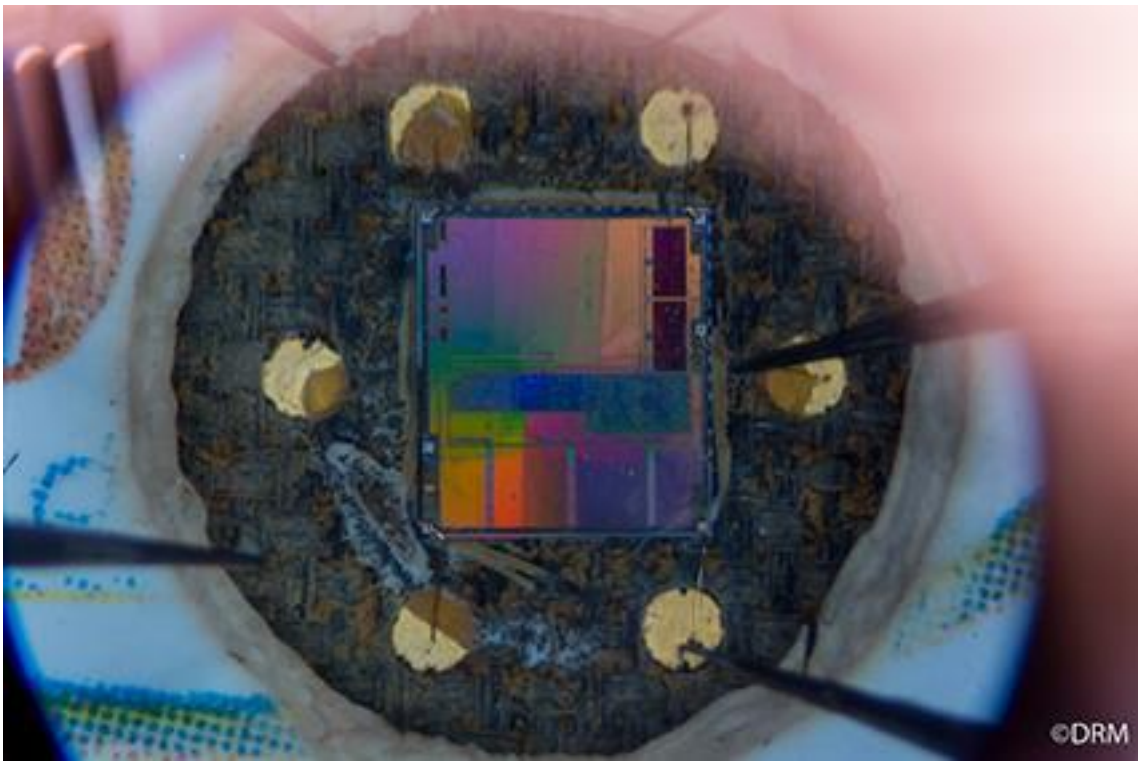
RESSOURCES PÉDAGOGIQUES

LE RENSEIGNEMENT A L'ERE DU NUMERIQUE



Auteur :

Ministère des Armées
Direction du renseignement militaire

SOMMAIRE

QU'EST-CE QUE LE RENSEIGNEMENT ? À QUOI ÇA SERT ?

- C'est une information construite et pertinente, délivrée pour guider des prises de décisions et des actions.

Le renseignement, c'est l'ensemble des informations et faits révélés et analysés par le travail des services compétents. L'objectif est de prévenir les atteintes aux intérêts d'une nation, de protéger les personnes, les biens et les institutions et de défendre et promouvoir les intérêts d'un pays.

En France, le renseignement, c'est aussi une politique publique qui met en œuvre des moyens et des outils de puissance publique et qui est, à ce titre, encadrée et contrôlée. C'est également un instrument de souveraineté qui contribue à préserver l'autonomie de décision de l'Etat. La France ne peut se dispenser d'un appareil de renseignement à la hauteur de son indépendance, de son statut de membre permanent au Conseil de sécurité de l'ONU, de sa présence dans le monde, de son dynamisme économique et de son rayonnement politique et culturel.

