connaissances ? En effet, les produits du renseignement sont des produits d'action inhérents. En d'autres termes, les produits de la connaissance peuvent générer la compréhension, mais les produits du renseignement devraient générer de l'action. » (Ratcliffe 2008)

Cela signifie que l'activité de renseignement génère des « connaissances exploitables ». Mais cette interprétation, tout en affirmant que le renseignement est un type de connaissance, semble confondre son statut épistémique avec sa fonction normative, celle des actions et décisions d'orientation.

Selon Simon Høffding, lorsque nous comparons le statut épistémique du renseignement selon les positions ci-dessus, la relation entre l'information et la connaissance dans le continuum est asymétrique en raison du niveau différent de plausibilité et de pertinence. (Rønn et Høffding 2013) Cependant, ce qui importe, c'est l'attitude propositionnelle d'un agent vis-à-vis du contenu

d'une information. En ce sens, les informations et les connaissances sont interdépendantes et pourraient donc toutes deux être traitées comme de renseignement.

Le concept principal du renseignement est la menace. Cela se reflète dans le travail fondateur de J. David Singer de 1958, *Threat Perception and the Armament-Tension Dilemma*, (Singer 1958) à travers un modèle quasi mathématique :

Perception des menaces = Capacité estimée x Intention estimée.

Les paramètres d'intention et de capacité peuvent être décrits comme l'épistème dominant utilisé pour comprendre la menace dans le domaine de l'analyse du renseignement. (Vandepeer 2011) Puisqu'ontologiquement important n'est que l'acteur de la menace, cela signifie que pour Singer, seules les intentions et les capacités de l'acteur de la menace comptent.

Samuel Huntington, dans *The Soldier and the State* (1957), soutient que le personnel militaire est qualifié pour évaluer les capacités, mais pas les intentions. (Huntington 1981) Malgré les changements qui incluent en priorité l'évaluation des acteurs non étatiques, la menace reste définie en utilisant un seul modèle, en se concentrant en particulier sur l'acteur de la menace. Cela signifie que les analystes connaissent et comprennent déjà l'acteur de menace qu'ils essaient d'évaluer. L'évaluation des menaces est basée sur la connaissance et la compréhension d'un acteur. L'identification est présumée.

Le modèle Singer a ensuite été élargi en ajoutant de nouveaux paramètres, les plus courants étant la vulnérabilité et les opportunités. Le paramètre de vulnérabilité est plutôt focalisé sur le référent de menace, ce qui fait que la vulnérabilité est définie comme la sensibilité d'un référent à une attaque. Richard Pilch utilise la formule suivante : (Howard et Sawyer 2003)

Menace = Vulnérabilité x Capacité x Intention

L'un des problèmes du paramètre de vulnérabilité est que plus la cible potentielle (référent) est générique, moins l'évaluation de la menace sera correcte.

Le paramètre d'opportunité apparaît également en complément du modèle conventionnel :

Menace = Opportunité x Capacité x Intention

L'opportunité incarne une compréhension à la fois de l'acteur de la menace et du référent, et peut être définie comme un moment ou une opportunité favorable pour un acteur de la menace par rapport à un référent. (Vandepeer 2011)

Malgré les efforts pour incorporer des paramètres supplémentaires, l'hypothèse principale est que l'épistème dominant, avec un accent principal sur l'acteur de la menace, reste essentiel pour l'évaluation de la menace.

La théorie de l'enquête examine les différentes manières dont chaque type d'enquête atteint son objectif. Bennets établit une distinction entre les données, les informations et les connaissances, déclarant que :

> « Les données sont des faits discrets et objectifs sur des événements qui incluent des chiffres, des lettres et des images sans contexte, tandis que les informations sont données avec un certain niveau de signification, car elles décrivent une situation ou une condition. Les connaissances reposent sur des données et des informations et sont créées au sein de l'individu. Ces connaissances représentent une compréhension du contexte, une compréhension des relations au sein d'un système et la capacité d'identifier les points de mise en œuvre et les faiblesses et de comprendre les implications futures des mesures prises pour résoudre les problèmes. » (Holsapple 2004)

Pour produire une information objective, l'analyste doit utiliser un processus adapté à la nature du problème, en utilisant l'un des modes fondamentaux de raisonnement: (Krizan 1999a) induction (la recherche de causalité, la découverte des relations entre les phénomènes étudiés), la déduction (l'application du général, du général au spécifique), l'intuition entraînée (appliquer une perspective spontanée, validée avec les faits et les outils disponibles), la méthode scientifique (falsifier des hypothèses et tester des scénarios fictifs).

Induction : lorsque les analystes font une généralisation ou découvrent des relations entre des phénomènes sur la base d'observations ou d'autres preuves.

« L'induction consiste à établir une relation entre un terme extrême et le terme moyen à l'aide de l'autre terme extrême ; par exemple, si B est le moyen terme de A et C, en prouvant par C que A s'applique à B ; c'est ainsi que nous appliquons les inductions. » (Aristotle 1989, chap. 2.23)

Stephen Marrin élargit l'approche inductive, indiquant que les analystes ont une approche analytique en deux étapes. (Marrin 2012a) Ils utilisent une « analyse de modèle et de tendance » intuitive - consistant à identifier des comportements répétés dans le temps, puis à s'appuyer sur des règles *ad hoc* ou des modèles mentaux dérivés de l'étude de la théorie pertinente - par exemple, l'économie, la science politique ou la psychologie - pour déterminer l'importance du modèle. (Duvenage 2010a) Michael Collier soutient que la méthode inductive laisse trop de place à la conjecture, à la superstition et à l'opinion.

Déduction : le raisonnement à partir des règles générales à des cas spécifiques, si l'hypothèse est testée, contrairement au raisonnement inductif où l'hypothèse est créée.

« Lorsque trois termes sont si étroitement liés que celui-ci est entièrement contenu dans celui du milieu et que celui du milieu est totalement ou entièrement exclu du premier, les extrêmes doivent se conformer au syllogisme parfait. Par « moyen terme », on entend ce terme qui est inclus dans un autre et en contient un autre en lui-même, et qui est au milieu par sa position ; c'est aussi ce terme avec « extrêmes » (a) celui qui est contenu dans un autre terme, et (b) dans lequel un autre terme est contenu. Car si A est vrai pour tout B, et B pour tout C, A doit nécessairement être vrai pour tout C. » (Aristotle 1989, chap. 1.4)

Krizan cite Clauser et Weir qui avertissent que le raisonnement déductif doit être utilisé avec prudence lors de l'analyse des informations, car il y a rarement des systèmes fermés ici, donc des hypothèses basées sur un autre ensemble de faits, appliquées à un nouveau problème et présumées vraies, peuvent être fausses et conduire à des conclusions incorrectes. (Krizan 1999a)

Contrairement aux arguments déductifs, dans le raisonnement inductif il est possible que la conclusion soit fausse, même si toutes les prémisses sont vraies. Au lieu d'être valides ou

invalides, les arguments inductifs sont forts ou faibles, ce qui montre la probabilité que la conclusion soit vraie.

Abduction : mode de raisonnement non officiel ou pragmatique pour décrire comment nous « justifions la meilleure explication » dans la vie quotidienne.

« Nous avons la réduction (απαγωγη, abduction) :

1. Lorsqu'il est évident que le premier terme s'applique au milieu, mais qu'il n'est pas évident que le milieu s'applique au dernier terme, il est néanmoins plus probable ou moins probable que la conclusion ; ou
2. S'il n'y a pas beaucoup de termes intermédiaires entre le dernier et le milieu.

Parce que dans tous ces cas, l'effet est de nous rapprocher de la connaissance. » (Aristotle 1989, chap. 2.25)

Waltz déclare que l'abduction est, dans le renseignement, une description pratique d'un ensemble interactif d'analyse et de synthèse pour arriver à une solution ou une explication, créant et évaluant plusieurs hypothèses. (Waltz 2003, 173) Dans l'abduction, l'analyste génère de façon créative un ensemble d'hypothèses et se propose de les examiner si les preuves disponibles sont sans équivoque étayées. La dernière étape, à savoir tester les preuves, est une inférence déductive. L'abduction peut être similaire à l'intuition dans le cas de l'analyste. Ce raisonnement est erroné car il est sujet à des erreurs cognitives, mais il a la capacité d'étendre la compréhension du problème du renseignement traité au-delà des prémisses d'origine.

Méthode scientifique : elle utilise l'induction pour développer l'hypothèse, et la déduction est utilisée pour la tester. Si le test ne valide pas l'hypothèse, une nouvelle hypothèse doit être formulée et de nouvelles expériences conçues pour valider cette hypothèse. (Marrin 2012a) Dans le renseignement, il n'y a pas d'expériences et d'observations directes du sujet, mais l'analyste peut développer des hypothèses ou des explications à partir des informations obtenues de différentes

sources. Les hypothèses peuvent ensuite être examinées pour la plausibilité et testées itérativement par rapport à de nouvelles informations. (Duvenage 2010a)

Techniques analytiques structurées : ils représentent des outils complémentaires aux méthodes d'analyse traditionnelles et intuitives et ne sont pas seulement des alternatives. L'utilisation des techniques analytiques structurées pourrait non seulement améliorer la qualité de l'analyse du renseignement, mais aussi renforcer la crédibilité de l'analyse, qui est souvent sujette à des critiques de la politisation réelle ou perçue et d'autres pressions organisationnelles. Heuer et Pherson classent 50 techniques analytiques structurelles en huit catégories qui correspondent aux pièges cognitifs courants et indiquent les fonctions que les analystes doivent remplir pour surmonter ces pièges. (Heuer et Pherson 2010) Certaines de ces méthodes sont:

- *Décomposition et visualisation* : dépasser les limites de la mémoire de travail
- *Générer des idées* : stimuler l'esprit de l'analyste avec de nouvelles possibilités pour étudier et visualiser un problème d'intelligence sous différents angles
- *Scénarios, indicateurs, marquages* : identifier ceux qui pourraient changer une situation et préciser les différents scénarios possibles
- *Générer et tester des hypothèses* : les analystes, dans le subconscient, font des hypothèses sur chaque information et les valident intuitivement ; des outils analytiques structurés aident à examiner un plus large éventail d'hypothèses, de possibilités et d'explications alternatives
- *Analyse des causes et effets* : les analystes doivent être prudents dans les hypothèses et conclusions qui n'ont pas été testées en ce qui concerne la cause et l'effet de certains événements ou indicateurs.

- *Techniques de recadrage* : aide les analystes à changer leur cadre de référence / mentalité sur un problème analytique en changeant des questions ou des perspectives
- *Techniques d'analyse des défis* : aide à fournir le meilleur produit possible aux clients là où il y a de grandes différences de points de vue, en mettant en évidence aussi les points de vue minoritaires
- *Analyse de l'aide à la décision* : permet aux analystes de voir le problème du point de vue des décideurs.

Biais : les biais peuvent fausser l'application correcte de l'argumentation inductive, empêchant ainsi la formation de la conclusion la plus logique basée sur des indices. Des exemples de tels biais incluent l'heuristique de disponibilité, les biais de confirmation et les biais de prédiction.

4.1. La connaissance tacite (Polanyi)

Owen Ormerod a développé une théorie selon laquelle le point de vue de Michael Polanyi sur la science peut aider à comprendre le processus et le « produit » de l'analyse du renseignement. (Ormerod 2018a) Les arguments de Michael Polanyi concernant les activités des scientifiques sont transférables dans le domaine de l'analyse du renseignement, offrant une perspective nuancée pour percevoir les défis épistémologiques et les problèmes auxquels sont confrontés les analystes. Les concepts de « connaissance tacite » et de « connaissance personnelle » de Polanyi contribuent au développement d'une compréhension plus épistémologiquement efficace de certains aspects du processus et du produit de l'analyse du renseignement.

Il existe une myriade de tentatives, à la fois dans la littérature sur la sécurité nationale et dans la littérature sur l'application des lois, pour aligner l'analyse du renseignement sur les principes et les pratiques « scientifiques ». (Cooper et Intelligence 2012) Ormerod soutient que la

théorie développée par Polanyi est transférable dans le domaine du renseignement. Les conceptions de Polanyi de connaissance tacites et personnelles ont une forte influence sur la perception de la pratique de l'analyse du renseignement.

