Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

Article de recherche

L'INTELLIGENCE SOUS LES FEUX DE LA RAMPE : DE LA THÉORIE CLASSIQUE À UNE NOUVELLE APPROCHE DE LA MISE EN ŒUVRE À L'ÈRE NUMÉRIQUE

Traduction en français à l'aide de l'IA (DeepL)

Paula Castro Castañer
Expert en sécurité chez Telefónica S.A.
Doctorant en sciences médico-légales à l'université d'Alcalá
Master en cybersécurité et vie privée de l'Universitat Oberta de Catalunya (UOC)
paula.castroc@edu.uah.es
ORCID : 0009-0008-0315-8387

Reçu le 14/02/2025
Accepté le 16/06/2025
Publié le 27/06/2025

Citation recommandée : Castro P. (2025). L'intelligence sous les feux de la rampe : de la théorie classique à une nouvelle approche de la mise en œuvre à l'ère numérique. *Logos Guardia Civil Magazine*, 3(2), p.p. 71-100.

Licence : Cet article est publié sous la licence Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).
Dépôt légal : M-3619-2023
NIPO en ligne : 126-23-019-8
ISSN en ligne : 2952-394X

ORCID : **0009-0008-0315-8387**

DÉDICACEUR

A mon tuteur, Hilario, pour m'avoir fait confiance et m'avoir soutenu dans tous mes projets.

ORCID : **0009-0008-0315-8387**

L'INTELLIGENCE SOUS LES FEUX DE LA RAMPE : DE LA THÉORIE CLASSIQUE À UNE NOUVELLE APPROCHE DE LA MISE EN ŒUVRE À L'ÈRE NUMÉRIQUE

Résumé: INTRODUCTION. 1.1. NOTE MÉTHODOLOGIQUE. 2. CONCEPT ET ÉVOLUTION DU RENSEIGNEMENT. 2.1. TYPES DE RENSEIGNEMENT. 2.2. ÉVOLUTION DES APPROCHES ET DES STRATÉGIES DE RENSEIGNEMENT. 3. LE CYCLE DU RENSEIGNEMENT. 4. PROPOSITION D'ACTUALISATION DU CYCLE DU RENSEIGNEMENT À L'ÈRE NUMÉRIQUE : LE MODÈLE IDEM. 4.1. EXEMPLE PRATIQUE DE MISE EN ŒUVRE DU MODÈLE IDEM. 5. CONCLUSIONS 6. 5. CONCLUSIONS 6. RÉFÉRENCES BIBLIOGRAPHIQUES.

Résumé : Cet article traite de l'évolution du renseignement dans le domaine de la défense et de la sécurité, depuis les approches traditionnelles jusqu'à son adaptation à l'ère numérique, en établissant une proposition qui répond à certaines des limites signalées dans la littérature sur le cycle classique du renseignement. À cette fin, des concepts clés sont explorés, tels que la définition du concept de renseignement, les différents types de renseignement et même le cycle de renseignement traditionnel et ses phases. En outre, un examen de l'évolution et des différentes approches qui ont été adoptées au cours de l'histoire dans le domaine du renseignement est présenté. Enfin, il propose un modèle de renseignement, appelé IDEM, avec des phases flexibles et combinant le talent des analystes humains et le traitement automatisé des big data pour assurer un renseignement proactif, adaptatif et de qualité face aux cybermenaces transnationales complexes.

Resumen: Este artículo aborda la evolución de la inteligencia en el ámbito de la Defensa y Seguridad, desde los enfoques tradicionales hasta su adaptación a la era digital, estableciendo una propuesta que responda a algunas de las limitaciones señaladas en la literatura sobre el ciclo clásico de inteligencia. Para ello se exploran conceptos clave como la definición del concepto de inteligencia, los diferentes tipos de inteligencia e incluso el tradicional ciclo de inteligencia y sus fases. Además, se presenta una revisión de la evolución y de los diferentes enfoques que se han ido adoptando a lo largo de la historia en materia de inteligencia. Por último, se propone un modelo de inteligencia, denominado IDEM, con fases flexibles y que combine el talento del analista humano y el procesamiento automatizado de grandes volúmenes de datos para garantizar una inteligencia proactiva, adaptativa y de calidad ante las complejas amenazas cibernéticas transnacionales.

Mots clés : cybermenaces, cyberveille, cycle du renseignement, modèle IDEM, approche en réseau

Palabras clave: Amenazas cibernéticas, ciberinteligencia, ciclo de inteligencia, modelo IDEM, enfoque en red

ORCID : **0009-0008-0315-8387**

ABBREVIATIONS

ABI : *Intelligence basée sur les activités*

CCN-CERT : Centre national de cryptologie - Équipe d'*intervention en cas d'urgence informatique*

CESID : Centro Superior de Información de la Defensa (Centre supérieur d'information de la défense)

CIA : *Central Intelligence Agency, Agence* centrale *de renseignement*

CIFAS : Centre d'intelligence des forces armées

CNI : Centre national de renseignement

COMINT : *Communications Intelligence (renseignements sur les communications)*

COP *: police de proximité*, police *orientée vers la collectivité*

CTI : *Cyber Threat Intelligence*, Cyber Threat *Intelligence*

CYBINT : *Cyber-renseignement,* cyber-renseignement

ELINT : *renseignement électronique*

FISINT : *Foreign* instrumentation *signals intelligence (renseignement d'origine* électromagnétique*)*

GEOINT : *Geospatial Intelligence, renseignement* géospatial

HUMINT : *Renseignement humain*

IDEM : Enhanced Dynamic Intelligence Enrichment and Enhancement (Enrichissement et amélioration dynamiques de l'intelligence)

IDS : *Intrusion Detection System,* Système de *détection d'intrusion*

ILP *: Intelligence-Led Policing, Police basée sur le renseignement*

IMINT : *Imagery Intelligence (renseignement par imagerie)*

ISR : *Intelligence Surveillance and Reconnaissance (renseignement,* surveillance et reconnaissance*), Intelligence,* surveillance and reconnaissance *(renseignement,* surveillance et reconnaissance*)*

JISR : *Joint Intelligence Surveillance and Reconnaissance (renseignement,* surveillance et *reconnaissance conjoints), Joint Intelligence,* Surveillance and *Reconnaissance (renseignement,* surveillance et *reconnaissance conjoints)*

MASINT : *Measurement* and *Signature Intelligence (renseignements sur* les mesures et les *signatures)*

ML : *Machine Learning,* Apprentissage *automatique*

NLP : *Natural Language Processing (traitement du langage naturel)*

OSCE : *Organisation pour la sécurité et la coopération en Europe,* Organisation *pour la sécurité et la coopération* en Europe

OSINT : *Open-Source Intelligence (renseignement de source ouverte)*

SCADA : système *de contrôle* et d'*acquisition de données (Supervisory Control* and *Data Acquisition)*

SECED : Service central de documentation

SIEM : *Security Information* and *Event Management (gestion des informations* et des *événements de sécurité)*

SIGINT : Signal *Intelligence (renseignement d'origine électromagnétique*)

SOCMINT : *Social Media Intelligence*, Social Media Intelligence

TCPED : *Tâche, Collecte, Traitement, Exploitation, Dissémination,* Approche, Collecte, Traitement, Exploitation, *Dissémination*

TTP : *menaces, techniques et procédures*

ORCID : **0009-0008-0315-8387**

1. INTRODUCTION

Dans un monde où l'intelligence artificielle semble dominer l'attention et les préoccupations du public, où l'intelligence sous toutes ses autres formes est-elle reléguée au second plan ? L'omniprésence de l'intelligence artificielle dans les débats contemporains occulte souvent l'importance d'autres types d'intelligence qui sont fondamentaux pour le progrès et le développement de l'humanité.

L'intelligence humaine, dans ses multiples manifestations, reste un pilier irremplaçable pour la prospérité de la société, encore plus dans les contextes complexes et changeants de cette ère numérique. L'une de ces manifestations est la veille concurrentielle, qui permet d'obtenir des recommandations actionnables en traitant des informations sur l'environnement externe à la recherche d'opportunités ou d'évolutions pouvant impacter la position concurrentielle d'une entreprise ou d'un pays (Lee, 2023). Ou encore l'intelligence prospective qui, sur la base d'informations passées et présentes, ainsi que de spéculations futures, tente de "dessiner" une carte cognitive pour déterminer différentes options et réduire le niveau d'incertitude qui accompagne toute décision (Montero Gómez, 2006).

Il est vrai que la croissance exponentielle de la numérisation, de l'exposition et de la mondialisation entraîne l'apparition et l'évolution de nouvelles formes de renseignement en réponse aux nouvelles technologies et méthodes de collecte de données, donnant naissance à des formes de renseignement telles que le renseignement de source ouverte (OSINT) ou le renseignement géospatial (GEOINT), entre autres. Ces disciplines tirent parti de la grande quantité d'informations disponibles pour fournir une vision globale, intégrée et détaillée de divers phénomènes. Toutefois, le renseignement ne doit pas se limiter à la collecte et à l'analyse de données, mais doit également intégrer des considérations éthiques et évaluer les conséquences potentielles à long terme des décisions.

Aujourd'hui, l'information et la technologie sont essentielles à presque tous les aspects de la vie, et le renseignement joue un rôle crucial, en particulier dans le domaine de la cybersécurité, car la capacité d'anticiper, d'identifier et d'atténuer les menaces est essentielle pour préserver l'intégrité, la confidentialité et la disponibilité des systèmes.

Toutefois, la question se pose de savoir si cette capacité est une réalité dans les agences gouvernementales et privées d'aujourd'hui, si le renseignement est efficace pour anticiper et atténuer les risques croissants dans le cyberespace, et si le cycle du renseignement est à jour pour répondre aux exigences de l'ère numérique. Le présent document vise à effectuer une analyse théorique pour répondre à ces questions et évaluer l'efficacité du renseignement dans le contexte actuel.