L'aide à la décision est la mission traditionnelle du renseignement. Elle vise à apporter aux hautes autorités de l'État, une information fiable sur leurs priorités et enjeux stratégiques en vue de faciliter la conduite de la politique nationale.

L'entrave représente la capacité à prévenir la concrétisation d'une menace et à y mettre fin. Elle peut être de plusieurs natures : judiciaire, militaire, politique, diplomatique ou administrative. La mission d'entrave est inséparable du renseignement, soit parce qu'elle est exercée directement par les services qui en ont la capacité, soit parce qu'elle s'appuie sur les éléments recueillis par le renseignement.

Le renseignement, outil de défense de nos intérêts et d'acquisition de connaissances dans les domaines stratégiques, est également un outil de promotion de nos intérêts (politique, économique, scientifique, militaire, culturel, etc.).

Le renseignement est non seulement une priorité, mais il doit aussi s'adapter à des formes inédites de conflits ou des menaces émergentes et affronter de nouveaux défis.

FOCUS 1 : L'ORGANISATION DU RENSEIGNEMENT EN FRANCE

➢ On parle de « communauté française du renseignement ».

Cette notion a émergé depuis le Livre blanc sur la défense et la sécurité nationale de 2008 et a été une première fois définie par un décret du 12 mai 2014, puis par le décret du 14 juin 2017. Les services qui composent cette communauté travaillent aujourd'hui en étroite collaboration, investis collectivement d'une mission qu'ils partagent.

Les services spécialisés de renseignement sont la Direction générale de la sécurité extérieure (DGSE), la Direction générale de la sécurité intérieure (DGSI), la Direction du renseignement militaire (DRM), la Direction du renseignement et de la sécurité de la défense (DRSD), la Direction nationale du renseignement et des enquêtes douanières (DNRED) et le service de Traitement du renseignement et d'action contre les circuits financiers clandestins (TRACFIN).

Ces six services, dits du « premier cercle », forment avec le Coordonnateur national du renseignement et de la lutte contre le terrorisme (CNRLT), l'académie du renseignement et l'inspection des services de renseignement, la communauté française du renseignement.

La Stratégie nationale du renseignement (SNR) constitue la feuille de route du renseignement. Elle en décrit à la fois les enjeux prioritaires, les objectifs qui sont poursuivis et les adaptations qui doivent en découler en termes d'organisation.

FOCUS 2 : AU SEIN DU MINISTÈRE DES ARMÉES, QUI FAIT QUOI EN MATIÈRE DE RENSEIGNEMENT ?

➢ Le ministère des Armées dispose de trois services de renseignement aux compétences complémentaires.

La Direction du renseignement militaire (DRM) :
Sous l'autorité du chef d'état-major des armées, elle appuie les forces armées en fournissant le renseignement nécessaire à la planification et à la conduite des opérations militaires. Elle permet au président de la République, chef des Armées, des choix autonomes et assure une veille stratégique permanente.

La Direction générale de la sécurité extérieure (DGSE) :
Elle recherche des renseignements par des moyens clandestins et agit hors du territoire national, partout dans le monde.

La Direction du renseignement et de la sécurité de la défense (DRSD) :

Elle recueille des renseignements pour contrer les menaces comme l'espionnage ou le terrorisme afin de protéger les forces armées et les 4 000 entreprises de défense, en France et à l'étranger.

FOCUS 3 : LA DIRECTION DU RENSEIGNEMENT MILITAIRE (DRM) ÉCLAIRE SUR LES RISQUES DANS LE MONDE

➢ Elle informe sur les capacités de nos adversaires et garantit ainsi la décision autonome des chefs politiques et militaires.

Dans un monde de compétition permanente, de contestation fréquente, dans un contexte d'accentuation des menaces armées, l'éclairage apporté par le renseignement, et notamment le renseignement d'intérêt militaire, est essentiel.

Créée en 1992 au lendemain de la 1re guerre du Golfe, la Direction du renseignement militaire (DRM) est le service de renseignement des armées.