Actuellement, il existe un intérêt croissant pour la recherche d'une « théorie du renseignement ». (Hunter et MacDonald 2017) Dans ce contexte, les problèmes épistémologiques seront mis en avant dans l'analyse du renseignement. (Lillbacka 2013, 304) L'analyse du renseignement est une activité visant à accroître les connaissances, et l'amélioration de l'analyse nécessite une compréhension de l'épistémologie ou de la théorie de l'origine et de la nature des connaissances pertinentes. Une manière discursive de percevoir le domaine de « l'activité du renseignement » peut être distinguée de deux manières fondamentales : (Bang 2017a) a) la manière d'obtenir des informations ; b) comment le renseignement peut aider les décideurs, sur la base des informations collectées et analysées. (Mudd et Abbey 2015)

Les bases épistémologiques des études du renseignement sont largement extraites du paradigme de la « sécurité nationale ». (O'Malley 2016) Patrick Walsh a présenté trois caractéristiques fondamentales qui représentent clairement le fondement de la profession dans le secteur du renseignement : « environnement du renseignement » (collecte et analyse), « secret » (couverture et collecte) et « surveillance » (suivi des sujets en question). (Walsh 2010, 29)

Les objectifs de l'analyste du renseignement peuvent généralement comprendre les catégories suivantes : 1. La modélisation normative nécessaire aux analystes pour représenter le fonctionnement des systèmes ; 2. Modélisation descriptive utilisée pour comprendre une situation donnée et son fonctionnement ; 3. Modélisation prédictive ou exploratoire représentant la façon dont un système dynamique pourrait fonctionner à l'avenir, dans certaines circonstances. (Waltz 2014, 2-3)

Il y a un fort intérêt à examiner psychologiquement les aspects de l'analyse. (Heuer 1999a) Cela est particulièrement vrai en termes de compréhension des connaissances dans l'analyse. (Waltz 2014, 1) Les analystes doivent être sensibles non seulement aux conclusions auxquelles ils parviennent, mais également à la manière dont ils sont parvenus à de telles déclarations. Comme l'a observé Heuer :

> « Les analystes du renseignement doivent être conscients de leurs propres processus de raisonnement. Ils devraient réfléchir à la façon dont ils émettent des jugements et parviennent à des conclusions, et pas seulement à des jugements et à des conclusions efficaces. » (Heuer 1999a, 31)

Dans ce sens psychologique, l'analyse du renseignement est une activité qui fait appel à des méta-connaissances ou, comme le note Mark Lowenthal, à la « pensée de la pensée » (Lowenthal cité dans (Moore et College 2010, 8)). Un objectif central de l'analyse du renseignement est une activité de transition de la « connaissance » à la « compréhension ». (Ellis-Smith 2016, 36)

Selon Ormerod, le concept de « connaissance personnelle » de Polanyi contribue à un cadre épistémologique plus nuancé pour expliquer ce que signifie pour les analystes de « connaître » les produits de l'activité de renseignement. (Ormerod 2018a) Pour Polanyi, la vérité est une condition objective, et la découverte de la vérité est obtenue en faisant correspondre une théorie avec une réalité objective. (Jacobs 2001, 464) Polanyi rejette le relativisme cognitif ou la relativité de la réalité basée sur notre perception. (Polanyi 1962, 315–16) Polanyi était convaincu qu'il existait une réalité objective; cependant, pour devenir intelligibles, nous devons essayer de « maîtriser et faire notre propre » interprétation et compréhension. (Polanyi et Sen 2009, 80) Selon Polanyi, le processus de découverte commence lorsque certaines impressions sont considérées comme inhabituelles et suggestives: un problème se présente à l'esprit; procéder à la collecte d'indices en

vue d'une ligne de résolution de problèmes spécifique; et culmine dans l'hypothèse d'une solution claire. (Polanyi 1964, 25)

Polanyi propose une approche difficile pour comprendre ces problèmes épistémologiques à partir de l'analyse du renseignement. Pour Polanyi, il y a l'hypothèse derrière l'acte d'observation. (Polanyi 1998, 19) Selon Polanyi, les recherches scientifiques impliquent une interaction permanente d'imagination et d'observation. Alors que le domaine du renseignement reconnaît qu'il est partiellement impliqué dans un jeu de devinettes, l'art de l'enquête, tel que le comprend Polanyi, offre un langage plus riche (Colapietro 2011, 58) et la base épistémologique pour reconnaître cet aspect dans l'analyse scientifique et du renseignement.

Polanyi soutient que, pour prendre en compte le processus de résolution de problèmes et faire des découvertes, nous devons suffisamment reconnaître le rôle important des connaissances tacites et la relation que ces connaissances ont avec les connaissances explicites. Polanyi situe cette forme de connaissance comme un élément essentiel de sa science et de son épistémologie.

> « Le concept de connaissance personnelle de Polanyi exprime épistémologiquement que, dans le domaine du renseignement, l'activité de l'analyste est trop diversifiée pour avoir une approche « descendante » unique pour comprendre les revendications de la connaissance en tant que produit. (Bang 2017a) Selon Polanyi, parce qu'il n'y a pas de « méthode scientifique », le scientifique doit s'appuyer sur des connaissances personnelles, ce qui remet considérablement en cause le fait que les revendications de connaissances doivent suffisamment reconnaître le rôle du « connaisseur ». C'est l'argument central qui soutient l'idée d'une compréhension ascendante de ce que signifie « savoir » quelque chose. Les exigences en matière de connaissances sont exprimées par le « coefficient personnel » des connaissances personnelles de l'analyste, qui, selon Polanyi, est une caractéristique fondamentale de ce que signifie « savoir » quelque chose. (Polanyi 1962) Les arguments de Polanyi concernant l'autorité de la science en tant que forme valable d'enquête et moyen de comprendre les affirmations sur le savoir, en tant qu'entreprise, soulignent davantage la perception à la hausse du savoir en tant que produit. Selon Polanyi, « l'autorité de l'opinion scientifique » est « essentiellement mutuelle », « établie parmi les scientifiques, pas au-dessus d'eux ». (Polanyi 1969, 56) Par conséquent, l'autorité des demandes de connaissances peut être qualifiée d'ascendante, selon l'opinion de Polanyi. Cette perspective est liée à la discipline de l'analyse du renseignement, offrant une manière alternative de considérer un large éventail de problèmes épistémologiques, principalement en relation avec ce que signifie « savoir » quelque chose ». (Ormerod 2018a, 103)

5. Méthodologies

La méthodologie, dans le renseignement, comprend les méthodes utilisées pour prendre des décisions sur les menaces, en particulier dans la discipline de l'analyse du renseignement.

L'énorme volume d'informations collectées par les agences de renseignement les met souvent dans l'incapacité de les analyser toutes. Selon McConnell, la communauté du renseignement américaine recueille plus d'un milliard d'informations par jour. (McConnell 2007) La nature et les caractéristiques des informations collectées ainsi que leur crédibilité ont également un impact sur l'analyse du renseignement.

Le paramètre de *capacité* est essentiel pour la compréhension actuelle de la menace. (Vandepeer 2011) Les analystes utilisent deux approches pour évaluer la capacité: utiliser des mesures indirectes et des mesures proxy. Une mesure permet une évaluation directe de la capacité. Les mesures indirectes sont des mesures indirectes utilisées pour effectuer des déductions de capacité.

Dans le cas de l'*évaluation* des forces militaires et armées d'un pays, en plus des mesures de capacité, il existe cinq mesures directes pour évaluer la capacité militaire: leadership et C2 (commandement et contrôle); l'ordre de combat; entraînement musculaire et mission; la durabilité de la force; et la sophistication technique, (Joint Publication 2-01 2012) ainsi que des mesures indirectes (appelées sujets militaires), notamment: les systèmes C4 (télécommunications et réseaux); industries de défense d'État; énergie / puissance; la géographie; la démographie; et la capacité médicale. Les capacités des États ne pouvaient être connues que lorsqu'elles étaient effectivement utilisées contre un adversaire.

La nature même d'une intention signifie qu'elle n'est pas « mesurable » en tant que capacité. Il est estimé ou déduit de facteurs observables, appelés indicateurs (facteurs observables utilisés

pour déduire ou observer les intentions actuelles ou futures). Les indicateurs fournissent un moyen de déduire plutôt que de quantifier.

Trois *indicateurs* apparaissent de manière significative dans l'évaluation des intentions de l'État : la capacité militaire de l'État ; l'idéologie de l'État ; et les mots, les actions et les comportements des chefs d'État. Par conséquent, les évaluations de la capacité militaire ne sont pas suffisantes pour déduire les intentions d'un État. L'idéologie d'un État est le reflet du leadership politique, troisième indicateur des intentions.

Les analystes du renseignement sont « essentiellement des traducteurs d'informations, dont le rôle est d'examiner les informations et de fournir des informations fiables dans un format pratique et opérationnel ». (Cope 2004, 188) Le modèle national d'information du Royaume-Uni décrit quatre produits clés que les analystes du renseignement créent à la suite du processus d'analyse: évaluations stratégiques, évaluations tactiques, profils cibles et profils de problèmes. (Association of Chief Police Officers, Bedford 2005) L'évaluation du renseignement implique leur crédibilité, ainsi qu'une évaluation de la fiabilité des sources. (Palmer 1991, 22) Il existe peu de systèmes officiels d'évaluation du renseignement utilisées par les analystes dans le monde. La plus connue de ces méthodes est le Système de l'amirauté (également appelé Système OTAN), qui est utilisé pour démontrer la valeur nette de certaines informations en fonction de la fiabilité de la source et de la validité des données. (Besombes, Nimier, et Cholvy 2009) Le modèle traditionnel est une matrice 6 x 6. Les agences opérant dans le cadre du Modèle national du renseignement au Royaume-Uni utilisent un système de classification alternatif communément appelé système 5x5x5.

La *théorie prismatique* de Robert Flood, qualifiée par d'autres de pluralisme méthodologique, utilise la métaphore pour décrire la pensée créative et transformatrice, à savoir

un prisme qui décompose la lumière dans ses couleurs composantes par double réfraction. Ce type de pensée produit plusieurs points de vue différents sur la même chose et une vision commune pour plusieurs choses différentes. Son objectif est de remettre en cause des hypothèses, de provoquer de nouvelles idées et de générer des perspectives inattendues. (Flood 1999)

Le concept de pensée prismatique a gagné du terrain dans l'analyse du renseignement. (Duvenage 2010a) Jones déclare qu'en plus de la pensée convergente, nous avons également besoin d'une pensée divergente pour assurer une analyse et une résolution des problèmes efficaces. (M. D. Jones 2009) La divergence aide les analystes à analyser un problème plus créatif, tandis que la convergence aide à parvenir à son terme.

Wolfberg propose une mentalité à spectre complet, dans laquelle l'analyste applique à la fois des méthodes intuitives et structurelles, selon le contexte spécifique, en supposant dès le départ qu'il existe de multiples problèmes interdépendants qui doivent être résolus simultanément. (Wolfberg 2006)

Waltz a conçu le processus intégré de raisonnement, dans lequel il a intégré les méthodes formelles et informelles de raisonnement pour l'analyse-synthèse dans l'environnement opérationnel du renseignement. (Waltz 2003) Le procès découle d'un ensemble de preuves et d'une question à leur intention qui explique les preuves. Ce processus, d'un ensemble d'enregistrements à la détection, aux explications ou aux découvertes, détecte la présence de preuves, explique les processus qui étaient à la base des preuves et découvre de nouveaux modèles à partir des preuves. Le modèle illustre quatre façons fondamentales d'utiliser l'ensemble de preuves: trois modes de raisonnement fondamentaux et un quatrième chemin de rétroaction: déduction (en testant sur des modèles / hypothèses connus précédemment), rétroduction (lorsque l'analyste conjecture (synthétise) une nouvelle hypothèse conceptuelle qui provoque un retour à l'ensemble de preuves),

l'abduction (crée des hypothèses explicatives inspirées de l'ensemble de preuves), l'induction (recherche d'énoncés généraux (hypothèses) sur les preuves).

Waltz caractérise le processus d'analyse-synthèse comme un processus de décomposition des preuves et de construction du modèle, aidant l'analyste à identifier les informations manquantes, les forces et les faiblesses du modèle. Le modèle remplit deux fonctions : hypothèse (si les preuves sont limitées) et explicative (lorsque davantage de preuves correspondent à l'hypothèse). Le processus implique trois espaces de phase définis par l'utilisation du terme « espace » et l'utilisation de techniques analytiques structurelles : espace de données (les données sont indexées et triées), espace d'arguments (les données sont examinées, corrélées et regroupées dans un ensemble d'hypothèses) et phase explicatif (les modèles sont composés pour servir d'explications).