1.1. NOTE MÉTHODOLOGIQUE

Pour l'élaboration de ce travail, une analyse narrative de la littérature académique et technique relative au renseignement dans les domaines de la défense et de la sécurité, ainsi que son adaptation à l'environnement numérique, a été réalisée. Cet examen a servi de base pour contextualiser l'évolution du concept, analyser de manière critique le cycle classique du renseignement et fournir la base de la proposition du modèle IDEM.

La recherche a été effectuée dans des bases de données universitaires telles que Scopus, Google Scholar et Dialnet, ainsi que dans des sources institutionnelles nationales et internationales. Des mots-clés en espagnol et en anglais ont été utilisés, tels que "cycle du renseignement", "cyber-renseignement", "cyber-renseignement" ou "cyber-menaces". La priorité a été donnée aux publications récentes (2000-2024) qui proposaient des approches théoriques, des modèles méthodologiques ou des analyses critiques du processus de renseignement. Occasionnellement, en raison de l'absence de littérature de source ouverte, des sites web réputés ou des sites web rédigés par des spécialistes techniques du domaine ont été consultés.

Les documents sans support académique ou institutionnel ont été exclus, de même que les textes qui ne traitaient pas spécifiquement de la dimension structurelle ou processuelle du renseignement. La littérature sélectionnée a été organisée autour de cinq axes thématiques : (1) définition du concept de renseignement, (2) classification des types de renseignement, (3) évolution historique et organisationnelle des services de renseignement, (4) examen critique du cycle traditionnel et (5) propositions contemporaines pour son adaptation à l'ère numérique.

Cette approche méthodologique a permis de détecter les lacunes théoriques pertinentes et de servir de base à l'élaboration d'un modèle actualisé qui intègre à la fois la dimension humaine et les capacités technologiques de l'intelligence d'aujourd'hui.

2. CONCEPT ET ÉVOLUTION DE L'INTELLIGENCE

Le terme "intelligence" est un concept abstrait et complexe à délimiter en raison de la multitude d'approches sous lesquelles il peut être étudié. Cette difficulté répond non seulement à la diversité des domaines qui l'analysent, mais aussi aux défis que pose, dans un même contexte, l'établissement d'une définition unique.

Dans le domaine de la défense et de la sécurité, la plupart des auteurs lient la naissance du renseignement à l'émergence des Etats et des relations interétatiques. Cependant, il n'existe pas de consensus sur la définition du renseignement, en raison notamment des différentes approches adoptées dans la pratique par les différents pays (Andric & Terzic, 2023). Cette disparité entrave à la fois les progrès théoriques de son étude et la compréhension approfondie des différentes dimensions et facteurs qui affectent sa pratique (Payá-Santos, 2023).

Dans ce contexte, l'une des premières classifications fondamentales, la trinité, a été établie par Sherman Kent, qui a défini trois réalités pour ce concept : l'intelligence en tant qu'organisation, en tant que processus et en tant que résultat (Díaz Fernández, 2013).

- **Le renseignement en tant qu'organisation : il** s'agit des services de renseignement qui relèvent principalement de l'administration publique, comme le Centre national de renseignement (CNI) et le Centre de renseignement des forces armées (CIFAS) en Espagne. Les fonctions de ces institutions comprennent l'obtention, l'évaluation, l'interprétation et la diffusion de renseignements pour protéger et promouvoir les intérêts de l'Espagne, tant à l'intérieur qu'à l'extérieur du pays ; la prévention, la détection et la neutralisation des menaces à la constitution, aux droits et libertés, à la souveraineté, à la sécurité de l'État, à la stabilité institutionnelle et au bien-être de la population ; la promotion de la

coopération avec les services de renseignement étrangers et les organisations internationales ; l'interprétation du trafic de signaux stratégiques ; la coordination de l'utilisation des moyens de cryptage ; la garantie de la sécurité des informations classifiées ; et la protection de ses propres installations, informations et ressources (Jefatura del Estado, 2002).

- **Le renseignement en tant que processus** : il comprend toutes les activités, généralement englobées dans ce que l'on appelle le cycle du renseignement (examiné plus en détail dans les sections suivantes), qui sont nécessaires pour répondre aux exigences des dirigeants et qui interprètent un environnement, un contexte ou un problème. Ces activités sont considérées comme un processus cyclique continu et vont de la collecte d'informations auprès de diverses sources à la diffusion des données intéressantes pour les utilisateurs finaux, en passant par l'analyse et le traitement de ces informations (Chainey & Chapman, 2013).
- **Le renseignement en tant que produit : il** s'**agit** du résultat et/ou de la connaissance obtenus, sous quelque forme que ce soit, à l'issue du cycle de renseignement. Ce produit doit influencer la prise de décision et avoir un impact sur le contexte interprété (Chainey & Chapman, 2013).

Récemment, une quatrième dimension a également été proposée : l'**intelligence en tant que culture,** définie par Navarro comme "l'ensemble des initiatives et des ressources qui favorisent la prise de conscience de sa nécessité et fournissent une compréhension civique de sa réalité" (Payá-Santos, 2023).

Quelle que soit l'interprétation retenue, le renseignement vise à réduire l'incertitude intrinsèque à la condition humaine et la complexité du monde contemporain dans la prise de décision pour prévenir et éviter tout danger ou menace (Jordan, 2015).

Pour ce faire, le renseignement s'appuie sur des connaissances théoriques liées à la politique, à l'économie, aux relations internationales, à la sécurité, à la sociologie, à la technologie, à la psychologie, etc. Il est donc essentiel de présenter des équipes de qualité composées d'experts dans les différents domaines afin d'aborder les problèmes sous des angles multiples et de trouver des solutions plus efficaces grâce à une approche transversale.

L'aspect multidisciplinaire récent du renseignement est une conséquence de l'élargissement du concept de sécurité et de la complexité croissante du contexte sociétal où les menaces asymétriques et la cyberguerre sont de plus en plus courantes.

En revanche, l'une des plus anciennes qualités du renseignement est le secret de ses activités et des informations obtenues. Toutefois, l'utilisation croissante de sources ouvertes (OSINT) modifie cette perspective. En outre, la mondialisation et l'expansion de l'utilisation d'Internet ont également une incidence sur les conflits, qui sont de plus en plus transnationaux et nécessitent une coopération internationale en matière de renseignement. Cependant, la protection des sources, en particulier des sources humaines (HUMINT), reste un principe fondamental, tout comme la nécessité de préserver la discrétion dans le traitement des informations afin d'éviter les contre-mesures, la désinformation ou la violation d'opérations sensibles.

En bref, on pourrait établir que le renseignement englobe le processus, le produit et l'institution qui réalise la collecte, l'évaluation et le traitement de l'information (Knight,

2024) en tant qu'outil de prise de décision, afin d'identifier, d'avertir et de prévenir les risques et les menaces, en réduisant l'incertitude (Francisco & Barrilao, 2019). Pour y parvenir, ces tâches doivent être réalisées de manière intentionnelle, opportune, planifiée, "secrète" et organisée (Andric & Terzic, 2023).

2.1. LES TYPES D'INTELLIGENCE

Il existe plusieurs classifications de l'intelligence, mais l'une des plus courantes est celle qui dépend du support dans lequel l'information est trouvée, établissant les types suivants (Kamiński, 2019) :

- **SIGINT** (*Signal Intelligence*) : il s'agit de renseignements obtenus à partir de l'interception de signaux, quelle que soit la manière dont ils sont transmis. Il existe trois sous-catégories : le renseignement sur les communications (COMINT), le renseignement électronique (ELINT) et le renseignement sur les instruments étrangers (FISINT). Il est particulièrement utile pour surveiller les menaces numériques et les conflits hybrides.
- **MASINT** *(Measurement and Signature Intelligence)* : basé sur la mesure d'attributs physiques, tels que les émissions électromagnétiques, les propriétés chimiques ou les caractéristiques acoustiques. Il est utilisé dans le cadre d'opérations militaires avancées et de détection d'armes afin de caractériser, localiser et identifier des cibles.
- **HUMINT** (*Human Intelligence)* : il s'agit de la plus ancienne méthode de collecte d'informations à partir de sources humaines, que ce soit par le biais d'entretiens, d'observations directes, d'infiltrations ou de collaborations avec des acteurs locaux. Elle est essentielle dans les contextes où les technologies ne peuvent y accéder.
- **GEOINT** *(Geospatial Intelligence)* et **IMINT** *(Imagery Intelligence) :* renseignement géospatial et renseignement d'imagerie. Le premier combine des cartes, des données géographiques et des informations de télédétection, tandis que le second se concentre sur l'analyse visuelle d'images satellites, aériennes ou de drones.
- **OSINT** *(Open-Source Intelligence)* : renseignements dérivés d'informations du domaine public sous forme physique, analogique ou numérique dans différents médias, tels que la radio, la télévision, les journaux, les magazines, Internet, les bases de données commerciales, les vidéos, les graphiques, les dessins, les réseaux sociaux, etc. rapports ouverts ou publics. Leur volume, leur accessibilité et leur utilité ont augmenté de façon exponentielle avec l'internet (Stewart Bertram, 2015).
- **SOCMINT** *(Social Media Intelligence*) : il s'agit parfois d'une sous-catégorie de l'OSINT, axée sur les médias sociaux. Il est utilisé pour surveiller les tendances, détecter les menaces émergentes, analyser les perceptions et suivre des acteurs spécifiques (Mahood, 2015).

Cependant, une autre typologie très répandue est celle de leur objectif : stratégique, tactique et opérationnel (Gruszczak, 2018).