Placée sous l'autorité du chef d'état-major des armées, elle est chargée de deux missions principales :

- elle fournit une aide à la prise de décision autonome des hautes autorités de notre pays, politiques et militaires : la DRM fournit au président de la République, au chef d'état-major des Armées, au ministre des Armées et aux grands commandements militaires, le renseignement de situation nécessaire à l'exercice de leurs responsabilités.
- elle appuie les forces armées en fournissant le renseignement nécessaire à la planification et à la conduite des opérations militaires.

Elle participe également aux travaux d'anticipation et de veille stratégique qui fixent notamment au niveau mondial, les zones géographiques d'intérêt prioritaire pour le renseignement militaire.

Le renseignement représente l'une des composantes-clé de notre souveraineté. Grâce aux femmes et aux hommes du renseignement militaire, les menaces d'aujourd'hui et de demain sont caractérisées.

La DRM regroupe environ 2 000 personnes, militaires ou civils. Ils sont analystes, spécialistes dans l'exploitation des images ou des signaux électromagnétiques, spécialistes dans le domaine de l'Intelligence artificielle ou des données.

Elle dispose de plateaux de production du renseignement, de centres techniques experts et d'un centre de formation. En outre, elle oriente et coordonne de manière fonctionnelle les moyens de renseignement issus de l'armée de Terre, de la Marine nationale et de l'armée de l'Air et de l'Espace au sein de la Fonction interarmées du renseignement qui représente 8 000 personnes.

La DRM, c'est aussi des capteurs. Elle dispose de satellites, de centres d'écoute ou encore de bateaux, des avions de renseignements, de capteurs terrestres, ou de spécialistes du renseignement humain soit en propre, soit au sein des trois armées.

La complémentarité de ses capteurs lui permet d'agir sur tout le spectre des menaces.

La DRM participe activement au dispositif national du renseignement articulé autour du Coordinateur national du renseignement et de la lutte contre le terrorisme (CNRLT), qui permet un meilleur partage des savoir-faire et des informations, dans le respect du périmètre de responsabilité dévolu à chaque service. La DRM contribue, notamment, aux côtés des autres services de renseignement, à la lutte contre le terrorisme.

FOCUS 4 : LE CYCLE DU RENSEIGNEMENT

➢ Le renseignement est un système itératif.

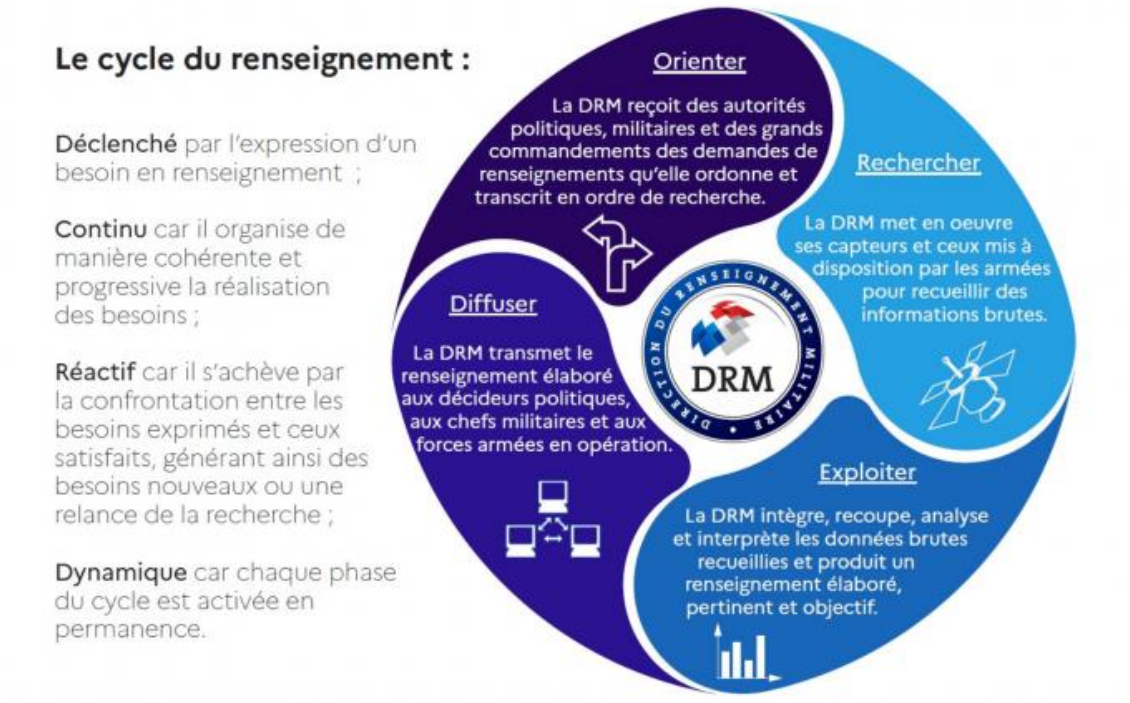
Le renseignement se construit à partir d'un cycle immuable, se décomposant en quatre phases. Il a pour but de satisfaire les besoins en renseignement liés au processus décisionnel du niveau concerné et de répondre aux demandes d'information de l'échelon supérieur.