Le flux du processus cognitif est identifié comme suit : il cherche et filtre, lit et extrait, schématise, construit le cas, raconte l'histoire, réévalue, cherche du soutien, cherche des preuves, cherche des relations, cherche des informations.

Un modèle analytique rigoureux pouvant aider les analystes a été développé par Zelik, Patterson et Woods en 2007. Ce modèle améliore la technique d'autocritique structurelle de Heuer et Pherson. Ce modèle comporte huit indicateurs de rigueur : exploration d'hypothèses, recherche d'informations, validation d'informations, analyse de perspective, analyse de sensibilité, collaboration de spécialistes, synthèse d'informations, critique explicative. Ce modèle explique les processus cognitifs, fournit la première métrique pour tester les produits informationnels et fournit un cadre pour l'apprentissage collaboratif.

La signification, un concept dérivé de la théorie cognitive et surtout organisationnelle, (Weick 1995) est utilisée dans la connaissance pour étudier et décrire comment l'individu, le

groupe et, plus précisément, l'organisation, font face aux incertitudes et s'adaptent à la complexité. Au niveau individuel, le sens implique la capacité de percevoir, d'analyser, de représenter, de visualiser et de comprendre l'environnement et la situation de manière contextuelle appropriée. (Cooper et Intelligence 2012) Cet aspect est connu dans l'analyse du renseignement sous le nom de conscience de la situation ou analyse de l'environnement. La pertinence de la signification dans l'analyse du renseignement devient claire lorsque l'on applique sept propriétés de la signification de Weick à la psychologie de l'analyse du renseignement de Heuer : contexte social, construction fondée sur l'identité, rétrospectivement, plutôt que conduite fondée sur l'exactitude, en cours, extraction de points de repère importants, mise en scène.

Fishbein et Treverton citent Klein, Stewart et Claxton, qui affirment que la recherche empirique a montré que le jugement intuitif sous-tend la plupart des décisions organisationnelles et est supérieur à l'analyse des questions marquées par l'ambiguïté ou l'incertitude. (Shulsky et Schmitt 2002)

Robert M. Clark a proposé une méthodologie pour analyser l'information en abordant le cycle d'information axé sur les cibles, comme alternative au cycle d'information traditionnel. (Clark 2003) Il a ainsi redéfini le processus d'information sous la forme d'un réseau intégré, dans lequel l'information peut circuler directement entre les différentes étapes du cycle (en pratique, il n'y a plus de cycle au sens traditionnel du terme).

Sherman Kent a encouragé les arguments et les dissensions parmi les analystes du renseignement à parvenir à un « large éventail d'opinions externes », (Davis 1995) en encourageant la « responsabilité collective de l'analyse » en mettant en réseau le renseignement avec des boucles de rétroaction entre les analystes et les différentes étapes du cycle du renseignement.

Les modèles conceptuels permettent aux analystes d'utiliser des outils descriptifs puissants pour estimer les situations actuelles et prévoir les circonstances futures. (Clark 2003, 37) Après avoir esquissé le modèle, l'analyste remplit le modèle en recherchant, en rassemblant des informations et en synthétisant. Il doit trouver des informations auprès d'un large éventail de sources classées et non classifiées, selon les cibles.

Les données collectées doivent être rassemblées, organisées et les preuves évaluées pour leur pertinence et leur crédibilité. Après avoir examiné les données, l'analyste inclut les informations dans le modèle cible, ce qui permet de déterminer où il y a des incohérences dans les résultats grâce à des recherches supplémentaires pour soutenir ou infirmer une certaine conclusion. Le modèle cible montre où il y a des lacunes dans le modèle. Tout écart oblige l'analyste à collecter des informations supplémentaires pour mieux décrire l'objectif.

Le modèle organisationnel de Robert M. Clark aide les analystes à décrire avec succès l'organisation cible et à voir les forces et les faiblesses de la cible, pour une analyse prédictive et fiable. (Clark 2003, 227)

Le général Stanley A. McChrystal a proposé en 2014 un cycle de ciblage appelé « *F3EA* » utilisé dans la guerre en Irak, ce qui signifie :

1. *Constatation* : une cible (personne ou lieu) est identifiée et localisée.
2. *Fixation* : la cible est ensuite surveillée en continu tout en établissant une identification positive.
3. *Finalisation* : une force d'attaque est assignée pour capturer ou tuer la cible.
4. *Exploitation* : Le matériel d'information est sécurisé et exploité, les détenus étant interrogés.

5. *Analyse* : les informations sont étudiées pour identifier des opportunités de ciblage supplémentaires. (McChrystal 2014)

Richards Heuer déclare qu'aucune méthode ne garantit le succès des conclusions. Les analystes doivent continuellement l'affiner, en fonction de leur contexte spécifique et de leurs expériences personnelles antérieures. (Heuer 1999a) De plus, à l'approche d'un cycle de réseau, il faut tenir compte du fait que ces modèles consomment beaucoup plus de temps qu'un cycle traditionnel. (Johnston 2005)

Les *techniques analytiques structurelles* sont utilisées pour provoquer le jugement, lors de l'identification des mentalités, du dépassement des préjugés, de la stimulation de la créativité et de la gestion de l'incertitude. Les exemples incluent la vérification des principales hypothèses, l'analyse des hypothèses concurrentes, l'avocat du diable, l'analyse de l'équipe rouge et l'analyse des scénarios / futurs alternatifs, entre autres. (US Government 2009) Les méthodes suivantes sont des moyens de valider les résultats du raisonnement de l'analyste:

Analyse d'opportunité : identifie, pour les décideurs, les opportunités ou vulnérabilités que leur organisation peut exploiter.

Analyse des clous de sécurité : résulte d'informations fiables ou très susceptibles d'être fiables. (Davis 1999)

Analyse des hypothèses concurrentes : plus de défis, selon Heuer, sont plus importants que plus d'informations, surtout pour éviter le rejet de la tromperie à portée de main, car la situation semble simple. L'analyse des hypothèses concurrentes a représenté un pas en avant dans la méthodologie de l'analyse de l'information. Les étapes de l'analyse des hypothèses concurrentes sont : (Heuer 1999a)

1. Identifier les *hypothèses* possibles à considérer. Utilisez un groupe d'analystes avec des perspectives différentes pour comprendre les possibilités.
2. Faites une liste des *preuves* et arguments significatifs pour et contre chaque hypothèse.
3. Préparez une *matrice* avec des hypothèses en haut et des preuves en bas. Analyser le « diagnostic » des preuves et des arguments - c'est-à-dire identifier les éléments les plus utiles pour évaluer la probabilité relative des hypothèses.
4. *Affinez* la matrice. Passez en revue les hypothèses et supprimez toutes les preuves et arguments non diagnostiques.
5. Tirer des *conclusions provisoires* sur la probabilité relative et l'incohérence de chaque hypothèse. Essayez de rejeter les hypothèses plutôt que de les prouver. (La réfutabilité ?)
6. Analysez la *sensibilité* de votre conclusion à quelques éléments de preuve essentiels. Considérez les conséquences pour votre analyse si ces preuves étaient fausses, trompeuses ou mal interprétées.
7. Rapportez les *conclusions*. Discutez de la probabilité relative de toutes les hypothèses, pas seulement les plus probables.
8. Identifier des *repères* pour une observation future qui peuvent indiquer que les événements ont un cours différent de celui attendu.

L'analyse des hypothèses concurrentes est auditable et aide à surmonter les biais cognitifs. Il permet de revenir sur les preuves et les hypothèses, et donc de suivre la succession des règles et des données qui ont conduit à la conclusion.

Van Gelder a proposé la *cartographie des hypothèses* comme alternative à l'analyse des hypothèses concurrentes. (van Gelder 2012)

L'*analyse structurelle* des hypothèses concurrentes offre aux analystes une amélioration par rapport aux limites d'origine, (Wheaton et Chido 2007) maximisant les hypothèses possibles et permettant à l'analyste de diviser une hypothèse en deux hypothèses complexes.

Une méthode de Valtorta et ses collègues utilise des *méthodes probabilistes*, ajoutant l'analyse bayésienne à l'analyse des hypothèses concurrentes. (Goradia, Huang, et Huhns 2005) Une généralisation de ce concept a conduit au développement de CACHE (Collaborative ACH Environment), (Shrager et al. 2010) qui a introduit le concept de communauté bayésienne. Le travail d'Akram et Wang applique des paradigmes de la théorie des graphes. (Shaikh Muhammad et Jiaxin 2006)

Les travaux de Pope et Jøsang utilisent la *logique subjective*, une méthodologie mathématique formelle qui traite explicitement l'incertitude, (Pope et Jøsang 2005) qui forme la base de la technologie Sheba utilisée dans les logiciels d'évaluation du renseignement.

Analogie : Habituellement dans l'analyse technique, mais les caractéristiques d'ingénierie qui se ressemblent ne signifient pas nécessairement qu'elles ont toutes les deux le même mode de fonctionnement simplement parce qu'elles sont similaires.

Dans le processus d'analyse du renseignement, les analystes doivent suivre une série d'étapes séquentielles :

1. *Définissez le problème* : les analystes doivent essayer de comprendre à la fois la pensée de l'adversaire et celle de leurs clients et alliés.
2. *Génération d'hypothèses :* basée sur des questions.
3. *Déterminer les besoins d'information et collecter des informations* : l'analyste peut demander une collecte spécifique sur le sujet ou, si cela n'est pas possible, identifier cette lacune dans le produit final

4. *Évaluation des sources* : l'analyste doit évaluer la fiabilité, la crédibilité et l'éventuelle falsification ou tromperie des informations.
5. *Évaluation des hypothèses (tests)* : tests par des méthodes telles que l'analyse des hypothèses concurrentes ou de diagrammes de liens, en prêtant attention aux biais cognitifs et culturels à l'intérieur et à l'extérieur de l'organisation.
6. *Production et emballage* : sous une forme écrite et orale très bien écrite, y compris des messages électriques, des rapports imprimés, des informations ou des vidéos ; trois caractéristiques sont essentielles pour le produit d'information : la rapidité, la portée et la régularité.
7. *Évaluation collégiale* : essentielle pour l'évaluation et la confirmation de l'exactitude.
8. *Retour d'information et évaluation du produit* : après la livraison, le processus se poursuit avec l'interaction entre le producteur et le client, grâce à un retour d'information mutuel, sur la base duquel l'analyse et les exigences sont affinées.

Une analyse efficace du renseignement doit, en fin de compte, être adaptée à l'utilisateur final, mais sans diminuer la qualité et la précision du produit. (M. L. Jones et Silberzahn 2013)

6. Analogies avec d'autres disciplines

6.1. Science

L'analyse du renseignement présente de nombreuses similitudes épistémologiques importantes avec la science (résolution de problèmes, découverte, utilisation habile des outils, vérification des demandes de connaissances) et s'intéresse davantage aux connaissances *a posteriori* qu'aux *a priori* (Agrell et Treverton 2015) sur la manière ou la base sur laquelle une proposition peut être connue. (Greco et Sosa 1999, 243–70) Tant l'analyse du renseignement que la science se concentrent sur les connaissances acquises à partir d'observations empiriques,

connaissances qui sont typiquement *a posteriori*. (Ormerod 2018b) En matière d'analyse du renseignement, des considérations épistémologiques sont parfois implicitement prises en compte dans la gestion des biais et des incertitudes au sein de systèmes de renseignement complexes. (M. D. Smith 2017)

Stephen Marrin et Jonathan D. Clemente notent que le renseignement est « sujette à une erreur aléatoire et systématique résultant des limitations intégrées des outils de collecte eux-mêmes et, par conséquent, le renseignement qui alimente l'analyse n'est jamais une représentation exacte de la réalité ». (Marrin 2012b) Pour comparer les méthodes utilisées dans le renseignement avec les méthodes scientifiques, trois critères pivots épistémiques peuvent être utilisés : la taille de l'échantillon, le point d'observation et l'intégrité des données. (Pritchard et Goodman 2009)

Les méthodes scientifiques impliquent la collecte d'énormes quantités d'informations pour obtenir des résultats significatifs. Les petits ensembles de données sont généralement rejetés en raison de l'incertitude statistique. Dans l'activité du renseignement, la taille des échantillons pertinents est extrêmement petite, souvent seulement quelques sources distinctes. D'énormes volumes de données sont collectés, mais la sélection des informations pertinentes est un processus difficile.