- **Veille stratégique : elle** se concentre sur l'identification des risques, des menaces et des opportunités afin de soutenir la définition des objectifs et la prise

de décision, en tenant compte de l'environnement, des acteurs concernés et des évolutions possibles.

- **Renseignement tactique** : se concentre sur la planification et l'exécution d'opérations spécifiques pour atteindre un objectif de portée limitée, dérivé des objectifs généraux du renseignement stratégique.
- **Renseignement opérationnel** : également appelé renseignement opérationnel dans le domaine militaire, il a pour but de permettre l'organisation et l'exécution d'activités pour remplir une mission spécifique (Jiménez Villalonga, 2018).

La coexistence et la complémentarité de ces catégories permettent de construire une intelligence globale, adaptée aux différents niveaux de décision.

2.2. ÉVOLUTION DES APPROCHES ET DES STRATÉGIES EN MATIÈRE DE RENSEIGNEMENT

De nombreux auteurs affirment que le renseignement est aussi vieux que l'histoire de l'humanité, étant donné que la dissimulation d'informations confidentielles et la découverte de celles de l'adversaire ont toujours été des outils permettant d'atteindre et de conserver le pouvoir. En témoignent des civilisations comme la Chine antique avec la sagesse millénaire du maître Sun Tzu (Navarro Bonilla, 2005) ou la Grèce classique avec les procédures de transmission d'informations secrètes d'Énée le tacticien (Vela Tejada, 1993).

À l'origine, le renseignement était un outil au service du pouvoir politique, avec un objectif éminemment militaire : connaître la force, la localisation et les capacités de l'ennemi afin de faciliter la prise de décision du dirigeant. Cependant, à mesure que les sociétés sont devenues plus complexes, leurs menaces se sont accrues, ce qui a conduit à l'élargissement progressif du renseignement vers des aspects sociaux, économiques ou politiques. Ainsi, les activités de renseignement ont pris un rôle crucial avec la naissance des Etats et des relations entre eux, dans le but de défendre et de protéger les intérêts nationaux (Andric & Terzic, 2023).

Cependant, ce n'est qu'au milieu du XXe siècle, notamment après les deux guerres mondiales et la guerre froide, que les puissances mondiales ont commencé à organiser formellement leurs services de renseignement (les États-Unis avec la CIA, le Royaume-Uni avec le MI6 et Israël avec le Mossad).

L'Espagne, bien que moins présente au niveau international dans ce domaine, a également tenté pour la première fois de mettre en place un service de renseignement à cette époque. Le Service central de documentation (SECED) a été créé en 1972 et le Centre supérieur d'information de défense (CESID) en 1977, mais ce n'est qu'en 2002 que l'actuel CNI (Centre national de renseignement, 2023) a été fondé.

À partir de là, la révolution technologique et l'explosion du volume d'informations disponibles ont marqué un changement radical : le renseignement a cessé d'être un domaine fermé et exclusivement centré sur l'État pour devenir une activité transversale et dynamique dont les implications dépassent la sphère politico-militaire. Bien que l'essence du renseignement reste la même, les méthodes, le calendrier et les objectifs ont subi de profondes transformations. L'accès massif aux données par le biais de sources ouvertes, l'accélération des flux d'information et la mondialisation des menaces ont réduit le cycle

de vie de l'information et remis en question le rôle central qu'occupait auparavant le secret (Payá-Santos, 2023).

Ce nouveau contexte a été aggravé par les attentats du 11 septembre, qui ont marqué un tournant, soulignant la nécessité d'identifier et de prévenir les menaces asymétriques et transnationales, brouillant la distinction classique entre renseignement interne et externe, et poussant les institutions policières à adopter des modèles plus analytiques, préventifs et collaboratifs (Knight, 2024).

Avec l'extension progressive du renseignement à d'autres domaines stratégiques, tels que le maintien de l'ordre, qui fonctionnait historiquement avec une logique réactive, les fonctions policières ont commencé à évoluer de manière significative. Son approche classique, axée sur la réponse aux crimes accomplis ou aux demandes de service, a été remise en question à mesure que les changements sociétaux et la complexité croissante de la criminalité exigeaient de nouvelles formes d'intervention (Organisation pour la sécurité et la coopération en Europe, 2017). Par la suite, divers courants philosophiques ont influencé le maintien de l'ordre, tels que (Gkougkoudis et al., 2022) :

- ***Community Policing* ou *Community-oriented policing* (COP) :** priorité à la coopération entre les citoyens et les forces de l'ordre, favorisant la confiance et la prévention (Carter & Fox, 2019).
- **Police de *résolution des problèmes*** : elle vise à identifier et à analyser les problèmes sous-jacents à la criminalité dans une perspective plus large et transversale et à rechercher des solutions structurelles et durables (Organisation pour la sécurité et la coopération en Europe, 2017).
- ***Police de tolérance zéro* :** réponse stricte aux infractions, même mineures, basée sur les idées développées par deux criminologues américains, James Q. Wilson et George Kelling, qui ont publié en 1982 un article intitulé "Broken Windows" (Grabosky, 1999).

Cependant, au cours des dernières décennies, en raison de la complexité des menaces et des risques, de nombreux universitaires et praticiens ont souligné que l'approche holistique la plus efficace pour lutter contre la mondialisation de la criminalité est l'*Intelligence-Led Policing* (ILP), qui se traduit par une police fondée sur le renseignement. Cette approche est apparue dans les années 1990 au Royaume-Uni comme une stratégie visant à améliorer l'efficacité fiscale des services de police, c'est-à-dire à optimiser l'allocation des ressources, la productivité opérationnelle et la qualité des résultats de l'action policière. Initialement mise en œuvre principalement pour lutter contre la grande criminalité et la criminalité organisée, elle a depuis évolué à l'échelle mondiale pour devenir un modèle proactif, fondé sur l'analyse des données et axé sur la prévention, la réduction et la perturbation de tous les types de criminalité. Aux États-Unis, ce sont les événements du 11 septembre 2001 qui ont finalement motivé son adoption, en concentrant son approche sur des formes plus complexes de criminalité (Summers & Rossmo, 2019).

L'ILP est une philosophie proactive visant à identifier et à prévenir les problèmes criminels à l'aide de données brutes et d'analyses mixtes (quantitatives et qualitatives), mais il ne s'agit pas d'une tactique ponctuelle, mais d'un cadre flexible, adaptatif et durable fondé sur des données objectives (Carter & Fox, 2019). Toutefois, sa mise en œuvre se heurte à des défis en termes de clarté terminologique et d'intégration des données, ainsi

qu'à la nécessité de garantir le respect des droits de l'homme dans la gestion du renseignement.

Parallèlement, le modèle de renseignement fondé sur les activités (ABI) a élargi les capacités d'analyse, en particulier face aux menaces émergentes. Ce modèle, dont les origines remontent à la guerre froide, a été développé en raison de la nécessité de gérer et d'analyser d'énormes volumes de données générées par les technologies modernes, telles que les drones et les médias sociaux, en particulier dans le contexte de la lutte contre le terrorisme. Les méthodes d'analyse traditionnelles se sont révélées inadaptées à ce nouvel environnement, car les analystes passent trop de temps à rechercher des informations et à surveiller des cibles connues, ce qui limite leur capacité à découvrir l'inconnu. L'ABI améliore ce processus en permettant la corrélation en temps réel de données provenant de diverses sources, surmontant ainsi les limites des méthodes traditionnelles de renseignement, de surveillance et de reconnaissance (ISR) (Atwood, 2015).

Une autre approche pertinente est le modèle 3i proposé par Ratcliffe en 2006, qui repose sur trois piliers fondamentaux : "interpréter", "influencer" et "avoir un impact" sur l'environnement criminel. Les analystes doivent interpréter activement l'environnement, influencer les décideurs qui, à leur tour, utilisent ces renseignements pour concevoir des stratégies qui affectent l'environnement criminel (Budhram, 2015). En 2016, il a ajouté un i supplémentaire, celui de l'intention, comme le montre la figure 1, soulignant la nécessité de clarifier et de comprendre les objectifs fixés (Organisation pour la sécurité et la coopération en Europe, 2017).

Chiffre 1

Le modèle des 4 i de Ratcliffe : intention, interprétation, influence et impact

Note : Adapté de *OSCE Guidance on Intelligence-led Policing (p. 24), par OSCE, 2017, OSCE.*

Police fondée sur le renseignement (p. 24), par l'OSCE, 2017, OSCE

En bref, le renseignement est passé d'une activité très secrète et centralisée à un processus transversal, interdisciplinaire, distribué et soutenu par la technologie. Cette évolution justifie le besoin de nouveaux modèles tels que l'IDEM, qui intègrent l'analyse humaine et le traitement automatisé pour faire face aux menaces modernes, en particulier dans le cyberespace. En outre, cette trajectoire nous permet d'observer une convergence croissante entre les logiques de sécurité, de défense et de technologie, positionnant le renseignement comme un élément clé de la souveraineté numérique et de la résilience institutionnelle.

3. LE CYCLE DU RENSEIGNEMENT

Bien que l'on attribue souvent à Sherman Kent la formulation scientifique de la méthode de renseignement, des recherches ultérieures ont montré qu'une méthodologie rigoureuse et un ensemble complet d'opérations (ce que l'on a appelé plus tard le cycle du renseignement) avaient déjà été esquissés, par exemple, pendant la guerre civile espagnole (Navarro Bonilla, 2004).

Le cycle du renseignement regroupe toutes les activités qui permettent de transformer l'information brute en renseignement et, comme son nom l'indique, il est de nature cyclique. Le cycle de renseignement classique comporte quatre phases, mais dans certains pays, des phases différentes ou des sous-phases différenciées sont ajoutées. Par exemple, en Espagne, le CCN-CERT établit six phases pour le cycle du renseignement : orientation et planification ; collecte ; transformation ; analyse et production ; diffusion et, enfin, évaluation (National Cryptologic Centre, 2015).