Le cycle du renseignement est défini comme une « séquence d'opérations par lesquelles les informations sont obtenues, regroupées, transformées en renseignement et mises à la disposition des utilisateurs ». Il illustre l'enchaînement naturel de la réflexion à des fins d'action afin de bien identifier toutes les étapes et leur succession logique depuis l'expression du besoin jusqu'à sa satisfaction.

Ce concept est fondamental mais nécessairement symbolique car il est loin de représenter l'ensemble des activités conduites souvent simultanément.

D'une part, les étapes peuvent être simultanées en raison du nombre de demandes à traiter selon des délais variables.

D'autre part, chaque étape peut développer en parallèle son propre cycle interne, à un rythme différencié selon la nature des besoins et des capteurs mis en jeu.



Il est également nécessaire d'introduire le rôle de l'animation du cycle du renseignement, que concrétisent, la gestion des données existantes, le processus de coordination de la recherche et de gestion des besoins en renseignement, ayant pour but d'optimiser le cycle et de le relancer si nécessaire.

Enfin, selon les besoins des demandeurs, le degré d'élaboration des produits peut être varié et conduire à des phases d'exploitation plus ou moins longues.

L'ÈRE DU NUMÉRIQUE : DE QUOI PARLE-T-ON ? POUR LES ARMÉES ET POUR LE RENSEIGNEMENT, QU'EST-CE QUE CELA IMPLIQUE ?

➢ Le numérique constitue l'un des changements les plus fondamentaux de la transformation du monde.

Depuis la fin des années 1980, le numérique a définitivement transformé notre vie dans tous les domaines et son usage est devenu peu à peu un impératif.

Internet est le moteur de cette transformation. L'information est transmise via un réseau mondial de machines grâce à un ensemble standardisé de protocoles de transfert de données, qui permet des applications variées comme le courrier électronique, le World Wide Web (la navigation sur les sites Internet), la messagerie instantanée, le partage de fichiers, le streaming, le podcasting, la téléconférence.

Cette révolution numérique impacte de façon très importante la vie des individus au point de parler d'une génération avant et une génération après le tout-connecté, la « génération C ».

Très concrètement, avec l'ère du numérique, on observe la massification des données disponibles à tous les niveaux de notre société. Ceci implique l'obligation pour tous les niveaux d'organisations d'une gestion maîtrisée de cette masse de données. Les organisations doivent faire preuve de plus d'agilité pour y parvenir.

Avec l'ère du numérique, on peut mener des actions sans être physiquement au contact. L'ère du numérique s'appuie sur quatre grands concepts :

- le big data ;
- la connectivité ;
- l'intelligence artificielle ;
- la cybersécurité.

Cinq grandes firmes américaines dominent le marché du numérique mondial. Ce sont les GAFAM : on utilise cet acronyme pour désigner les géants que sont Google (Alphabet), Apple, Facebook (Meta), Amazon et Microsoft. Ce leadership connaît aujourd'hui plusieurs obstacles, dont un de taille, la concurrence chinoise.

L'innovation chinoise dirigée par l'Etat a façonné ses propres champions : les BATX (Baidu, Alibaba, Tencent, Xiaomi). Depuis l'attaque américaine envers les entreprises chinoises Huawei et TikTok, la guerre technologique entre la Chine et les États-Unis est devenue une réalité.