En science, les chercheurs conservent généralement les données originales, qui sont directement examinées, garantissant ainsi un haut degré de fiabilité et de certitude. Dans le domaine de l'information, les données et les renseignements parviennent rarement aux analystes de première main. Même l'identité de certaines personnes peut être incertaine.

En science, les chercheurs sont attentifs à leurs propres biais, mais en général, les données ne sont pas consciemment affectées. Dans le monde des services de renseignement, la situation est très différente : les données et les renseignements sont manipulées délibérément et à grande

échelle, dans le but de fausser la réalité. Parfois, même les membres d'une même organisation incluse dans le cycle d'information ont des raisons de déformer les données ou même d'introduire de fausses données, souvent pour de l'argent ou d'autres avantages.

À la suite des attentats du 11 septembre aux États-Unis, des efforts ont été faits pour « le scientifiquement » des méthodes utilisées dans le renseignement. (Marrin et Torres 2017) Certains des plus anciens articles dans le domaine, y compris celui de Sherman Kent, ont soutenu des méthodes scientifiques non seulement pour comprendre certaines questions, mais aussi pour effectuer des évaluations vérifiables. (Agrell 2012, 130) R. A. Random a écrit en 1958 que rejeter la méthodologie scientifique en faveur de l'intuition reviendrait à renoncer à la rationalité au profit de la « devinette » D'autres chercheurs dans le domaine du renseignement soutiennent que la méthode scientifique est fondamentale pour l'analyse du renseignement. (Marrin 2012c, 531)

Les caractéristiques d'une telle « méthode scientifique » sont les suivantes : collecte de données, formation d'hypothèses, tests d'hypothèses et conclusions pouvant être utilisées comme sources prédictives fiables. (Platt 1957, 75)

Cette analogie est généralement considérée comme correcte dans la mesure où le processus est « systématique » et « logique » : (Ylikoski 2017) « En tant que science, l'analyse du renseignement est un processus systématique qui génère et teste objectivement des hypothèses. En suivant la méthode scientifique, les analystes adhérer aux règles pour développer des jugements solides et logiques. » (Martin 2011, 30)

Les activités scientifiques et le renseignement se réfèrent à la fois à la « vérification » et à la « falsification » des énoncés de connaissances. (Shrager et al. 2010) Des efforts dans le domaine de l'activité d'information pour aligner l'analyse avec les objectifs de la science, en particulier avec la « contrefaçon », ont été encouragés par plusieurs scientifiques. (Shaikh Muhammad et Jiaxin

2006) Comme l'explique Polanyi, centraliser la compréhension dans la science de la connaissance est une reconnaissance suffisante de la connaissance personnelle, en partie parce qu'il n'y a pas de « règles » dans le domaine de la science. (Ormerod 2018b) Pour cette raison, le scientifique, selon Polanyi, doit s'appuyer sur ses connaissances personnelles pour décider, par exemple, si les preuves ou les indices doivent être acceptées ou rejetées, en tant qu'analyste du renseignement. Les arguments présentés par Polanyi influencent à la fois le domaine de la sécurité nationale et les domaines de l'application des lois à partir de l'analyse du renseignement, car ces domaines utilisent des observations empiriques pour développer et comprendre les revendications de connaissances. (Peters et Cohen 2017) Dans le domaine de la sécurité nationale, la centralité de l'empirisme peut être observée en ce qui concerne l'existence de grands systèmes de collecte d'informations. Polanyi conteste la base épistémologique d'une croyance excessive contre le rôle central supposé de l'empirisme et la logique de l'induction dans la science : « Le rôle joué par les nouvelles observations et expériences dans le processus de découverte en science est généralement surestimé », (Polanyi 1964, 29) une opinion opposée à la compréhension conventionnelle de la science promue par Karl Popper. (Popper 1972, 23-27)

6.2. Archéologie

La métaphore du puzzle est utilisée à la fois dans le renseignement et l'archéologie. Les deux disciplines impliquent la collecte de preuves pour construire une image aussi complète que possible. (Pritchard et Goodman 2009) Certaines pièces ne sont pas vues depuis le début et d'autres sont déformées et ne peuvent pas contribuer à la logique de l'assemblage. Il serait peut-être utile de se tourner vers la rétro-ingénierie pour comprendre comment l'image originale a été divisée, quelles sont les étapes et ce qui est arrivé aux parties manquantes.

David Clarke a souligné une théorie de l'archéologie basée sur la relation entre la culture ancienne connue et les restes découverts par l'excavatrice, un puzzle terminé et les pièces manquantes et doivent être analysés.

Les étapes nécessaires à toute interprétation archéologique sont :

1. La gamme des modèles d'activité et des processus sociaux et environnementaux qui existaient autrefois, c'est ce que l'archéologue essaie de comprendre.
2. L'échantillon et les restes qui ont été déposés à ce moment-là.
3. L'échantillon de cet échantillon qui a survécu et doit être récupéré.
4. L'échantillon de l'échantillon réellement récupéré. (Clarke 1968)

L'archéologue peut utiliser l'intuition pour l'interprétation, mais cela peut facilement échouer. L'analyste du renseignement, à son tour, essaie de comprendre le problème en utilisant ce qui est disponible, c'est-à-dire une partie de l'échantillon.

Les étapes proposées par David Clarke sont :

1. La gamme de modèles d'activité et de processus sociaux et environnementaux qui existaient autrefois (respectivement, l'activité totale pertinente pour demander au service de renseignement)
2. L'échantillon et les restes qui ont été déposés à ce moment-là (les analystes du renseignement tentent de savoir quels éléments de l'activité de leur adversaire deviennent des renseignements, ce qui doit être collecté et à partir de quelles sources)
3. L'échantillon de cet échantillon qui a survécu pour être récupéré (fragments d'informations détenues par certaines sources, compte tenu de leur éventuelle distorsion)
4. L'échantillon de l'échantillon qui est réellement récupéré (informations collectées via différents systèmes et sources de collecte, d'une importance capitale)

Après avoir identifié l'exactitude de l'activité de renseignement pour chacune des étapes, les types de théorie applicables peuvent être considérés :

Théorie des hypothèses et des dépositions : Le lien entre 1 et 2. Déterminer la relation entre l'activité totale divisée et l'échantillon potentiellement accessible aux systèmes de collecte. Quelles sources utiliser ? Quels sont les préjugés ?

Théorie post-dépositaire : Le lien entre 2 et 3. Dans quelle mesure le passage du temps peut-il déformer l'échantillon ?

Théorie de la restauration : Le lien entre 3 et 4. Dans quelle mesure les données collectées représentent-elles tout ce qui est possible ? Quelle quantité de matériel a été collectée et quelle nature ? Quelles activités similaires pourraient avoir lieu dans d'autres parties où l'accès est facile ?

Théorie analytique : Le lien entre 4 et 1. Le collecteur d'informations doit sélectionner les informations pertinentes, en fonction de la compréhension de l'analyste des besoins en renseignement. Dans le même temps, des contraintes (technologiques ou autres) peuvent limiter la capacité du collecteur à transmettre des données de certains types pour une analyse plus approfondie. Dans ce cas, certaines décisions de priorisation peuvent être établies en abandonnant certaines informations.

Théorie de l'interprétation : L'analyste propose ses évaluations aux décideurs. Ici, les biais cognitifs apparaissent et des méthodes sont utilisées pour les contracter en interrogeant les hypothèses et en générant des hypothèses alternatives.

L'analogie archéologique est loin d'être parfaite. Mais il illustre les étapes par lesquelles une image est démontée en fragments pour analyse. Les analystes doivent être conscients que leurs

données sont incomplètes, mais la nature de cette incomplétude peut ne pas être entièrement comprise, ce qui entraîne de graves implications. (Pritchard et Goodman 2009)

6.3. Affaires

Le renseignement est traditionnellement caractéristique aux organisations gouvernementales impliquées dans les questions de sécurité nationale. Mais les entreprises privées innovantes adaptent de plus en plus le modèle des services de renseignement au monde des affaires pour aider à planifier leurs propres stratégies. Le processus de transformation des informations brutes en informations traitées exploitables est presque identique pour les organisations gouvernementales ainsi que pour les entreprises, ces dernières développant le système de collecte et d'analyse des informations en utilisant leurs propres méthodologies. (Krizan 1999b)

Les deux activités semblent être deux domaines indépendants, mais la façon d'aborder les défis est assez similaire, selon les capacités d'alerte ; (Miscik 2017) dans les deux cas, les décideurs s'attendent à connaître à l'avance les menaces et les opportunités. La recherche universitaire a montré qu'il est possible d'effectuer une analyse comparative des deux domaines (gouvernement et entreprise) et d'identifier les parallèles possibles entre eux. (Barnea 2018) Dans les deux domaines, le produit du renseignement est celui qui soutient le processus de prise de décision à la suite des informations sur les changements dans l'environnement externe déterminés par les menaces spécifiques. Mais l'étude ontologique, épistémologique et méthodologique de ce processus est beaucoup mieux développée de nos jours dans les affaires (Busenitz et Barney 1997) afin que les services nationaux de renseignement puissent reprendre bon nombre des théories et techniques développées dans le domaine de l'intelligence économique.

Une similitude fondamentale entre l'activité nationale de renseignement et l'intelligence économique est que les deux fonctionnent sur la base du « cycle du renseignement », (Omand

2011) un processus systématique en plusieurs étapes qui garantit la conduite des activités de renseignement sous contrôle.

L'intelligence économique (IE) est un domaine dont l'activité consiste à définir, collecter, analyser et diffuser des informations sur les produits, les clients, les concurrents et tout aspect de l'environnement nécessaires pour soutenir les managers dans le processus de prise de décision stratégique d'une organisation. Il s'agit d'une pratique commerciale légale, par opposition à l'espionnage industriel, qui est illégal. (SCIP 2014) L'IE se concentre sur l'environnement commercial externe, (Haag 2012) étant un processus impliqué dans la collecte d'informations, leur transformation en informations traitées, puis leur utilisation dans la prise de décision. (McGonagle et Vella 2003)

IE est souvent considéré comme synonyme d'analyse des concurrents, mais est plus que l'analyse des concurrents ; il couvre l'ensemble de l'environnement et des parties prenantes : clients, concurrents, distributeurs, technologies et données macroéconomiques. Les organisations utilisent IE pour comparer avec d'autres organisations (« comparaison concurrentielle »), pour identifier les risques et les opportunités sur leurs marchés, et pour tester leurs plans de réaction du marché (« business wargame »). (Kurtz 2018)

L'*information stratégique* se concentre sur les problèmes à long terme, en analysant les problèmes qui affectent la compétitivité d'une entreprise sur plusieurs années. L'horizon en temps réel de l'information stratégique dépend en fin de compte de l'industrie et de la rapidité avec laquelle elle change. Ce type d'activité d'information implique, entre autres, l'identification de signaux faibles et l'application d'une méthodologie et d'un processus spécifiques, initialement développés par Gilad. (Gilad 2014)

Dans l'information tactique, l'accent est mis sur la fourniture d'informations conçues pour améliorer les décisions à court terme, le plus souvent liées à l'intention d'augmenter la part de marché ou les revenus.

Les avancées techniques du traitement parallèle massif offert par l'architecture « big data » ont permis la création de plusieurs plateformes de reconnaissance des entités cibles. (Krapohl 2013)

L'IE a été influencé par l'information stratégique nationale. Fleisher suggère que les informations commerciales se présentent sous deux formes. Sa forme (contemporaine) plus étroite se concentre davantage sur les technologies de l'information et l'accent interne que sur IE, tandis que la définition (historique) plus large est plus complète que IE. La gestion des connaissances, lorsqu'elle est effectuée spécifiquement, est considérée comme une pratique organisationnelle basée sur la technologie de l'information qui utilise l'exploration de données, l'intranet d'entreprise et la cartographie des actifs organisationnels pour les rendre accessibles aux membres de l'organisation pour la prise de décision. IE partage certains aspects avec la gestion des connaissances ; contient des informations humaines et basées sur l'expérience pour une analyse qualitative plus sophistiquée. La gestion des connaissances est essentielle pour un changement efficace. Un facteur clé efficace est un système informatique puissant, dédié à l'exécution de l'ensemble du cycle de l'information. (Barnea 2009)

L'informatique décisionnelle (ID), appelée « business intelligence », est « un ensemble de techniques et d'outils pour transformer des données brutes en informations significatives et utiles à des fins d'analyse commerciale ». (Evelson 2008) Les *technologies* de l'ID peuvent manipuler de grandes quantités de données non structurées pour aider à identifier, développer et créer de nouvelles opportunités commerciales stratégiques. Le *but* de l'ID est de permettre une

interprétation facile de ces grands volumes de données. (Sfetcu 2016) Les technologies d'ID offrent des perspectives historiques, actuelles et prédictives des opérations commerciales. Les *fonctions* communes des technologies de l'ID sont les rapports, le traitement analytique en ligne, la recherche analytique, l'exploration de données, l'extraction de processus, le traitement d'événements complexes, la gestion des performances commerciales, la comparaison (analyse comparative), la fouille de textes, l'analyse prédictive et l'analyse normative.