- La première phase, appelée **orientation et planification**, établit le quoi et le comment, c'est-à-dire les exigences du produit de renseignement à produire et les actions à entreprendre pour l'obtenir. L'objet de l'étude, la portée, les objectifs, le délai et le type de rapport doivent être clairs pour que le travail dans les autres phases soit efficace et aboutisse à une qualité supérieure et conforme aux normes juridiques nationales et internationales (Organisation pour la sécurité et la coopération en Europe, 2017).
- L'étape suivante, la **collecte, consiste à** recueillir des données brutes, par exemple à partir des sources mentionnées ci-dessus (SIGINT, MASINT, HUMINT, GEOINT, IMINT, OSINT). Ce processus est complexe, car les analystes doivent trouver le juste équilibre entre la collecte de toutes les données nécessaires et suffisantes et la surcharge d'informations redondantes. Pour ce faire, ils doivent être conscients de l'existence, de la pertinence, de l'accessibilité et de la fiabilité des sources sélectionnées, ainsi que des contraintes juridiques et des exigences en matière d'autorisation (Organisation pour la sécurité et la coopération en Europe, 2017). En outre, la validité et l'exactitude des informations doivent être évaluées avant de passer aux autres étapes du cycle du renseignement.
- Dans la phase de **transformation**, les données brutes collectées à l'étape précédente sont converties en ensembles structurés tels que des bases de données, des références bibliographiques, etc. Cette étape consiste à cataloguer, hiérarchiser et référencer les informations collectées.
- La quatrième phase, l'**analyse et la production**, se compose des activités par lesquelles les informations transformées sont intégrées, évaluées, analysées et préparées afin d'obtenir le produit final. Au sein de cette phase, deux sous-phases peuvent être établies : la première consiste à intégrer les données obtenues de différentes sources afin d'établir des hypothèses et d'identifier un modèle de renseignement ; la seconde consiste à interpréter les données, c'est-à-dire à aller au-delà des informations obtenues, en réfutant ou en soutenant les hypothèses préétablies (Organisation pour la sécurité et la coopération en Europe, 2017). Généralement, cette phase aboutit à ce que l'on appelle le *renseignement actionnable, un* produit de renseignement qui répond aux exigences définies dans la phase de pilotage et de planification et donc aux besoins du consommateur. Ce produit peut à son tour être de plusieurs types, tels qu'une analyse de tendance, une évaluation à long terme, un renseignement d'actualité,

un renseignement d'estimation ou d'alerte, etc. (National Cryptologic Centre, 2015).

- Au stade de la **diffusion**, le produit final est livré au consommateur qui l'a demandé et, si nécessaire et légalement admissible, il sera également partagé avec d'autres parties prenantes.
- La dernière phase correspond à l'**évaluation**, qui permet un retour d'information continu sur toutes les phases précédentes du cycle du renseignement et sur les résultats obtenus, ce qui permet d'ajuster et d'affiner à la fois les activités individuelles et le cycle dans son ensemble. Cela est particulièrement utile pour répondre de manière optimale à l'évolution des besoins en matière de renseignement.

Cependant, de nombreux experts remettent en question ce modèle traditionnel de l'intelligence et l'une des critiques formulées est la simplification excessive de ce modèle par rapport à la grande complexité du processus réel d'acquisition de l'intelligence. Robert Clark souligne que ce terme "est devenu un concept théologique : personne ne remet en question sa validité", même s'il ne décrit pas les étapes précises à suivre (Phythian et al., 2013).

En outre, Arthur Hulnick souligne que l'idée selon laquelle les clients des services de renseignement guident les producteurs au début du cycle est erronée, car les clients s'attendent souvent à être alertés par le système de renseignement, de sorte que le processus de collecte est principalement motivé par la nécessité de combler les lacunes en matière de données et non par des orientations politiques (Pothoven et al., 2023).

Par ailleurs, les organismes de collecte de données ne sont pas toujours sollicités ; souvent, les bases de données existantes, alimentées depuis des années, sont consultées directement pour préparer un rapport. Ou encore, de nouvelles données brutes peuvent être demandées aux équipes qui les collectent, mais une nouvelle demande de renseignements n'est généralement pas formulée au niveau du client (Jordán, 2011).

Quant à la phase d'analyse, sa définition au sein du cycle du renseignement n'est pas critiquée en soi, mais il est indiqué que c'est l'étape au cours de laquelle la plupart des erreurs sont commises, non pas en raison d'un manque d'informations, mais plutôt le contraire, en raison d'une surcharge de données qui conduit à ce que des informations pertinentes soient ignorées ou interprétées de manière inadéquate par les analystes (Jordán, 2016). Les analystes doivent être conscients de leurs propres processus mentaux et de leurs erreurs potentielles, en évitant les simplifications cognitives involontaires et, bien sûr, les préjugés. En outre, dans certains cas, comme dans les situations de crise, les données brutes arrivent directement sans passer par cette phase.

Quant à la phase de diffusion, elle n'est parfois pas non plus franchie, car toutes les analyses produites ne parviennent pas aux consommateurs. Beaucoup ne sont pas lues par les destinataires et sont stockées directement dans la base de données interne. Dans d'autres cas, les clients ont souvent déjà pris leurs décisions et ignorent les informations qui ne les soutiennent pas.

De même, en ce qui concerne le cycle du renseignement en général, sa définition en tant que séquence de phases finalement disposées de manière circulaire est critiquée, alors qu'il s'agit d'un processus plus dynamique, où toutes les phases s'alimentent les unes les autres et peuvent avancer et reculer dans n'importe quelle direction au sein du cycle. Elle met également en évidence des problèmes d'organisation, de commandement et de

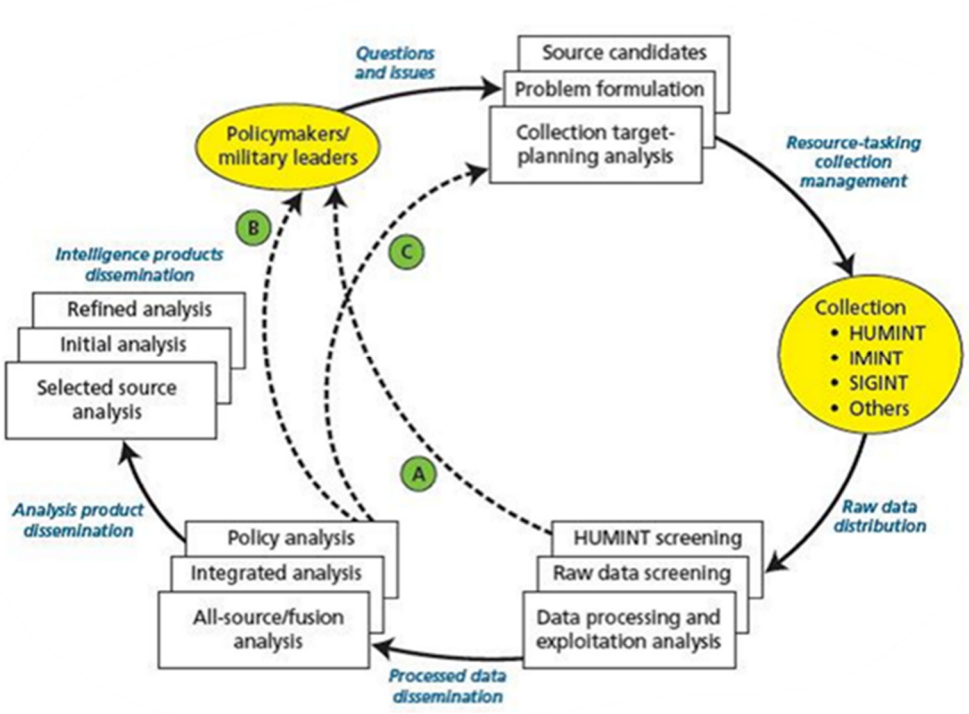
circulation de l'information qui entraînent un manque de flexibilité dans l'action et la communication, ralentissant les processus de prise de décision (Organisation pour la sécurité et la coopération en Europe, 2017).

Des commentateurs tels que Peter Gill et Mark Phythian affirment que le concept de cycle du renseignement a été rendu obsolète par les avancées technologiques, la révolution de l'information et l'évolution des menaces et des cibles. Ils proposent de le remplacer par un "réseau de renseignement" qui reflète mieux les interactions complexes entre le ciblage, la collecte et l'analyse, et met en évidence les facteurs contextuels qui influencent le processus et peuvent être affectés par ses résultats (Pothoven et al., 2023).

D'autre part, plusieurs auteurs ont tenté de saisir la complexité du cycle du renseignement dans des schémas alternatifs au schéma traditionnel. Comme le montre la Figure2 , Treverton et Gabbard proposent une approche plus réaliste qui inclut des raccourcis entre les phases, montrant que certaines étapes sont parfois manquées, par exemple que des informations non analysées peuvent parvenir directement aux décideurs. Mark Lowenthal présente un cycle composé de rétroactions constantes, où les nouveaux besoins et les ambiguïtés réactivent le processus, le rendant plus dynamique et multicouche, comme on peut le voir surFigure3 . Robert M. Clark présente le concept de *renseignement centré sur la cible*, un modèle collaboratif et axé sur la cible, dans lequel tous les participants construisent ensemble une image partagée de la question de renseignement qui les intéresse, représentée dans la Chiffre 4 (Jordan, 2016).