Le numérique fournit une occasion unique de façonner notre avenir. En même temps, il s'agit d'une importante responsabilité : nous devons nous assurer que ces transformations auront un impact positif dans un contexte où le numérique est devenu un enjeu de pouvoir.

FOCUS 1 : LA MENACE CYBER, QU'EST-CE QUE C'EST ? LE RENSEIGNEMENT EST-IL UTILE DANS LE CYBER ?

En matière cyber, la menace, qu'elle soit étatique, provenant d'entreprises privées ou d'organisations criminelles, a fortement évolué. Elle est de plusieurs natures : vol de données, sabotage au préjudice des entreprises comme des administrations, pénétration à des fins d'espionnage, chantage en vue d'obtenir une rançon… Certaines de ces opérations relèvent désormais d'une nouvelle forme de criminalité organisée, de terrorisme, voire de guerre. Le cyberespace constitue un nouvel espace de conflictualité.

Aussi, l'intensité de la menace et les risques encourus sont tels qu'il est essentiel, au-delà des dispositifs de sécurité dont la France est dotée, que les services de renseignement contribuent à leur recherche et à leur anticipation dans leurs champs respectifs de compétence. Il est ainsi essentiel de caractériser et de suivre les acteurs de cette

cyber-malveillance. L'évaluation de la menace permet d'adapter les mesures de protection des systèmes d'information.

De plus, le développement de l'Internet des objets et des communications spatiales, ainsi que l'évolution des maliciels[1] aux effets de plus en plus destructeurs, nécessitent une adaptation constante des capacités des services et une meilleure diffusion du renseignement vers les entités chargées de la protection et de l'entrave. L'évolution rapide des technologies implique de disposer d'un dispositif étatique agile et d'un personnel hautement qualifié.

Enfin, par le biais d'Internet et des réseaux sociaux, l'espace cyber est un vecteur de diffusion des messages haineux et de manipulation de l'information qui mérite un suivi du Renseignement pour identifier les messages ou les campagnes les amplifiant, en attribuer l'origine et faciliter leur entrave administrative et judiciaire.

FOCUS 2 : LE COMMANDEMENT DE LA CYBERDÉFENSE DU MINISTÈRE DES ARMÉES

- Le numérique est un espace de conflictualité important : les attaques sont nombreuses et se complexifient.

La guerre cyber fait partie des capacités de nos armées. Il s'agit de contrer des Etats adversaires de la France ou qui cherchent à espionner, à voler des données, à se prépositionner en vue d'un conflit futur.

Créé en 2017 et placé sous l'autorité directe du chef d'état-major des armées, le Commandement de la cyberdéfense (COMCYBER) est un commandement opérationnel, qui rassemble l'ensemble des forces de cyberdéfense du ministère sous une autorité interarmées. Il a pour mission la défense des systèmes d'information, ainsi que la conception, la planification et la conduite des opérations militaires dans le cyberespace. Il a une mission de fédération et de conduite des actions des différents acteurs cyber du ministère.

Il est aujourd'hui doté de 3 600 combattants.

Un « cyber soldat » ou « cyber combattant » est une personne qui va se mouvoir et être spécialisé dans l'espace numérique, comme d'autres sont spécialisés dans l'espace terrestre, maritime, aérien ou l'espace exo-atmosphérique. Son domaine de spécialité est la lutte informatique défensive.

Sa mission : quand il y a quelque chose d'étrange sur un réseau, quand un attaquant est soupçonné d'avoir pris pied dans un système du ministère des Armées, le rôle du COMCYBER est d'intervenir, de comprendre ce qui s'est passé, de récupérer des traces de l'attaque et d'expulser l'attaquant du système d'information.

Le nombre de cyberattaques augmentent en quantité et en qualité. En 2021, le COMCYBER a compté plus de 12 000 événements de sécurité, dont 14 incidents sont remontés jusqu'au niveau de la présidence de la République.

[1] Des logiciels malveillants.