L'ID peut être utilisée pour prendre en charge un large éventail de décisions commerciales, des opérations aux stratégies. Lorsqu'elles sont combinées, les données internes et externes peuvent fournir une image plus complète qui crée réellement des « renseignements » qui ne peuvent pas être déduites d'un seul ensemble de données. (Feldman et Himmelstein 2013)

Souvent, les scénarios d'ID tournent autour de processus métier distincts, chacun reposant sur une ou plusieurs sources de données. Ces étapes essentielles de l'information décisionnelle comprennent, sans s'y limiter :

- Sources de données pour collecter les données nécessaires
- Transformer les données en renseignement et les présenter de manière appropriée
- Requête et analyse du renseignement.
- Action sur les renseignements collectée.

Une similitude notable entre le renseignement gouvernemental et les informations économique est l'objectif de maximiser le profit des renseignements pour le client. Les changements sont difficiles à surveiller, en raison de la difficulté d'évaluer l'importance des signaux et des bruits dans les prévisions, pour réduire l'incertitude. (Rafii et Kampas 2002) En outre, sur la base des renseignements, dans les deux cas, ils agissent de manière proactive et essaient d'obtenir des informations pouvant envoyer des alertes sur les changements pertinents et

leur signification. (Prescott 2012) Dans les deux domaines, les renseignements présentées aux décideurs peuvent souvent être un catalyseur d'actions futures et une nouvelle initiative pour en récolter les fruits.

6.4. Médecine

La pratique médicale consistant à diagnostiquer l'identification, la collecte, l'analyse et la diffusion est similaire à celle du renseignement. (Converse 2008, 1) Marrin et Clemente soutiennent que les deux disciplines appliquent des approches générales similaires pour obtenir des informations. (Marrin et Clemente 2005, 709) Pour mieux comprendre les données et les informations recueillies, l'analyste utilise des disciplines connexes, similaires aux médecins dans le diagnostic des patients.

Selon Owen Ormerod, une autre similitude se pose dans le cas des défis auxquels sont confrontés à la fois l'intégration du diagnostic ou des évaluations analytiques dans un contexte plus large, allant d'hypothèses alternatives à des preuves qui invalident, et en utilisant le raisonnement déductif et inductif pour distinguer les informations pertinentes de bruit. (Marrin et Clemente 2005, 715)

« La base de cette analogie perçue entre l'analyse du renseignement et la profession médicale est la conviction que, à mesure que davantage d'informations seront collectées, le praticien deviendra plus confiant dans son évaluation. » Mais ce n'est pas toujours le cas. Dans certaines circonstances de la profession médicale, le processus de diagnostic implique des considérations qui ne sont pas « scientifiques » ou structurées de manière caractéristique, mais qui relèvent de la partisanerie du médecin, des compétences artisanales et de ce que Polanyi appellerait « connaissances personnelles ». Le poststructuraliste Michael Foucault a présenté un argument similaire selon lequel le travail du médecin est influencé par la culture environnante, dans la

mesure où il ne « découvre » pas la vérité « là » mais l'assemble plutôt dans l'esprit, qui est en partie le produit de son environnement. Il est trop simpliste de comprendre l'activité du médecin ou de l'analyste du renseignement en tant qu'observateurs neutres qui ne recueillent et n'analysent que des « faits ». (Ormerod 2018b, 28)

Certains experts du renseignement ont fait valoir que l'analyse du renseignement peut bénéficier de l'adoption de modèles similaires à ceux diagnostiqués dans le domaine médical. (Manjikian 2013, 1) Richards Heuer a souligné le domaine médical comme une profession qui pourrait être imitée par le renseignement. Comme il le dit, le médecin observe les symptômes du patient et en utilisant ses connaissances spécialisées sur le corps, une hypothèse est générée pour expliquer ces observations, suivie de tests pour recueillir des informations supplémentaires pour évaluer l'hypothèse et appliquer un diagnostic. Cette analogie médicale met l'accent sur la capacité d'identifier et d'évaluer correctement toutes les hypothèses plausibles. En ce sens, la collection se concentre sur des informations qui pourraient révéler des hypothèses alternatives : « Bien que l'analyse et la collecte soient toutes deux importantes, l'analogie médicale attache plus de valeur à l'analyse et moins à la collecte que les métaphores de la mosaïque. » (Heuer 1999b, 62)

7. Conclusions

Il n'y a pas de consensus universel sur la façon de mieux comprendre l'analyse du renseignement. Il existe, en particulier, des lacunes dans la littérature sur les dimensions épistémologiques de l'analyse du renseignement, tant en termes de processus d'analyse que de produits ou de « connaissance ». Le point de vue de Polanyi sur la façon dont les scientifiques participent à la résolution de problèmes aidera à comprendre le processus épistémologique et le produit d'analyse du renseignement. Il a souligné que la « connaissance pratique » des scientifiques sur la compréhension des phénomènes est une illustration de la fonction instrumentale de la

connaissance tacite. (Ormerod 2018b) La relation entre les connaissances tacites et explicites est la clé pour comprendre la valeur du traitement de ce concept de Polanyi. Il a fait valoir qu'il existe un lien étroit entre la connaissance tacite et la connaissance personnelle, concluant que la logique de la perception (obtenue en partie grâce au connaissance tacite) est la même que la logique de la découverte et donc de la connaissance produite - la connaissance personnelle. Le langage nuancé de Polanyi pour couvrir la sensibilisation à la perception donne au renseignement un nouveau contexte pour analyser un certain nombre de questions conceptuelles et pratiques dans un sens épistémologique. Ces idées, appliquées aux considérations épistémologiques rencontrées par l'analyste du renseignement dans le processus d'analyse et l'utilisation de techniques analytiques structurelles, enrichiront le langage et la logique pour comprendre ces questions. La théorie de la connaissance personnelle de Polanyi apporte de nouveaux arguments concernant l'analyse du renseignement en tant que produit

Selon Owen Ormerod, l'analyse du renseignement peut être caractérisée comme une entreprise épistémologique, qui vise à développer une compréhension claire des produits de la connaissance. La perspective de Polanyi sur la connaissance sert à quelques considérations épistémologiques fondamentales concernant la connaissance en tant que produit. Ce concept de connaissance personnelle contribue à une compréhension plus profonde de la connaissance en tant que produit dans la discipline de l'analyse du renseignement. La perspective inverse la hiérarchie épistémologique traditionnelle, qui apprécie généralement la connaissance propositionnelle sur les manières plus que « tacite » ou « personnelle » de comprendre les énoncés de la connaissance. Cette position épistémologique contribue à la discipline de renseignement en fournissant une image plus solide de la dimension personnelle de la connaissance en tant que produit. Les approches de ce que signifie « savoir » quelque chose offre à l'analyse du renseignement une

compréhension épistémologique nuancée et détaillée de la dimension personnelle de la connaissance et de la connaissance en tant que produit.

Il s'agit d'une manière nuancée de comprendre de manière plus globale, d'un point de vue épistémologique, le processus de résolution des problèmes au sein du processus d'analyse du renseignement. Une reconnaissance suffisante du primat de la connaissance tacite est fondamentale pour mieux apprécier le processus de résolution de problèmes dans l'analyse du renseignement. Ainsi, une explication épistémologique robuste du processus de résolution de problèmes est fournie, qui sert à articuler l'aspect général connu de la « connaissance » dans le renseignement. Très important, ce cadre de compréhension du processus d'une pratique qualifiée, impliquant la connaissance tacite du praticien, souligne la centralisation de ces problèmes épistémologiques rencontrés par l'analyste du renseignement et prolonge le discours dans ce domaine. (Ormerod 2018b)

Étant donné que l'activité de l'analyste du renseignement est parfois « désordonnée et contingente » (Dahl 2017) plutôt que « systématique » et « logique », il pourrait être possible de comprendre les activités des analystes comme une « entreprise artistique » impliquant les deux aspects de « l'art », ainsi que la science. (Bang 2017b)

Les analystes doivent être conscients de leurs cadres, des méthodes intuitives qu'ils utilisent et des autres méthodes plus structurelles disponibles pour ajouter de la valeur, en particulier lorsque l'interprétation individuelle est insuffisante. Les divers outils et techniques analytiques aideront les analystes et les décideurs à comprendre, à verbaliser et à communiquer leurs processus de réflexion. Les analystes devraient idéalement être formés à tous les différents outils et techniques afin de pouvoir appliquer l'outil le plus approprié, intuitif / non autorisé ou structuré, à un problème spécifique et à une étape du processus de renseignement. (Duvenage 2010b)

Le plus grand défi pourrait être de convaincre les analystes, leur management et leurs clients des avantages des méthodes analytiques structurelles. Une introduction graduelle et naturelle de ces méthodes dans le flux ordinaire des processus et produits d'information pourrait être plus efficace qu'un réalignement à grande échelle de la pensée. La création d'opportunités de formation et l'éducation des clients à demander des preuves de l'application des techniques pourraient contribuer à ce processus.

Cela impliquerait un engagement fort des services de renseignement, avec le potentiel de changer la nature dépassée de ceux qui restaient dépendants des méthodes traditionnelles. L '« espace » des renseignements s'est étendu des gouvernements aux ONG, aux institutions et sociétés transnationales, aux entreprises privées et aux groupes d'intérêt et aux pressions représentant diverses communautés, concepts et idéologies. Un avertissement rapide est devenu crucial. Le processus décisionnel est devenu dispersé et granulaire. La « démocratisation » actuelle des services de renseignement a un impact majeur sur la collecte et l'analyse du renseignement, et le processus décisionnel, rendant les services de renseignement plus transparents, de prendre en compte les débats publics de leurs actions et parfois les justifier publiquement.

En outre, les récentes attaques terroristes aux États-Unis, au Royaume-Uni, en Espagne, en France, etc., ont démontré la nécessité d'intégrer les facteurs, la collaboration entre toutes les organisations de renseignement pour obtenir une vue d'ensemble et pour empêcher efficacement et en temps opportun des actions ciblées contre la sécurité nationale, redéfinissant non seulement le nouveau paradigme de la menace, mais aussi la façon dont les organisations répondent et s'adaptent à ces nouveaux défis.

Les institutions chargées de l'application des lois et de renseignement dans les pays en développement disposent rarement de systèmes de renseignement adéquats, sous-estimant la

valeur des analystes. Quiggin présente une image intimidante (Quiggin 2007) indiquant que moins de 1% des budgets de renseignement des pays sont dépensés pour l'analyse, tandis que 99% sont dépensés pour la technologie, le secret, l'infrastructure et d'autres éléments. Tous les spécialistes conviennent que, dans la situation géopolitique actuelle, un partenariat synergique entre les organisations de renseignement, les analystes du renseignement et le milieu universitaire est obligatoire. Aux États-Unis, la tendance est d'offrir des programmes de licence, de maîtrise et de doctorat liés au renseignement.

Un domaine dont les services de renseignement peuvent bénéficier est la gestion des connaissances, impliquée dans un débat rigoureux sur les concepts, les théories et les approches des connaissances et leur utilisation. Les théoriciens de la gestion des connaissances tels que Firestone et McElroy suggèrent que les organisations de renseignement devraient tenir compte des avantages que cette discipline peut apporter au secteur du renseignement. (Firestone et McElroy 2003)

Des changements majeurs dans le plan d'analyse du renseignement au cours des dernières années aux États-Unis, en établissant des méthodes d'analyse alternatives et en facilitant la collaboration inter-organisationnelle grâce aux dernières technologies Web, y compris les réseaux sociaux, ont produit des résultats au-delà des attentes. Malheureusement, très peu de pays ont choisi cette voie abandonnant la commodité des stratégies traditionnelles. Le nouveau paradigme des services de renseignement nécessite des changements majeurs au niveau organisationnel et une formation des professionnels pour comprendre et adopter les nouveaux concepts et technologies.