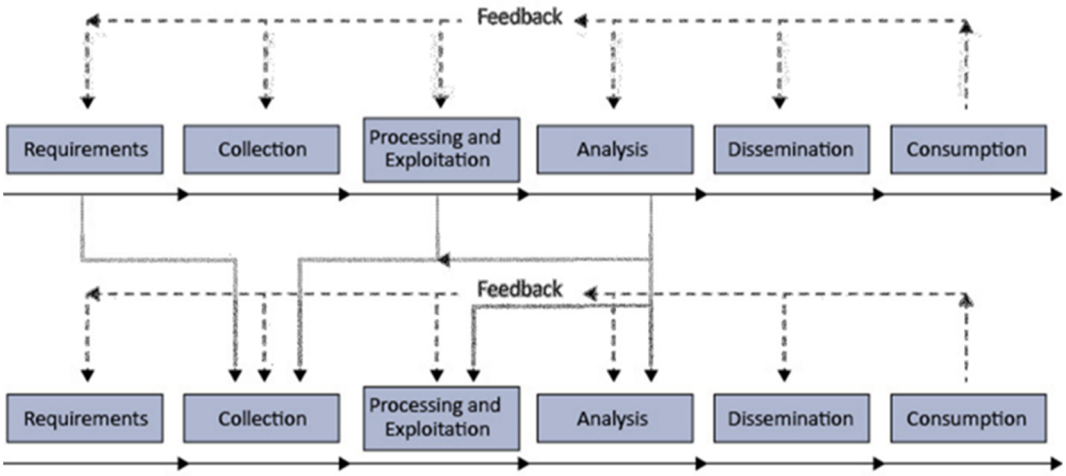
Figure2

L'approche de Treverton et Gabbard



Note : Tiré de *A Review of the Intelligence Cycle* (p. 4) par J. Jordán, 2016, *Analyse GESI (Grupo de Estudios En Seguridad Internacional)*, 2.

Figure3
Processus multi-strates Mark Lowenthal



Note : Tiré de *A Review of the Intelligence Cycle* (p. 5) par J. Jordán, 2016, *Analyse GESI (Grupo de Estudios En Seguridad Internacional)*, 2.

Chiffre 4
Target-Centric Intelligence par Robert M. Clark

Note : Tiré de *A Review of the Intelligence Cycle* (p. 6) par J. Jordán, 2016, *Analyse GESI (Grupo de Estudios En Seguridad Internacional)*, 2.

Enfin, des propositions telles que le concept JISR (Joint Intelligence, Surveillance and Reconnaissance) de l'OTAN ont également vu le jour. Ce terme désigne l'ensemble intégré de capacités de renseignement et d'opérations qui synchronise et intègre la planification et l'exécution de toutes les capacités de collecte de renseignements, ainsi que leur traitement, leur exploitation et leur diffusion. Ce concept découle de la nécessité d'améliorer le partage des informations et des renseignements pour prévenir les crises, les menaces terroristes, les activités criminelles transnationales et les cybermenaces

(Gruszczak, 2018). Le renseignement, la surveillance et la reconnaissance (ISR) ont toujours été des activités essentielles des opérations militaires, mais elles étaient divisées selon les niveaux de commandement (stratégique, opérationnel et tactique), ou selon les différentes disciplines du renseignement, en fonction du type et de la complexité des sources d'information concernées. Dans le contexte actuel, cette division limite l'utilisation optimale des spécialistes, des agences, des sources et des activités de renseignement. C'est pourquoi le modèle JISR est proposé, dans lequel les activités de renseignement, de surveillance et de reconnaissance fonctionnent comme une seule unité, s'intégrant à tous les niveaux et dans tous les domaines (ministère de la défense, 2023).

Cependant, le modèle JISR présente le même processus que l'ISR, qui se compose de cinq phases : planification, collecte, traitement, exploitation et diffusion (TCPED). La principale différence avec le cycle traditionnel du renseignement est que ce processus n'est ni linéaire ni circulaire, mais que les différentes étapes sont exécutées de manière dynamique, séquentielle, simultanée ou indépendante, en fonction du résultat recherché. Toutefois, dans ce modèle, le processus ISR est généralement aligné sur la phase de collecte du cycle du renseignement, et les résultats de cette collecte sont incorporés dans la phase de traitement, tout en soutenant le cycle de décision.

Toutefois, cette approche est également confrontée à plusieurs limites. Tout d'abord, les ressources peuvent être insuffisantes pour répondre à toutes les exigences, notamment en raison de la forte demande et de la faible disponibilité de certaines capacités de collecte. Il existe également des problèmes techniques tels que les limites de la puissance de calcul et de la bande passante, qui affectent la capacité de traitement et de diffusion des résultats. Les adversaires peuvent interférer par des attaques sur les capacités de RSR, le camouflage, la dissimulation et la désinformation. En outre, l'accès au DSI peut être limité par des obstacles physiques, cognitifs, virtuels, juridiques et politiques (ministère de la défense, 2023).

Aujourd'hui, le renseignement en tant que processus devrait donc s'éloigner des modèles linéaires et cycliques traditionnels pour s'orienter vers des structures plus fluides et en réseau, capables de répondre avec agilité aux menaces émergentes et de tirer parti du vaste volume de données disponibles (Jiménez Villalonga, 2018).

4. PROPOSITION D'ACTUALISATION DU CYCLE DU RENSEIGNEMENT À L'ÈRE NUMÉRIQUE : LE MODÈLE IDEM

Le cycle classique du renseignement a constitué pendant des décennies l'épine dorsale du renseignement en tant que processus. À l'époque, cette représentation séquentielle était logique, car elle facilitait la normalisation, la formation des analystes et la gestion des opérations. Toutefois, le modèle présente des limites importantes lorsqu'il est transposé dans les contextes actuels de complexité, d'incertitude et d'évolution rapide, en particulier dans des domaines tels que le cyberespace.

Dans cet environnement extrêmement dynamique, le renseignement est devenu un outil essentiel pour comprendre et anticiper les menaces, en particulier dans le domaine numérique. À mesure que les organisations étendent leur présence dans le cyberespace pour maximiser leur visibilité et leur portée, elles augmentent également leur exposition à des attaques potentielles. Cette transformation exige de repenser le rôle du

renseignement au-delà de sa formulation classique, en l'adaptant aux particularités d'un environnement décentralisé, interconnecté et en constante évolution.

Toutefois, cette adaptation n'est pas simple. La prolifération des termes et des approches reflète à la fois la jeunesse du domaine et son expansion rapide. Dans certains cadres conceptuels, le terme cyberintelligence ou CYBINT est utilisé comme un sous-type de COMINT (Jiménez Villalonga, 2018), mais il pourrait également être considéré comme un type de renseignement supérieur qui englobe et coordonne les activités OSINT, SIGMINT, SOCMINT et même HUMINT (Portillo, 2019).

Dans le contexte européen, il est plus courant de parler de renseignement sur les cybermenaces (CTI), qui désigne l'application systématique du renseignement pour identifier, analyser et atténuer les menaces qui pèsent sur le cyberespace. Selon Gartner (Lee, 2023), le renseignement sur les cybermenaces repose sur des connaissances factuelles qui fournissent un contexte, des mécanismes, des indicateurs et des conseils pratiques sur les menaces émergentes ou existantes.

C'est pourquoi la CTI joue un rôle crucial en aidant les organisations à développer une stratégie de sécurité proactive qui leur permet de comprendre et d'anticiper les tactiques, techniques *et* procédures (TTP) des adversaires. Elle facilite également l'identification des menaces à la source et la réponse efficace aux incidents avant qu'ils ne causent des dommages importants.

Cependant, lorsqu'il s'agit de mettre en œuvre des systèmes de recherche ou de travail dans ce domaine, il manque encore des cycles méthodologiques spécifiques et largement acceptés pour structurer le processus de collecte et d'analyse du renseignement cybernétique. Par conséquent, on a tendance à se rabattre sur le cycle traditionnel du renseignement ou sur l'une des approches alternatives existantes. Mais, comme nous l'avons vu, toutes ces approches présentent des limites importantes quant à leur application efficace dans les environnements numériques.

Le **modèle classique** est rigide et séquentiel ; le **modèle proposé par Treverton et Gabbard** permet une certaine flexibilité, mais manque de rétroaction claire ; le **modèle centré sur la cible** propose un cycle continu plus proche de la cible, mais sans structure réellement flexible entre les phases ; et l'**approche multiniveaux de Lowenthal** introduit du dynamisme, mais maintient une certaine linéarité et les connexions bidirectionnelles entre les phases ne sont pas entièrement comprises.

Tableau 1
Tableau comparatif des différents modèles de représentation de l'intelligence en tant que processus

	Modèle classique	Modèle Treverton et Gabbard	Modèle de Mark Lowenthal	Modèle centré sur la cible
Structure	Linéaire ou cyclique (phases successives dans un cercle)	Semi-linéaire (avec des "raccourcis" possibles)	Multi-niveaux (avec des couches actives si nécessaire)	Cyclique (ciblé)
Début du processus	À la demande du consommateur	Semblable à la méthode classique, mais permet de redémarrer à partir de phases intermédiaires.	De nouveaux besoins à la réactivation de phases antérieures	A partir de l'analyse de la cible (à partir d'une analyse précédente ou de nouveaux besoins et informations)
Principales phases	Pilotage et planification, collecte, traitement, analyse et production, diffusion, évaluation	Similaire au modèle classique, mais sans ordre strict ni mention de retour d'information.	Identique à la méthode classique, avec des cycles internes et un *retour d'information* continu.	Les besoins et les *lacunes*, la collecte, l'analyse et la diffusion sont étroitement liés à l'objectif suivant
Interaction entre les phases	Limité (retour d'information à la fin)	Moyen (linéaire avec raccourcis)	Décharge (continue et simultanée)	Moyenne (cycles connectés par la cible)
Flexibilité et adaptabilité	Faible (modèle rigide et séquentiel)	Moyen (une certaine fluidité, mais maintien de phases définies)	Élevée (orientée vers une reformulation permanente du processus)	Moyen : (dynamisme autour de la cible)
Diffusion de renseignements	A la fin du processus	Peut être omis ou avancé si le produit l'exige.	Elle peut se produire à différents niveaux et à différents moments, en fonction du cycle interne activé.	Fin du processus, après la phase de production
Retour d'information	A la fin du processus	Pas de référence explicite	À tous les stades	Pas de référence explicite

C'est pourquoi ce travail propose le modèle de renseignement IDEM (Enhanced Dynamic Enriched Intelligence) avec une approche en réseau, non linéaire et hautement adaptative, dans laquelle les phases du processus de renseignement ne se succèdent pas de manière séquentielle, mais interagissent de manière dynamique, flexible et continue, permettant un retour d'information constant entre les phases et les équipes de travail.