FOCUS 3 : L'AGENCE NATIONALE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION AIDE LES VICTIMES DE CYBERATTAQUES

➢ Les conséquences d'une cyberattaque peuvent être très graves et n'épargnent aucune cible.

Dans bien des cas, les conséquences d'une cyberattaque sont dramatiques : entre 50% et 80% des PME dont les données sont bloquées finissent par faire faillite, estime un rapport du Sénat publié en juin 2021[1].

Entre 2020 et 2021, le nombre d'attaques aux logiciels de rançon a été multiplié par quatre d'après l'Agence nationale de sécurité des systèmes d'information (ANSSI).

L'ANSSI emploie aujourd'hui plus de 500 agents et a dressé une liste d'acteurs privés et publics qui ont l'obligation de se protéger en matière cyber. Ce sont les Opérateurs d'intérêt vital (OIV) et les opérateurs de services essentiels (OSE). La liste détaillée est secrète mais on y trouve les grands acteurs de l'énergie, de la finance, des transports et télécommunications, de la santé ou des médias.

En cas de cyberattaque, l'ANSSI a vocation à aider les services publics ainsi que les grandes entreprises. Pour les autres, le site cybermalveillance.gouv.fr permet de s'orienter.

FOCUS 4 : LA NUMÉRISATION EST UN ENJEU MAJEUR POUR LE RENSEIGNEMENT

➢ La donnée est un défi pour le renseignement et l'univers cyber est, de ce point de vue, presque infini. C'est à la fois une source d'informations et un nouvel espace de conflictualité.

Les technologies numériques sont omniprésentes et permettent de renouveler les modes d'action historiques du renseignement. Il n'y a pas de frontière entre ce que l'on appelle l'espace numérique et l'activité humaine. Un service de renseignement doit pouvoir y agir en coordination directe avec ses pairs de la communauté nationale du renseignement.

Force est de constater que la numérisation a considérablement transformé l'écosystème du renseignement. La quantité de données à traiter ne cesse de croître et l'enjeu est de les exploiter toujours mieux avec une ressource humaine qui doit rester maîtrisée. Cela donne un terrain de jeu gigantesque, notamment dans le domaine de l'Intelligence artificielle (IA) puisqu'il s'agit désormais d'utiliser les nouvelles technologies pour optimiser le croisement des données et automatiser les traitements.

D'une manière générale, l'appropriation de ces technologies de big data et d'IA imposent une transformation profonde de l'organisation qui va bien au-delà de la sphère technique. Il s'agit de changer notamment les processus de fonctionnement, la doctrine et faire évoluer certains métiers.

Il s'agit donc bien d'une démarche de transformation visant à adapter les services de renseignement au dimensionnement sans précédent de la volumétrie des données collectées et capitalisées.

[1] *La cybersécurité des entreprises, prévenir et guérir : quels remèdes contre les cyber virus ?* Rapport d'information, Sénat, 10 juin 2021.

FOCUS 5 : ENJEU STRATÉGIQUE POUR LE RENSEIGNEMENT, L'INTELLIGENCE ARTIFICIELLE EST AU CŒUR DE LA RÉVOLUTION NUMÉRIQUE

Concept né dans les années 50, l'Intelligence artificielle (IA) est aujourd'hui une réalité qui touche quasiment tous les métiers. Son essor a été facilité par des avancées technologiques majeures, en particulier les vitesses de calcul des processeurs (GPU) et la miniaturisation des composants. Aujourd'hui, les opportunités sont telles que l'IA est considérée comme une technologie d'importance stratégique.

Qu'est-ce que l'intelligence artificielle ?

L'IA est un ensemble de techniques permettant à des machines ou des algorithmes d'accomplir des tâches et de résoudre des problèmes normalement réservés aux humains. La traduction automatique, la détection de signaux faibles, l'identification de véhicules dans des images sont des exemples d'application qui intègrent cette technologie.

Toutes ces techniques évoluent à une vitesse vertigineuse dans le secteur civil et sont des moteurs continus de l'innovation numérique dans le monde de la défense.

Intelligence artificielle et renseignement ?