Les services de renseignement ont commencé à comprendre progressivement la nécessité d'étudier d'autres disciplines, y compris les aspects commerciaux ou philosophiques (ontologiques, épistémologiques, méthodologiques) de leurs propres activités, pour voir comment ils peuvent

améliorer leurs compétences et en rencontrer de nouveaux défis. Un excellent exemple est la façon dont le FBI s'est réinventé après le 11 septembre 2001 à la suite d'une étude notable menée par trois chercheurs de Harvard sous la direction de Jan Rivkin. (Gulati, Raffaelli, et Rivkin 2016)

Bibliographie

Agrell, Wilhelm. 2012. « The Next 100 Years? Reflections on the Future of Intelligence ». *Intelligence and National Security* 27 (1): 118-32. https://doi.org/10.1080/02684527.2012.621601.

Agrell, Wilhelm, et Gregory F. Treverton. 2015. *National Intelligence and Science: Beyond the Great Divide in Analysis and Policy*. Oxford, New York: Oxford University Press.

Aladashvili, Besik. 2017. *Fearless: A Fascinating Story of Secret Medieval Spies*.

Anderson, Terence, David Schum, et William Twining. 2009. *Analysis of Evidence*. 2 edition. Cambridge; New York: Cambridge University Press.

Andrew, Christopher. 2018. *The Secret World: A History of Intelligence*. New Haven, CT: Yale University Press.

Aristotle. 1989. *Prior Analytics*. Hackett Publishing.

———. 1991. « The Metaphysics ». 1991. https://www.amazon.com/Metaphysics-Great-Books-Philosophy/dp/0879756713.

Arrow, Kenneth J. 1966. « Exposition of the Theory of Choice under Uncertainty ». *Synthese* 16 (3): 253-69. https://doi.org/10.1007/BF00485082.

Artner, Stephen, Richard S. Girven, et James Bruce. 2016. « Assessing the Value of Structured Analytic Techniques in the U.S. Intelligence Community ». Product Page. 2016. https://www.rand.org/pubs/research_reports/RR1408.html.

Association of Chief Police Officers, Bedford. 2005. « Guidance on the National Intelligence Model ». https://whereismydata.files.wordpress.com/2009/01/national-intelligence-model-20051.pdf.

Australia Department of Defence. 2002. « Future Warfighting Concept ». http://www.defence.gov.au/publications/fwc.pdf.

Australia Department of Defence, Canberra. 2009. « Defending Australia in the Asia Pacific Century: Force 2030 (2009 Defence White Paper) ». Text. 2009. https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1516/DefendAust/2009.

Bang, Martin. 2017a. « A Shared Epistemological View Within Military Intelligence Institutions ». *International Journal of Intelligence and CounterIntelligence* 30 (1): 102-16. https://doi.org/10.1080/08850607.2016.1177401.

———. 2017b. « A Shared Epistemological View Within Military Intelligence Institutions ». *International Journal of Intelligence and CounterIntelligence* 30 (1): 102-16. https://doi.org/10.1080/08850607.2016.1177401.

Barnea, Avner. 2009. « Intelligence Solutions Through the Use of Expert Tools_CIM_March_April_09 | International Politics | Israel ». Scribd. 2009. https://www.scribd.com/document/17752171/Intelligence-Solutions-Through-the-Use-of-Expert-Tools-CIM-March-April-09.

———. 2018. « Nationak Strategic Intelligence and Competitive Intelligence: How a Comparative View and Mutual Learning Can Help Each? » ResearchGate. 2018. https://www.researchgate.net/publication/323884850_Nationak_Strategic_Intelligence_and_Competitive_Intelligence_How_a_Comparative_View_and_Mutual_Learning_Can_Help_Each.

Berkowitz, Bruce. 2002. « Intelligence and the War on Terrorism ». ResearchGate. 2002. https://www.researchgate.net/publication/248543624_Intelligence_and_the_War_on_Terrorism.

Berkowitz, Bruce D., et Allan E. Goodman. 2000. *Best Truth: Intelligence in the Information Age*. Yale University Press.

Besombes, Jérôme, Vincent Nimier, et Laurence Cholvy. 2009. « Information Evaluation in Fusion Using Information Correlation ». ResearchGate. 2009. https://www.researchgate.net/publication/224577351_Information_evaluation_in_fusion_using_information_correlation.

Bittner, Thomas, et Barry Smith. 2003. « A Theory of Granular Partitions ». In *Foundations of Geographic Information Science*, édité par M. Duckham, M. F. Goodchild, et M. F. Worboys, 117–151. London: Taylor & Francis.

Boyd, John R. 1976. « Destruction and Creation ». http://www.goalsys.com/books/documents/DESTRUCTION_AND_CREATION.pdf.

Brei, William S. 1996. *Getting Intelligence Right: The Power of Logical Procedure*. Joint Military Intelligence College.

Busenitz, Lowell W., et Jay B. Barney. 1997. « Differences between entrepreneurs and managers in large organizations: Biases and heuristics in strategic decision-making ». *Journal of Business Venturing* 12 (1): 9-30. https://doi.org/10.1016/S0883-9026(96)00003-1.

Buzan, Barry, Ole Wæver, Ole Waever, et Jaap de Wilde. 1998. *Security: A New Framework for Analysis*. Lynne Rienner Publishers.

Cao, Longbing. 2010. « (PDF) Domain-Driven Data Mining: Challenges and Prospects ». ResearchGate. 2010. https://www.researchgate.net/publication/220073304_Domain-Driven_Data_Mining_Challenges_and_Prospects.

Chomsky, Noam. 1992. *Deterring Democracy*. Reissue edition. New York: Hill and Wang.

CIA.gov. 2009a. « Our Mission — Central Intelligence Agency ». 2009. https://www.cia.gov/offices-of-cia/clandestine-service/our-mission.html.

———. 2009b. « Who We Are — Central Intelligence Agency ». 2009. https://www.cia.gov/offices-of-cia/clandestine-service/who-we-are.html.

Clark, Robert M. 2003. *Intelligence Analysis: A Target-Centric Approach*. Washington, D.C: Cq Pr.

Clarke, David L. 1968. *Analytical Archaeology*. Methuen.

Clausewitz, Carl von. 1989. *On War*. Princeton University Press.

Codevilla, Angelo. 1992. *INFORMING STATECRAFT (INTELLIGENCE FOR A NEW CENTURY)*. Free Press.

Colapietro, Vincent. 2011. « Intellectual Passions, Heuristic Virtues, and Shared Practices: Charles Peirce and Michael Polanyi on Experimental Inquiry ». Tradition and Discovery: The Polanyi Society Periodical. 2011. https://doi.org/10.5840/traddisc2011/201238326.

Conrad, Sherri J. 1985. « Executive Order 12,333: Unleashing the CIA Violates the Leash Law ». https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=4410.

Converse, Ray. 2008. « Intelligence and Medicine: Parallel Cognitive Traps ». http://www.pherson.org/wp-content/uploads/2013/11/03.-Intelligence-and-Medicine-Parallel-Cognitive-Traps_FINAL.pdf.

Cooper, Jeffrey R., et Center for the Study of Intelligence. 2012. *Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis*. CreateSpace Independent Publishing Platform.

Cope, Nina. 2004. « 'Intelligence Led Policing or Policing Led Intelligence?' Integrating Volume Crime Analysis into Policing ». *The British Journal of Criminology* 44 (2): 188-203. https://doi.org/10.1093/bjc/44.2.188.

Cross, Mai'a K. Davis. 2015. « The Limits of Epistemic Communities: EU Security Agencies ». ResearchGate. 2015. https://www.researchgate.net/publication/270578352_The_Limits_of_Epistemic_Communities_EU_Security_Agencies.

Cunningham, Hamish. 2006. « Information Extraction, Automatic ». ResearchGate. 2006. https://www.researchgate.net/publication/228630298_Information_Extraction_Automatic.

Dahl, Erik J. 2017. « Getting beyond analysis by anecdote: improving intelligence analysis through the use of case studies ». *Intelligence and National Security* 32 (5): 563-78. https://doi.org/10.1080/02684527.2017.1310967.

Davis, Jack. 1995. « A Policymaker's Perspective On Intelligence Analysis ». https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol38no5/pdf/v38i5a02p.pdf.

———. 1999. « Improving Intelligence Analysis at CIA: Dick Heuer's Contribution to Intelligence Analysis ». 1999. http://www.au.af.mil/au/awc/awcgate/psych-intel/art3.html.

Dean, Geoff, et Petter Gottschalk. 2007. *Knowledge Management in Policing and Law Enforcement: Foundations, Structures and Applications*. Oxford, New York: Oxford University Press.

Department of Homeland Security. 2010. « Quadrennial Homeland Security Review Report: A Strategic Frameworkfor a Secure Homeland ». https://www.dhs.gov/xlibrary/assets/qhsr_report.pdf.

Diane Publishing Company. 2000. *A Consumer's Guide to Intelligence*. Diane Publishing Company.

Duvenage, Magdalena Adriana. 2010a. « Intelligence Analysis in the Knowledge Age : An Analysis of the Challenges Facing the Practice of Intelligence Analysis ». Thesis, Stellenbosch : University of Stellenbosch. https://scholar.sun.ac.za:443/handle/10019.1/3087.

———. 2010b. « Intelligence Analysis in the Knowledge Age : An Analysis of the Challenges Facing the Practice of Intelligence Analysis ». Thesis, Stellenbosch : University of Stellenbosch. https://scholar.sun.ac.za:443/handle/10019.1/3087.

Ehrman, John. 2009. « Toward a Theory of CI — Central Intelligence Agency ». 2009. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol53no2/toward-a-theory-of-ci.html.

———. 2011. « What Are We Talking About When We Talk about Counterintelligence? » ResearchGate. 2011. https://www.researchgate.net/publication/237421011_What_are_We_Talking_About_When_We_Talk_about_Counterintelligence.

Ekpe, Bassey. 2005. « Theories of Collective Intelligence and Decision-Making: Towards a Viable United Nations Intelligence System ». Doctoral, University of Huddersfield. http://eprints.hud.ac.uk/id/eprint/7481/.

Ellis-Smith, James. 2016. « Analysis and Influence in Combat Intelligence ». *Journal of the Australian Institute of Professional Intelligence Officers* 24 (1): 34. http://search.informit.com.au/documentSummary;dn=256667623307302;res=IELHSS.

Evans, Jonathan. 2007. « Jonathan Evans, MI5 Director General's Speech on Intelligence, Counter-Terrorism and Trust, 5 November 2007 ». https://www.theguardian.com/uk/2007/nov/05/terrorism.world.

Evelson, Boris. 2008. « Topic Overview: Business Intelligence ». 2008. https://www.forrester.com/report/Topic+Overview+Business+Intelligence/-/E-RES39218#.

Feigenbaum, Edward A., et Pamela McCorduck. 1984. *The Fifth Generation: Artificial Intelligence and Japan's Computer Challenge to the World*. New American Library.

Feldman, David, et Jason Himmelstein. 2013. *Developing Business Intelligence Apps for SharePoint: Combine the Power of SharePoint, LightSwitch, Power View, and SQL Server 2012* (version 1 edition). 1 edition. Beijing: O'Reilly Media.

Firestone, Joseph M., et Mark W. McElroy. 2003. *Key Issues in the New Knowledge Management*. Butterworth-Heinemann.

Flood, Robert L. 1999. *Rethinking The Fifth Discipline: Learning Within the Unknowable*. Psychology Press.

Floridi, Luciano. 2002. « What Is the Philosophy of Information? » *Metaphilosophy* 33 (1-2): 123-45. https://doi.org/10.1111/1467-9973.00221.

Gelder, Tim van. 2012. « Exploring New Directions for Intelligence Analysis ». *Tim van Gelder* (blog). 2012. https://timvangelder.com/2012/12/11/exploring-new-directions-for-intelligence-analysis/.

Gentry, John A. 2015. « Has the ODNI Improved U.S. Intelligence Analysis? » *International Journal of Intelligence and CounterIntelligence* 28 (4): 637-61. https://doi.org/10.1080/08850607.2015.1050937.

Gilad, Ben. 2014. « CI Education Harvard style? » http://www.academyci.com/wp-content/uploads/2014/09/CI_Harvard_Style.pdf.

Godfrey, E. Drexel. 1978. « Ethics and Intelligence ». *Foreign Affairs*, 1978. https://www.foreignaffairs.com/articles/united-states/1978-04-01/ethics-and-intelligence.