Alors que le modèle traditionnel commence par la **direction et la planification,** où les exigences en matière de renseignement sont établies en fonction des besoins du décideur, le modèle IDEM propose de commencer par une phase d'**identification et de hiérarchisation des menaces** en temps réel. L'une des critiques les plus récurrentes du cycle traditionnel est son manque de flexibilité, car une fois les objectifs définis, le processus tend à suivre une trajectoire fixe, ce qui est inefficace dans le contexte actuel, où les menaces évoluent rapidement et ne sont pas toujours alignées sur les besoins précédemment établis. Par conséquent, l'objectif de cette phase devrait être de détecter et de hiérarchiser les menaces émergentes de manière proactive, sans s'appuyer uniquement sur les orientations initiales des consommateurs, qui souvent n'arrivent pas à temps ou ne

sont pas formulées du tout. Cette phase deviendrait un processus dynamique et continu en soi, alimenté par une surveillance constante, une reconnaissance en temps réel des modèles de menaces émergentes et la capacité de réorienter rapidement les efforts de renseignement à mesure que de nouvelles menaces ou des changements de conditions apparaissent (Dahj, 2022).

La phase suivante, la **collecte**, reste fondamentale pour le renseignement en tant que processus, car sans données ni informations, il est impossible d'obtenir des connaissances exploitables. Dans le modèle classique, l'un des plus grands défis consistait à filtrer efficacement de grands volumes de données pour éviter à la fois la saturation de l'information et la perte d'informations critiques. À l'ère numérique, cette tâche est devenue encore plus complexe en raison de l'augmentation exponentielle du nombre de sources et de données disponibles, sous l'effet des nouvelles technologies, de la mondialisation et de la courte durée de conservation de l'information. L'IDEM s'attaque à cette complexité en utilisant des technologies avancées telles que l'*apprentissage* automatique et l'intelligence artificielle, qui permettent une collecte automatisée, continue et complète. Bien qu'ils traitent des volumes nettement plus importants, ces outils permettent de filtrer, de hiérarchiser et d'enrichir les informations en temps réel, garantissant ainsi leur pertinence et leur utilité.

Dans cette approche, il n'est pas utile d'établir une phase spécifique pour la **transformation des** données comme dans le modèle classique. Grâce à des technologies avancées, telles que le traitement du langage naturel (NLP*)* et les outils d'analyse des *big data*, la conversion des données brutes en informations pertinentes et contextualisées peut se produire simultanément à plusieurs stades du processus. Les données peuvent ainsi être traitées, structurées et analysées en parallèle, ce qui facilite une réponse agile aux nouvelles informations ou aux changements dans l'environnement.

En outre, la séparation entre la **transformation** et l'**analyse** peut entraîner un manque d'intégration et une perte de contexte pendant la transition. C'est pourquoi IDEM remplace ces deux phases du modèle classique par une étape unique de **contextualisation et d'enrichissement** qui se concentre sur la mise en contexte des données, l'interprétation de leur pertinence et la compréhension du lien avec d'autres événements et modèles. De cette manière, l'analyse peut être continuellement mise à jour et ajustée à mesure que de nouvelles données apparaissent et que de nouvelles questions se posent, développant ainsi une capacité d'adaptation continue. Il est également essentiel de traiter et d'intégrer des informations provenant de sources de données multiples, car elles facilitent une interprétation plus approfondie et plus efficace, en particulier dans le contexte actuel de menaces hybrides. Contrairement à l'approche traditionnelle, ainsi qu'aux systèmes ISR classiques, qui établit un processus individuel pour chaque type de source (OSINT, HUMINT, SIGINT, COMINT, etc.) (ministère de la défense, 2023), l'IDEM propose un modèle interconnecté et multi-capteurs, plus efficace dans la détection et l'analyse de phénomènes complexes, comme le suggère la doctrine JISR du ministère américain de la défense, discutée dans la section 2.2

En revanche, le modèle IDEM prévoit une étape spécifique pour la **production de** renseignements exploitables. Alors que, dans le cycle traditionnel, l'analyse et la production se concentrent sur la production de rapports et de recommandations qui aident à la prise de décision, IDEM préconise des produits qui ne sont pas seulement réactifs, mais aussi prédictifs, permettant l'anticipation d'événements et de tendances ou

l'évaluation d'impacts qui facilitent l'ajustement des stratégies et des décisions en temps réel. L'accent est mis ici sur l'intelligence en tant qu'aide à la décision dynamique, et non en tant que produit fermé.

Parallèlement au développement de toutes ces phases, la phase de **retour d'information** définie dans le cycle de renseignement traditionnel est indispensable, mais réinterprétée comme un processus transversal. Pour assurer une amélioration continue et un processus plus efficace, il est crucial que les points d'amélioration ou les faiblesses soient mis en évidence tout au long de chacune des phases. Cela permettra de prendre en compte ces observations non seulement dans les étapes suivantes, mais aussi dans les recherches futures, plutôt que d'attendre l'obtention du produit de renseignement final, comme c'est le cas dans le modèle traditionnel.

Enfin, dans le cycle traditionnel, la **diffusion** est réservée à la fin du processus, une fois que le rapport de renseignement a été produit. IDEM rompt avec cette logique en proposant une diffusion modulaire et progressive, en partageant non seulement le renseignement en tant que tel, mais aussi les menaces reconnues et classées dans la phase d'identification et de hiérarchisation, ou les données collectées à partir des différentes sources disponibles, ou encore les données contextualisées et enrichies dans différents formats. Il est évident que cette diffusion précoce doit être gérée avec soin, en assurant la protection des sources pour éviter les contre-mesures et la désinformation de la part des cibles et pour protéger les sources humaines (HUMINT). Toutefois, la nature transnationale des crimes actuels exige une coopération internationale entre les différents services de renseignement et, par conséquent, un échange d'informations entre eux en temps utile et sans retard pour obtenir des résultats plus efficaces.

Cependant, malgré les capacités techniques offertes par l'automatisation, le rôle de l'analyste humain reste essentiel à chacune des étapes décrites ci-dessus. Les outils automatisés fonctionnent selon des paramètres et des algorithmes définis par leurs programmeurs, qui sont réellement capables d'interpréter les informations dans un contexte plus large, en tenant compte des facteurs culturels, politiques et situationnels. En outre, les modèles prédictifs manquent de flexibilité cognitive pour gérer les ambiguïtés, les contradictions ou les exceptions et peuvent échouer face à des entrées erronées, des données biaisées ou des situations imprévues.

Les analystes, en revanche, sont capables de s'adapter, d'innover et de réajuster leurs approches en réponse à de nouveaux paradigmes, alors que les modèles d'intelligence artificielle ont besoin d'une grande quantité de données d'entraînement pour pouvoir développer de nouvelles méthodologies d'analyse et ne sont pas en mesure d'appliquer des approches créatives si de nouvelles questions se posent. Cette capacité des humains à collaborer au sein des équipes, à discuter des interprétations, à restructurer les stratégies sur la base du *retour d'information* reçu est essentielle à la réussite de la mise en œuvre des stratégies de renseignement (Jordan, 2011).

Tableau 2
Tableau comparatif du modèle classique et du modèle IDEM proposé

	Modèle classique	Modèle IDEM (proposition propre)
Structure	Linéaire ou cyclique (phases successives dans un cercle)	Modulaire, dynamique et en réseau (cercles concentriques et interconnectés)
Début du processus	À la demande du consommateur	Proactive, sans demande préalable
Principales phases	Pilotage et planification, collecte, traitement, analyse et production, diffusion, évaluation	Identification et hiérarchisation, collecte, contextualisation et enrichissement, production de renseignements, retour d'information et diffusion.
Interaction entre les phases	Limité (retour d'information à la fin)	Décharge : phases interactives et bidirectionnelles
Flexibilité et adaptabilité	Faible (modèle rigide et séquentiel)	Très élevé (phases simultanées et réinitialisables)
Diffusion de renseignements	A la fin du processus	transversale et continue dès les premières étapes du processus
Retour d'information	A la fin du processus	Constante : à tous les stades
Technologie appliquée	Non explicitement couvert	Intégration de technologies avancées (IA, ML, NLP, *big data*)
Participation humaine	Central, mais hiérarchique	Combinaison synergique d'un analyste humain et d'outils automatisés
Applicabilité dans les environnements numériques	Limitée	Élevé (orienté vers les cybermenaces et les scénarios complexes)

Voici un schéma représentatif du modèle IDEM, dans lequel les différentes phases sont disposées en cercles concentriques. Cette disposition reflète, d'une part, la proximité croissante du produit final de renseignement à mesure que l'on se rapproche du centre et, d'autre part, la nature constante de toutes les étapes, puisque les phases les plus internes sont contenues dans les phases externes. Toutefois, le modèle n'établit pas un parcours linéaire, il n'est pas nécessaire de passer par toutes les étapes pour atteindre le centre. Ce caractère dynamique est représenté par des flèches indiquant les flux possibles d'entrée et de sortie entre les différentes étapes, ce qui permet des transitions directes et bidirectionnelles en fonction des besoins du contexte.