Goodman, Michael S. 2007. « Studying and Teaching About Intelligence: The Approach in the United Kingdom — Central Intelligence Agency ». 2007. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol50no2/html_files/Studying_Teaching_6.htm.

Goradia, Hrishikesh, Jingshan Huang, et Michael N Huhns. 2005. « Extending Heuer's Analysis of Competing Hypotheses Method to Support Complex Decision Analysis ». ResearchGate. 2005. https://www.researchgate.net/publication/241836758_Extending_Heuer's_Analysis_of_Competing_Hypotheses_Method_to_Support_Complex_Decision_Analysis.

Greco, John, et Ernest Sosa. 1999. *The Blackwell Guide to Epistemology* (version 1 edition). 1 edition. Malden, Mass: Wiley-Blackwell.

Grenon, Pierre, et Barry Smith. 2004. « SNAP and SPAN: Towards Dynamic Spatial Ontology ». http://ontology.buffalo.edu/smith/articles/SNAP_SPAN.pdf.

Gulati, Ranjay, Ryan Raffaelli, et Jan Rivkin. 2016. « Does "What We Do" Make Us "Who We Are"? Organizational Design and Identity Change at the Federal Bureau of Investigation ». https://www.hbs.edu/faculty/Pages/item.aspx?num=50565.

Haag, Stephen. 2012. *Management Information Systems for the Information Age: Ninth Edition*. McGraw-Hill Higher Education.

Haas, Peter M. 1992. « Introduction: epistemic communities and international policy coordination | International Organization | Cambridge Core ». 1992. https://www.cambridge.org/core/journals/international-organization/article/introduction-epistemic-communities-and-international-policy-coordination/CE9CFC049E0F2A14635F1E3EB51960C9.

———. 2001. « Policy Knowledge: Epistemic Communities ». In *International Encyclopedia of the Social and Behavioral Sciences*, édité par N. J. Smelser et B. Baltes, 17–11578.

Hayes, Joseph. 2007. « Chapter One — Central Intelligence Agency ». 2007. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/chapter_1.htm.

Herman, Michael. 2001. *Intelligence Services in the Information Age: Theory and Practice*. Taylor & Francis.

Heuer, Richards J. 1999a. *Psychology of Intelligence Analysis*. Lulu.com.

———. 1999b. *Psychology of Intelligence Analysis*. Lulu.com.

Heuer, Richards J., et Randolph H. Pherson. 2010. *Structured Analytic Techniques for Intelligence Analysis*. CQ Press.

Hogan, Bernie, Juan Antonio Carrasco, et Barry Wellman. 2007. « Visualizing Personal Networks: Working with Participant-Aided Sociograms ». *Field Methods* 19 (2): 116-44. https://doi.org/10.1177/1525822X06298589.

Holsapple, Clyde, éd. 2004. *Handbook on Knowledge Management 1: Knowledge Matters*. International Handbooks on Information Systems. Berlin Heidelberg: Springer-Verlag. //www.springer.com/gp/book/9783540435273.

Howard, Russell, et Reid Sawyer. 2003. *Terrorism and Counterterrorism: Understanding the New Security Environment, Readings and Interpretations, Revised & Updated 2004*. 1 edition. Guilford, Conn.: McGraw-Hill/Dushkin.

Hsu, Jennifer Y. J., et Reza Hasmath. 2017. « A Maturing Civil Society in China? The Role of Knowledge and Professionalization in the Development of NGOs ». SSRN Scholarly Paper ID 2563696. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=2563696.

Hulnick, Arthur S. 2006. « What's Wrong with the Intelligence Cycle ». 2006. https://www.researchgate.net/publication/245493621_What's_Wrong_with_the_Intelligence_Cycle.

Hunter, Duncan, et Malcolm N. MacDonald. 2017. « The emergence of a security discipline in the post 9-11 discourse of U.S. security organisations ». *Critical Discourse Studies* 14 (2): 206-22. https://doi.org/10.1080/17405904.2016.1268185.

Huntington, Samuel P. 1981. *The Soldier and the State: The Theory and Politics of Civil–Military Relations*. Revised edition. Cambridge, Mass: Belknap Press: An Imprint of Harvard University Press.

Husserl, Edmund. 1900. « Logische Untersuchungen ». 1900. https://philpapers.org/rec/HUSLU.

Ikle, Fred. 2005. *Every War Must End (Columbia Classics)*. Revised edition edition. Columbia University Press.

Intelligence.gov. 2013. « Seventeen Agencies and Organizations United Under One Goal ». 2013. https://web.archive.org/web/20130502012837/http://www.intelligence.gov/about-the-intelligence-community/.

Jacobs, Struan. 2001. « Michael Polanyi, Tacit Cognitive Relativist ». *Heythrop Journal* 42 (4): 463–479.

Johnson, William R., et William Hood. 2009. *Thwarting Enemies at Home and Abroad: How to Be a Counterintelligence Officer*. 3.2.2009 edition. Washington, D.C: Georgetown University Press.

Johnston, Rob. 2003. « Integrating Methodologists into Teams of Substantive Experts ». https://apps.dtic.mil/dtic/tr/fulltext/u2/a525552.pdf.

———. 2005. *Analytic Culture in the US Intelligence Community: An Ethnographic Study*. University of Michigan Library.

Joint Publication 2-01. 2012. « Joint and National Intelligence Support to Military Operations ». https://www.bits.de/NRANEU/others/jp-doctrine/jp2_01%2812%29.pdf.

Jones, Milo L., et Philippe Silberzahn. 2013. « Constructing Cassandra: Reframing Intelligence Failure at the CIA, 1947–2001 | Milo Jones and Philippe Silberzahn ». 2013. http://www.sup.org/books/title/?id=22067.

Jones, Morgan D. 2009. *The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving*. Crown Publishing Group.

Jordan, Lloyd F. 2008. « The Arab Mind by Raphael Patai. Book review by Lloyd F. Jordan — Central Intelligence Agency ». 2008. https://web.archive.org/web/20080213114422/https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/docs/v18i3a06p_0001.htm.

Keman, Hans. 1998. *Autonomous Policy Making By International Organisations*. Édité par Bob Reinalda et Bertjan Verbeek. London ; New York: Routledge.

Kent, SHERMAN. 1966. *Strategic Intelligence for American World Policy*. Princeton University Press. https://www.jstor.org/stable/j.ctt183q0qt.

Keynes, J. M. 1937. « The General Theory of Employment ». *The Quarterly Journal of Economics* 51 (2): 209-23. https://doi.org/10.2307/1882087.

Krapohl, Don. 2013. « Working .NET Entity Extractor Using OpenNLP Models ». *A | I – Augmented Intelligence* (blog). 2013. http://www.augmentedintel.com/wordpress/index.php/augmented-intel-free-online-analytics-applications-for-corporate-intelligence/working-net-entity-extractor-using-opennlp-models/.

Krizan, Lisa. 1999a. « Intelligence Essentials for Everyone ». ResearchGate. 1999. https://www.researchgate.net/publication/235073074_Intelligence_Essentials_for_Everyone.

———. 1999b. « Intelligence Essentials for Everyone ». ResearchGate. 1999. https://www.researchgate.net/publication/235073074_Intelligence_Essentials_for_Everyone.

Kurtz, Jay. 2018. « What Is A Business Wargame? » 2018. http://competitive-intelligence.mirum.net/competitive-intelligence-methods/what-is-a-business-wargame.html.

Kydd, Andrew. 1997. « Game Theory and the Spiral Model ». *World Politics* 49 (3): 371-400. https://www.jstor.org/stable/25054007.

Laqueur, Walter. 1993. *The Uses and Limits of Intelligence*. Transaction Publishers.

Leckie, Gloria J., Karen E. Pettigrew, et Christian Sylvain. 1996. « Modeling the Information Seeking of Professionals: A General Model Derived from Research on Engineers, Health Care Professionals, and Lawyers ». ResearchGate. 1996. https://www.researchgate.net/publication/237440858_Modeling_the_Information_Seekin

g_of_Professionals_A_General_Model_Derived_from_Research_on_Engineers_Health_Care_Professionals_and_Lawyers.
Lillbacka, Ralf G. V. 2013. « Realism, Constructivism, and Intelligence Analysis ». *International Journal of Intelligence and CounterIntelligence* 26 (2): 304-31. https://doi.org/10.1080/08850607.2013.732450.
Little, E. G., et G. L. Rogova. 2005. « Ontology meta-model for building a situational picture of catastrophic events ». *2005 7th International Conference on Information Fusion* 1: 8-NaN.
Little, Eric G., et Galina L. Rogova. 2006. « An Ontological Analysis of Threat and Vulnerability ». *2006 9th International Conference on Information Fusion*, 1-8. https://doi.org/10.1109/ICIF.2006.301716.
Loik, Ramon. 2013. « Security Integration in Europe: How Knowledge-Based Networks Are Transforming the European Union, by M.K. Davis Cross (Ann Arbor, MI: University of Michigan Press, 2012, ISBN 9780472117895); Xviii+281pp., £55.95 Hb. » *JCMS: Journal of Common Market Studies* 51 (3): 576-77. https://doi.org/10.1111/jcms.12016_5.
Manjikian, Mary. 2013. « Positivism, Post-Positivism, and Intelligence Analysis ». *International Journal of Intelligence and CounterIntelligence* 26 (3): 563-82. https://doi.org/10.1080/08850607.2013.758002.
Marrin, Stephen. 2012a. *Improving Intelligence Analysis: Bridging the Gap between Scholarship and Practice*. Routledge.
———. 2012b. « Is Intelligence Analysis an Art or a Science? » *International Journal of Intelligence and CounterIntelligence* 25 (3): 529-45. https://doi.org/10.1080/08850607.2012.678690.
———. 2012c. « Is Intelligence Analysis an Art or a Science? » *International Journal of Intelligence and CounterIntelligence* 25 (3): 529-45. https://doi.org/10.1080/08850607.2012.678690.
Marrin, Stephen, et Jonathan D. Clemente. 2005. « Improving Intelligence Analysis by Looking to the Medical Profession ». *International Journal of Intelligence and CounterIntelligence* 18 (4): 707-29. https://doi.org/10.1080/08850600590945434.
Marrin, Stephen, et Efren Torres. 2017. « Improving how to think in intelligence analysis and medicine ». *Intelligence and National Security* 32 (5): 649-62. https://doi.org/10.1080/02684527.2017.1311472.
Martin, Kirsty. 2011. « The Paradox of Intuitive Analysis and the Implications for Professionalism ». ResearchGate. 2011. https://www.researchgate.net/publication/258839553_The_Paradox_of_Intuitive_Analysis_and_the_Implications_for_Professionalism.
Matschulat, Austin B. 2007. « Coordination and Cooperation in Counterintelligence — Central Intelligence Agency ». 2007. https://web.archive.org/web/20071010091345/https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/docs/v13i2a05p_0001.htm.
McChrystal, General Stanley. 2014. *My Share of the Task: A Memoir*. Reprint edition. New York, NY: Portfolio.
McConnell, Mike. 2007. « Overhauling intelligence ». 2007. https://www.researchgate.net/publication/293761677_Overhauling_intelligence.