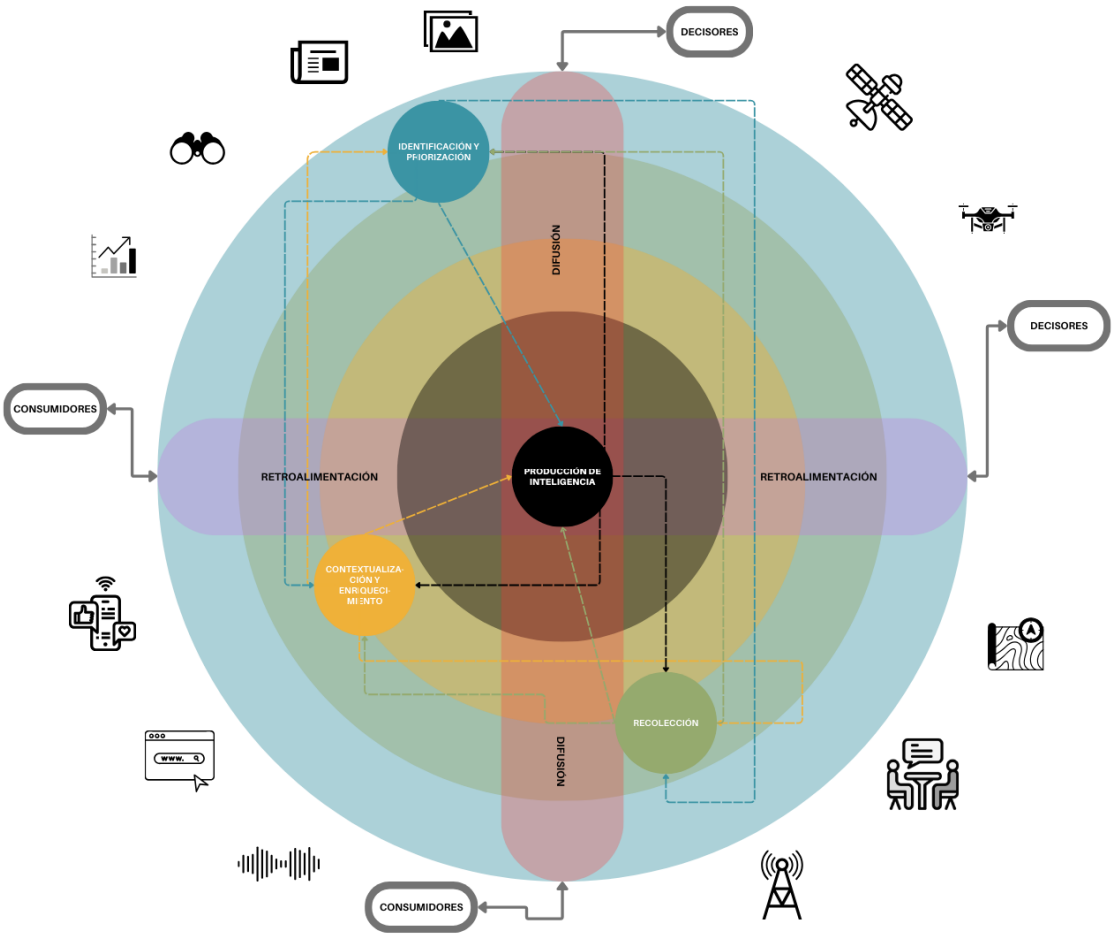
Perpendiculairement à ces cercles et perpendiculairement l'un à l'autre, deux éléments clés sont intégrés, représentés par des rectangles transversaux. Le premier représente la phase de retour d'information, transversale à toutes les phases et opportune pour l'amélioration continue de l'ensemble du cycle. Le second symbolise la phase de diffusion, également collatérale à toutes les étapes et essentielle pour obtenir des produits plus complets et des résultats plus efficaces.

À l'extérieur du schéma se trouvent les consommateurs et les décideurs. Leur nombre et leur importance dépendent à la fois des besoins en matière de renseignement et de l'impact escompté de l'analyse effectuée. Ces personnages sont représentés par des flèches bidirectionnelles, qui indiquent leur double fonction : établir la cible et les critères

du renseignement, tout en recevant des informations en retour ou des produits de renseignement pour faciliter leur prise de décision.

Des icônes provenant de différentes sources d'information sont également incorporées, soutenant ainsi la stratégie de collecte, de contextualisation et d'enrichissement des données provenant de différentes sources pour un processus de renseignement plus complet, plus transversal et plus efficace.

Chiffre 5
Modèle d'intelligence IDEM



Note : Élaboration propre, Paula Castro Castañer, 2024.

La combinaison de l'adaptabilité, de l'expérience, du jugement critique et du talent humain avec la capacité des machines à traiter de grands volumes de données crée une synergie qui garantit une prise de décision plus efficace, pluridisciplinaire, informée et flexible, tout en assurant une meilleure qualité et pertinence de l'information générée.

4.1. EXEMPLE PRATIQUE DE MISE EN ŒUVRE DU MODÈLE IDEM

Un exemple pratique illustrant l'utilité de l'application de ce modèle de renseignement est celui d'un fournisseur national d'énergie qui détecte une anomalie dans ses systèmes de contrôle SCADA. Dans cette situation, il n'y a pas encore d'incident confirmé ni de demande explicite de la part des décideurs (car ils ne sont probablement pas encore au

courant de cette situation), ce qui implique que l'activation du processus de renseignement se fait de manière proactive et autonome, sur la base de signaux identifiés dans l'environnement opérationnel. Toutefois, l'équipe de renseignement interne active le modèle IDEM afin d'anticiper s'il s'agit d'une menace réelle ou d'une fausse alerte.

L'IDS émet une alerte automatique concernant un trafic anormal vers les serveurs de sauvegarde, ce qui déclenche la phase d'identification et de hiérarchisation. Cette alerte, bien que préliminaire, est suffisante pour que l'équipe de renseignement interne classe la menace comme prioritaire, compte tenu de l'impact potentiel qu'une compromission de cette nature pourrait avoir sur l'infrastructure critique du pays. En conséquence, il est décidé de supprimer temporairement la priorité accordée aux enquêtes ouvertes sur les campagnes d'hacktivisme et à la surveillance géopolitique à faible impact, ainsi qu'à d'autres tâches de surveillance de routine dans les forums et canaux obscurs. Cette réorientation permet de concentrer les efforts humains et technologiques sur une seule hypothèse de travail : une éventuelle intrusion ciblée avancée.

La collecte est déclenchée simultanément à partir de multiples sources internes (journaux, SIEM, enregistrements d'authentification) et externes (flux de renseignements cybernétiques, bases de données d'indicateurs de compromission, alertes émanant d'entités coopérantes ou de fournisseurs de renseignements). Au cours de cette étape, lorsque des indices suggèrent des motivations économiques derrière l'attaque possible, comme, par exemple, l'extraction de données de marché au lieu d'informations opérationnelles, le processus revient brièvement à la phase d'identification afin de reformuler l'hypothèse initiale. Ce retour permet à l'analyse de se concentrer sur la possibilité d'un cas d'espionnage économique industriel en cours de développement, ce qui modifie l'orientation des activités restantes du processus de renseignement.

Dans la phase de contextualisation et d'enrichissement, les données collectées sont intégrées aux informations historiques provenant d'incidents antérieurs et à l'analyse des tendances dans le secteur de l'énergie. Des techniques d'analyse comportementale, d'attribution de TTP et d'exploration de données historiques sont utilisées. Ces méthodologies facilitent la détection de schémas et de coïncidences avec des campagnes précédemment attribuées à des acteurs étatiques ou à des groupes intermédiaires, c'est-à-dire des entités opérant en tant que mandataires ou agents indirects d'autres acteurs ayant des intérêts géopolitiques ou économiques.

Les renseignements sont diffusés sous différents formats adaptés aux besoins spécifiques de chaque type de destinataire. Il peut s'agir d'alertes tactiques destinées aux équipes de cybersécurité chargées d'apporter une réponse immédiate, de rapports stratégiques destinés aux responsables des systèmes énergétiques et de recommandations préventives destinées aux autres opérateurs du secteur afin de renforcer leur position de défense.

Il est important de noter que cette production et cette diffusion de renseignements se font en continu et parallèlement au développement de l'enquête, sans attendre une "conclusion définitive". Cette approche permet une réponse précoce et dynamique aux menaces émergentes, puisque d'autres acteurs concernés du secteur de l'énergie pourraient signaler des incidents similaires dans leurs réseaux après avoir reçu ces produits, ce qui permettrait de rouvrir des cycles d'analyse et de réajuster la hiérarchisation des menaces à l'échelle nationale.

Outre le retour d'information externe de la part des acteurs concernés, qui permet d'ajuster les hypothèses et les priorités en fonction des signaux émis par l'environnement, il existe également une phase continue de retour d'information interne visant à améliorer le processus de renseignement proprement dit. Par exemple, au cours de la phase de contextualisation, l'équipe de renseignement détecte que certains indicateurs clés de compromission (IoC) n'ont pas été considérés comme prioritaires par les systèmes d'alerte automatisés. Cette observation est documentée et transmise à l'équipe chargée d'ajuster les seuils de sensibilité du SIEM, ce qui permet d'affiner les critères de détection pour de futurs cas similaires. Enfin, à la fin du cycle, un examen interne des performances du modèle IDEM dans ce cas précis est effectué, évaluant des paramètres tels que le temps de réponse, la précision des hypothèses initiales et l'utilité des produits générés. Cette évaluation alimente une base de connaissances interne qui permet d'ajuster les méthodologies, les outils et les flux de travail, en veillant à ce que le modèle évolue de manière adaptative et sur la base de l'expérience accumulée.