McGonagle, John J., et Carolyn M. Vella. 2003. *The Manager's Guide to Competitive Intelligence*. Greenwood Publishing Group.
Miscik, Jami. 2017. « Intelligence and the Presidency How to Get It Right ». ResearchGate. 2017. https://www.researchgate.net/publication/319978753_Intelligence_and_the_presidency_how_to_get_it_right.
Moore, David T., et National Defense Intelligence College. 2010. *Critical Thinking and Intelligence Analysis*. Books Express Publishing.
Morgan, Richard O. 2012. « Latif v. Obama: The Epistemology of Intelligence Information and Legal Evidence ». https://gould.usc.edu/why/students/orgs/ilj/assets/docs/7%20-%20Morgan%20V2.pdf.
Morin, Jean-Frederic, et Selim Louafi. 2017. « Boundary Organizations in Regime Complexes: A Social Network Profile of IPBES ». ResearchGate. 2017. https://www.researchgate.net/publication/320657829_Boundary_Organizations_in_Regime_Complexes_A_Social_Network_Profile_of_IPBES.
Mudd, Philip, et Greg Abbey. 2015. *The HEAD Game: High-Efficiency Analytic Decision Making and the Art of Solving Complex Problems Quickly*. Unabridged edition. Audible Studios on Brilliance Audio.
Nagy, John A. 2016. *George Washington's Secret Spy War: The Making of America's First Spymaster*. St. Martin's Press.
NATO. 2018. « AAP-6 - NATO Glossary of terms and definitions ». https://apps.dtic.mil/dtic/tr/fulltext/u2/a574310.pdf.
Office of the Director of National Intelligence. 2005. « National Intelligence Strategy of the United States of America: Transformation through Integration and Innovation ». https://www.dni.gov/files/documents/CHCO/nis.pdf.
O'Malley, Pat. 2016. « 'Policing the Risk Society' in the 21st Century ». SSRN Scholarly Paper ID 2729631. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=2729631.
Omand, David. 2009. « TheNationalSecurityStrategy: Implications for the UK intelligence community ». https://warwick.ac.uk/fac/soc/pais/people/aldrich/vigilant/national_security_strategy1.pdf.
———. 2011. *Securing the State* (version UK ed. edition). UK ed. edition. London: C Hurst & Co Publishers Ltd.
Ormerod, Owen. 2018a. « Advancing the Epistemology of Intelligence Analysis: A Polanyian Perspective ». ResearchGate. 2018. https://www.researchgate.net/publication/328232543_Advancing_the_epistemology_of_intelligence_analysis_A_Polanyian_perspective.
———. 2018b. « Advancing the Epistemology of Intelligence Analysis: A Polanyian Perspective ». ResearchGate. 2018. https://www.researchgate.net/publication/328232543_Advancing_the_epistemology_of_intelligence_analysis_A_Polanyian_perspective.
Palmer, Bill. 1991. *Strategic intelligence for law enforcement*. Canberra: Australian Bureau of Criminal Intelligence.
Persico, Joseph E. 2002. *Roosevelt's Secret War: FDR and World War II Espionage*. Random House.

Peters, Adrienne M. F., et Irwin M. Cohen. 2017. « The mandate and activities of a specialized crime reduction policing unit in Canada ». *Police Practice and Research* 18 (6): 570-83. https://doi.org/10.1080/15614263.2017.1363970.
Pherson, Randolph. 2013. « The Five Habits of the Master Thinker ». *Journal of Strategic Security* 6 (3). http://dx.doi.org/10.5038/1944-0472.6.3.5.
Platt, Washington. 1957. *Strategic Intelligence Production: Basic Principles*. F.A. Praeger.
Polanyi, Michael. 1962. *Personal Knowledge: Towards a Post-Critical Philosophy*. https://www.press.uchicago.edu/ucp/books/book/chicago/P/bo19722848.html.
———. 1964. *Science, Faith and Society*. Later Printing edition. Chicago: University of Chicago Press.
———. 1969. *Knowing and Being*. Édité par Marjorie Grene. 1st Edition edition. Chicago: University of Chicago Press.
———. 1998. *The Logic Of Liberty*. First Edition. Indianapolis: Liberty Fund Inc.
Polanyi, Michael, et Amartya Sen. 2009. *The Tacit Dimension*. Reissue edition. Chicago ; London: University of Chicago Press.
Pope, Simon, et Audun Jøsang. 2005. « Analysis of Competing Hypotheses using Subjective Logic (ACH-SL) ». https://apps.dtic.mil/dtic/tr/fulltext/u2/a463908.pdf.
Popper, Karl R. 1972. *Objective Knowledge: An Evolutionary Approach* (version Revised edition). Revised edition. Oxford Eng. : New York: Oxford University Press.
Prescott, John E. 2012. « The Evolution of Competitive Intelligence ». *Revista Inteligência Competitiva* 2 (2). https://doi.org/10.24883/ric.v2i2.45.
Pritchard, Matthew C., et Michael S. Goodman. 2009. « Intelligence: The Loss of Innocence ». *International Journal of Intelligence and CounterIntelligence* 22 (1): 147-64. https://doi.org/10.1080/08850600802487018.
Quiggin, Thomas A. 2007. *Seeing The Invisible: National Security Intelligence In An Uncertain Age*. Hackensack, NJ: Wspc/Others.
Radaelli, Claudio M. 1999. « The public policy of the European Union: whither politics of expertise? » *Journal of European Public Policy* 6 (5): 757-74. https://doi.org/10.1080/135017699343360.
Radner, Roy. 1972. « Normative Theory of Individual Decision: An Introduction ». http://pages.stern.nyu.edu/~rradner/.
Rafii, Farshad, et Paul J. Kampas. 2002. « How to Identify Your Enemies Before They Destroy You ». *Harvard Business Review*, 2002. https://hbr.org/2002/11/how-to-identify-your-enemies-before-they-destroy-you.
Ratcliffe, Jerry H. 2008. *Intelligence-Led Policing*. 1 edition. Cullompton, Devon: Willan.
Richelson, Jeffrey. 1988. *Foreign Intelligence Organizations*. Ballinger Publishing Company.
Robertson, K. G. 1987. « Intelligence requirements for the 1980s ». *Intelligence and National Security* 2 (4): 157-67. https://doi.org/10.1080/02684528708431921.
Robertson, Ken. 1996. « Intelligence, Terrorism and Civil Liberties ». https://journals.lib.unb.ca/index.php/JCS/article/viewFile/14756/15825.
Rønn, Kira Vrist, et Simon Høffding. 2013. « The Epistemic Status of Intelligence: An Epistemological Contribution to the Understanding of Intelligence ». 2013. https://www.researchgate.net/publication/263573379_The_Epistemic_Status_of_Intelligence_An_Epistemological_Contribution_to_the_Understanding_of_Intelligence.
Rudd, Kevin. 2008. « The First National Security Statement to the Australian Parliament, Address by the Prime Minister of Australia ». https://dfat.gov.au/people-to-people/public-

diplomacy/programs-activities/Pages/speech-by-prime-minister-kevin-rudd-to-the-parliament.aspx.
Salmen, David, Tatiana Malyuta, Alan Hansen, Shaun Cronen, et Barry Smith. 2011. « Integration of Intelligence Data through Semantic Enhancement ». In *STIDS*.
SCIP. 2014. « Code of Ethics - Strategic and Competitive Intelligence Professionals (SCIP) ». 2014. https://www.scip.org/page/CodeofEthics.
Scott, Len, et Peter Jackson. 2004. « The Study of Intelligence in Theory and Practice ». *Intelligence and National Security* 19 (2): 139-69. https://doi.org/10.1080/0268452042000302930.
Sebenius, James K. 1992. « Challenging Conventional Explanations of International Cooperation: Negotiation Analysis and the Case of Epistemic Communities ». *International Organization* 46 (1): 323-65. https://doi.org/10.1017/S0020818300001521.
Sfetcu, Nicolae. 2016. *Cunoaştere şi Informaţii*. Nicolae Sfetcu.
Shaikh Muhammad, Akram, et Wang Jiaxin. 2006. « Investigative Data Mining: Connecting the dots to disconnect them ». Intelligence Tools Workshop. http://www.huitfeldt.com/repository/ITW06.pdf.
Shelley, Louise I. 1990. « Policing Soviet Society: The Evolution of State Control ». *Law & Social Inquiry* 15 (3): 479-520. https://www.jstor.org/stable/828493.
Shoham, Dany, et Michael Liebig. 2016. « The intelligence dimension of Kautilyan statecraft and its implications for the present ». *Journal of Intelligence History* 15 (2): 119-38. https://doi.org/10.1080/16161262.2015.1116330.
Shrager, Jeff, Dorrit Billman, Gregorio Convertino, J. P. Massar, et Peter Pirolli. 2010. « Soccer Science and the Bayes Community: Exploring the Cognitive Implications of Modern Scientific Communication ». *Topics in Cognitive Science* 2 (1): 53-72. https://doi.org/10.1111/j.1756-8765.2009.01049.x.
Shulsky, Abram N., et Gary James Schmitt. 2002. *Silent Warfare: Understanding the World of Intelligence*. Potomac Books, Inc.
Silver, Mark S., M. Lynne Markus, et Cynthia Mathis Beath. 1995. « The Information Technology Interactive Model: A Foundation for the MBA Core Course ». 1995. https://misq.org/catalog/product/view/id/668.
Singer, J. David. 1958. « Threat-Perception and the Armament-Tension Dilemma ». *The Journal of Conflict Resolution* 2 (1): 90-105. https://www.jstor.org/stable/172848.
Smith, Barry. 1996. « Mereotopology: A theory of parts and boundaries - ScienceDirect ». 1996. https://www.sciencedirect.com/science/article/pii/S0169023X96000158.
———. 2012. « Ontology for the Intelligence Analyst ». 2012. https://philarchive.org.
Smith, Barry, Lowell Vizenor, et James Schoening. 2009. « Universal Core Semantic Layer ». In .
Smith, Michael Douglas. 2017. « A Good Intelligence Analyst ». *International Journal of Intelligence and CounterIntelligence* 30 (1): 181-85. https://doi.org/10.1080/08850607.2016.1230708.
Soustelle, Jacques. 2002. *Daily Life of the Aztecs*. Courier Corporation.
Stewart, Thomas A. 2001. *The Wealth of Knowledge: Intellectual Capital and the Twenty-first Century Organization*. New York, NY, USA: Doubleday.
US Department of the Army. 1981. « Executive Order 12333. (1981, December 4). United States Intelligence Activities, Section 3.4(a). EO provisions found in 46 FR 59941, 3 CFR ». https://fas.org/irp/doddir/army/fm34-60/.

———. 1995. « Field Manual 34-60: Counterintelligence ». https://fas.org/irp/doddir/army/fm34-60/.
US Government. 2009. « A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis ». https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf.
Vandepeer, Charles. 2011. « Rethinking threat: intelligence analysis, intentions, capabilities, and the challenge of non-state actors. » Thesis. https://digital.library.adelaide.edu.au/dspace/handle/2440/70732.
———. 2014. « Applied Thinking for Intelligence Analysis : A Guide for Practitioners ». 2014. //www.awm.gov.au/index.php/collection/LIB100045502.
Volkswagen Foundation. 2002. « Basic Formal Ontology ». http://basic-formal-ontology.org/.
Walsh, Patrick F. 2010. *Intelligence and Intelligence Analysis*. 1 edition. New York, NY: Willan.
Waltz, Edward. 2003. *Knowledge Management in the Intelligence Enterprise*. Artech House.
———. 2014. *Quantitative Intelligence Analysis: Applied Analytic Models, Simulations, and Games*. Lanham, Maryland: Rowman & Littlefield Publishers.
Weick, Karl E. 1995. *Sensemaking in Organizations*. SAGE.
Weiner, Tim. 2007. « Pssst: Some Hope for Spycraft ». *The New York Times*, 2007, sect. Week in Review. https://www.nytimes.com/2007/12/09/weekinreview/09weiner.html.
Wheaton, Kristan J., et Michael T. Beerbower. 2006. « Towards a New Definition of Intelligence ». Stanford Law School. 2006. https://law.stanford.edu/publications/towards-new-definition-intelligence/.
Wheaton, Kristan J., et Diane E. Chido. 2007. « Structured Analysis of Competing Hypotheses: Improving a Tested Intelligence Methodology ». 2007. https://web.archive.org/web/20070928154654/http://www.mcmanis-monsalve.com/assets/publications/intelligence-methodology-1-07-chido.pdf.
Wheeler, Douglas L. 2012. « A Guide to the History of Intelligence 1800–1918 ». https://www.afio.com/publications/Wheeler_Hist_of_Intel_1800-1918_in_AFIO_INTEL_WinterSprg2012.pdf.
Wimalasuriya, Daya C., et Dejing Dou Dejing Dou. 2010. « (PDF) Ontology-Based Information Extraction: An Introduction and a Survey of Current Approaches ». ResearchGate. 2010. https://www.researchgate.net/publication/220195792_Ontology-based_information_extraction_An_Introduction_and_a_survey_of_current_approaches.
Wolfberg, Adrian. 2006. « Full-Spectrum Analysis: A New Way of Thinking for a New World. » Military Review, July-August 2006. http://cgsc.cdmhost.com/cdm/ref/collection/p124201coll1/id/414.
Woolsey, James. 1998. « Testimony, 12 February 1998, US House of Representatives Committee on National Security ». https://fas.org/irp/congress/1998_hr/h980212w.htm.
Ylikoski, Petri. 2017. « The Illusion of Depth of Understanding in Science ». https://doi.org/10.31235/osf.io/qz7sg.
Yuen, Derek M. C. 2014. *Deciphering Sun Tzu: How to Read « The Art of War »*. Oxford University Press.
Zheng, Jack. 2014. « Information system a system view ». Technology. https://www.slideshare.net/jgzheng/information-system-a-system-view.