Cette dynamique de retour en arrière, de reformulation et d'action simultanée permise par le modèle IDEM ne serait pas réalisable dans le modèle classique du cycle du renseignement, ni dans de nombreux modèles proposés dans la littérature examinée, où les processus sont plus rigides, linéaires et dépendent de l'initiative des décideurs.

5. CONCLUSIONS

Le renseignement, entendu comme organisation, processus, produit et même culture, joue un rôle clé dans la gestion de l'incertitude dans des environnements de menaces volatiles, interconnectés et de plus en plus hybrides. Sa nature multidisciplinaire et la diversité des approches utilisées par les différents pays et disciplines rendent difficiles une définition unique et une classification fermée de ses types, mais reflètent également sa richesse conceptuelle et la nécessité d'une coopération et d'une adaptation constante.

Le cycle classique du renseignement, bien que précieux à l'époque pour sa structure et sa normalisation, présente des limites importantes pour relever les défis contemporains, en particulier dans le domaine numérique. La nature dynamique et décentralisée du cyberespace, ainsi que le volume et la vitesse des données, exigent des modèles plus souples et plus adaptatifs. Le modèle IDEM proposé dans le présent document répond à ce besoin au moyen d'une structure modulaire, non linéaire et en réseau, où les phases interagissent simultanément et se nourrissent constamment les unes des autres.

Cette nouvelle approche réorganise les étapes du cycle traditionnel et ajoute des éléments clés tels que l'identification proactive des menaces, la contextualisation intégrée à l'analyse, la diffusion précoce et transversale du renseignement et l'intégration systématique du retour d'information. Elle intègre également des technologies avancées telles que l'intelligence artificielle et l'apprentissage automatique afin d'optimiser la gestion de grands volumes de données et d'améliorer les capacités prédictives.

Cependant, la technologie seule ne suffit pas. Le jugement humain, la capacité critique, la créativité analytique et la connaissance du contexte restent essentiels. La synergie entre les analystes et les systèmes automatisés permet d'obtenir des renseignements plus efficaces, plus précis et plus utiles pour la prise de décision.

En bref, le renseignement du 21e siècle doit être agile, multidisciplinaire et collaboratif. Seules des approches hybrides, ouvertes à l'apprentissage et à l'amélioration continue, permettront d'anticiper et d'atténuer efficacement les menaces émergentes. Le modèle IDEM est un pas dans cette direction : une proposition adaptative et réaliste pour relever les défis que l'ère numérique impose aux systèmes de renseignement contemporains.

La réalité du contexte actuel continue de présenter des défis et des difficultés considérables pour anticiper et atténuer efficacement les menaces contemporaines, en particulier celles qui se manifestent dans le cyberespace, car il est difficile de suivre et de devancer les cybercriminels. Il est donc nécessaire que la communauté du renseignement continue à rechercher et à développer des stratégies qui réduisent les faiblesses actuelles, favorisent la sensibilisation à la culture du renseignement, la diffusion de l'information et la coopération internationale.

6. RÉFÉRENCES BIBLIOGRAPHIQUES

Andric, J. et Terzic, M. (2023). Intelligence cycle in the fight against terrorism with usage of OSINT data. Journal of Information Systems & Operations Management, 17(1). https://doi.org/10.1080/2158379X.2021.1879572

Atwood, C. P. (2015). Activity-Based Intelligence Revolutionizing Military Intelligence Analysis (Le renseignement basé sur les activités révolutionne l'analyse du renseignement militaire). Joint Force Quarterly, 77. https://ndupress.ndu.edu/Media/News/Article/581866/activity-based-intelligence-revolutionizing-military-intelligence-analysis/

Budhram, T. (2015). Intelligence-led policing : A proactive approach to combating corruption. South African Crime Quarterly, 52. https://doi.org/10.17159/2413-3108/2015/i52a30

Carter, J. G. et Fox, B. (2019). Community policing and intelligence-led policing : An examination of convergent or discriminant validity. Policing : An International Journal, 42(1), 43-58. https://doi.org/10.1108/PIJPSM-07-2018-0105

Centre national de cryptologie (2015). CCN-STIC-425 Cycle de renseignement et d'analyse d'intrusion.

National Intelligence Centre (2023). Origines des services de renseignement. https://www.cni.es/sobre-el-cni/nuestra-historia

Chainey, S. et Chapman, J. (2013). A problem-oriented approach to the production of strategic intelligence assessments. Policing : An International Journal of Police Strategies & Management, 36(3), 474-490. https://doi.org/10.1108/PIJPSM-02-2012-0012

Dahj, J. N. M. (2022). Maîtriser la cyber-intelligence. Packt Publishing Ltd.

Díaz Fernández, A. M. (2013). Le rôle de l'intelligence stratégique dans le monde d'aujourd'hui. Cuadernos de Estrategia, 162, 35-66. https://dialnet.unirioja.es/servlet/articulo?codigo=4275959

Francisco, J., & Barrilao, S. (2019). Services de renseignement, secret et garantie judiciaire des droits. Teoría y Realidad Constitucional, 309-340.

Gkougkoudis, G., Pissanidis, D. et Demertzis, K. (2022). Intelligence-Led Policing and the New Technologies Adopted by the Hellenic Police. Digital, 2, 143-163. https://doi.org/10.3390/digital2020009

Grabosky, P. N. (1999). Zero tolerance policing. Australian Institute of Criminology, 102(Trends & issues in crime and criminal justice).

Gruszczak, A. (2018). Le défi de l'adaptation des services de renseignement de l'OTAN. https://www.globsec.org/what-we-do/publications/natos-intelligence-adaptation-challenge

Jefatura del Estado (2002). Loi 11/2002, du 6 mai, régissant le Centre national d'intelligence.

Jiménez Villalonga, R. (2018, 26 novembre). Les types d'intelligence. https://global-strategy.org/tipos-de-inteligencia/

Jordán, J. (2011). Introduction à l'analyse du renseignement. 2340-8421, 2, Art. 2. https://www.seguridadinternacional.es/resi/index.php/revista

Jordán, J. (2015). Introducción a la Inteligencia en el ámbito de Seguridad y Defensa. Análisis GESI (Grupo de Estudios En Seguridad Internacional), 26, Art. 26. https://www.seguridadinternacional.es/resi/index.php/revista

Jordán, J. (2016). Un examen du cycle du renseignement. Análisis GESI (Grupo de Estudios En Seguridad Internacional), 2. https://www.seguridadinternacional.es/resi/index.php/revista

Kamiński, M. A. (2019). Les sources de renseignement dans le processus de collecte d'informations par la communauté du renseignement des États-Unis. Security Dimensions, 32(32), 82-105. https://doi.org/10.5604/01.3001.0014.0988

Knight, T. C. (2024). Five Thousand Candles : Optimizing Information Sharing Policies for Homeland Security (Cinq mille bougies : optimisation des politiques de partage de l'information pour la sécurité intérieure). Système universitaire public américain.

Lee, M. (2023). Cyber Threat Intelligence (1ère éd.), John Wiley & Sons, Inc.

Mahood, L. M. E. K. (2015). SOCMINT : suivre et aimer le renseignement sur les médias sociaux [Collège des Forces canadiennes]. https://www.cfc.forces.gc.ca/254-eng.html.

Ministère de la défense (2023). Renseignement, surveillance et reconnaissance.

Montero Gómez, A. (2006). Inteligencia Prospectiva de Seguridad (24 ; domaine : sécurité et défense). https://www.realinstitutoelcano.org/publicaciones/

Navarro Bonilla, D. (2004). El Ciclo de Inteligencia y sus límites. Cuadernos Constitucionales de La Cátedra Fadrique Furió Ceriol, 48, 51-66. https://dialnet.unirioja.es/servlet/articulo?codigo=2270935

Navarro Bonilla, D. (2005). Information, espionnage et renseignement dans la monarchie hispanique (XVIe-XVIIe siècles). Revista de Historia Militar, Extraordinario, 13-40. https://bibliotecavirtual.defensa.gob.es/BVMDefensa/es/catalogo_imagenes/grupo.do?path=309075

Organisation pour la sécurité et la coopération en Europe (2017). Guide de l'OSCE sur la police fondée sur le renseignement (Département des menaces transnationales, Unité des questions stratégiques de police, Ed. ; Vol. 13).

Payá-Santos, C. A. (2023). Les performances de l'intelligence en Espagne dans les sphères publiques, commerciales et académiques. Revista Científica General José María Córdova, 21(44), 1029-1047. https://doi.org/10.21830/19006586.1222

Phythian, M., Warner, M., Gill, P., Richards, J., Davier, P. H. J., Gustafson, K., Ridgen, I., Brantly, A., Sheptycki, J., Strachan-Morris, D., Omand, D., & Hulnick, A. S. (2013). Understanding the Intelligence Cycle (M. Phythian, Ed.).

Portillo, I. (2019). Savoir ce que sont la cyberveille et le renseignement sur les cybermenaces. https://www.ginseg.com/ciberinteligencia/conociendo-que-es-la-ciberinteligencia-y-el-cyber-threat-intelligence/

Pothoven, S., Rietjens, S. et de Werd, P. (2023). Producer-client paradigms for defense intelligence. Defence Studies, 23(1), 68-85. https://doi.org/10.1080/14702436.2022.2089658

Stewart Bertram (2015). Le Tao de l'intelligence Open Source. IT Governance Publishing.

Summers, L. et Rossmo, D. K. (2019). Offender interviews : implications for intelligence-led policing. Policing, 42(1), 31-42. https://doi.org/10.1108/PIJPSM-07-2018-0096

Vela Tejada, J. (1993). Tradition et originalité dans l'œuvre d'Énée le tacticien : la genèse de l'historiographie militaire. Minerva. Revista de Filología Clásica, 7, 79-92. https://doi.org/https://doi.org/10.24197/mrfc.7.1993