Dans le cadre de la Stratégie nationale pour l'intelligence artificielle[1] (SNIA) voulue par le Président de la République, le domaine de la défense et la sécurité a été identifié comme un axe d'effort prioritaire pour la France. La ministre des Armées, consciente des opportunités et de la nécessité de coordonner les différentes initiatives dans ce domaine a créé en septembre 2018, au sein de son ministère, une « task force Intelligence artificielle ». Le renseignement est alors apparu comme un des axes stratégique et prioritaire.

Quels enjeux pour le renseignement ?

Aujourd'hui tous les experts métiers du renseignement sont abreuvés en continu de données extrêmement riches, de natures variées. Chaque jour, chaque minute, les capteurs déversent des quantités gigantesques de données. Tout l'enjeu de l'intelligence artificielle, est donc d'aider le traitant dans sa mission titanesque de les exploiter toujours mieux et toujours plus vite, sachant qu'il évolue dans un monde où des informations importantes sont noyées au milieu d'un flux d'échanges incessants et où les tentatives d'influence existent.

[1] La SNIA a un budget de 1,5 milliard d'euros sur la période 2018-2022 (https://www.intelligence-artificielle.gouv.fr/fr/secteurs-prioritaires/l-intelligence-artificielle-et-monde-de-la-defense)

Compétences et métiers IA :

Le développement et l'usage de solutions d'intelligence artificielle supposent de disposer de personnels formés en mesure de comprendre les mécanismes mis en œuvre. Ce qui impose d'avoir une compétence aussi bien en mathématiques que dans le domaine de l'informatique. Ce socle de connaissance offre alors une pluralité de métiers dans le domaine du renseignement : *datascientist*, chef de projet IA, experts IA, développeur …

Illustration par des extraits du discours de Florence Parly, ministre des Armées, *Point d'étape sur le feuille de route de l'Intelligence artificielle*, Creil, le 10 mai 2021 :

« Depuis plusieurs années déjà, le constat d'une course mondiale à l'intelligence artificielle est partagée. Le domaine de la défense y occupe une place stratégique. La France s'est mise en ordre de bataille pour saisir les opportunités offertes par l'intelligence artificielle et pour rejoindre les leaders en la matière. »

« Au-delà de la collecte et du stockage des données, les armées, nos services de renseignement, la direction générale de l'armement, ont bien saisi l'impérieuse nécessité de les structurer, les analyser, les corréler, pour en extraire le renseignement dont nous avons besoin, optimiser nos capteurs, gagner en performance grâce à la maintenance prédictive ou encore aider à la planification de nos missions. Bien évidemment, les applications sont nombreuses et il s'agit là que de quelques illustrations de l'apport de l'intelligence artificielle pour éclairer nos décisions et conduire nos opérations. »

« Le traitement massif des données, c'est le nouveau nerf de la guerre. C'est ce qui nous permettra de prendre la bonne décision lorsqu'il s'agit d'exploiter quotidiennement des Téraoctets de données d'imagerie satellitaire. C'est aussi ce qui nous permettra d'améliorer le maintien en condition opérationnelle de nos aéronefs à partir de l'analyse des données de vol et d'un suivi précis de l'usage des équipements embarqués. C'est ce qui nous permettra d'élaborer des itinéraires qui minimiseront le passage de nos blindés en zone ennemie sur les théâtres d'opérations extérieures. C'est encore ce qui permettra d'intégrer des mécanismes intelligents dans les systèmes de combats des bâtiments de la Marine nationale.

En matière de traitement massif des données, nous ne pouvons donc dépendre de personne. C'est un enjeu de souveraineté essentiel. C'est pourquoi nous avons lancé en 2018 le programme national Artémis. Artémis, c'est une solution souveraine de traitement massif des données et d'algorithmes d'intelligence artificielle adaptée aux besoins de la défense. C'est un projet qui, à terme, réunira tous les ingrédients d'une IA appliquée à la défense : puissance de calcul, de la sécurité et de la modularité. Il offrira la boite à outils indispensable à une partie des développements à base d'IA du ministère des Armées. »

LE RENSEIGNEMENT, UN CADRE JURIDIQUE STRICT ET NÉCESSAIRE

Le recours accru aux traitements de données, les développements capacitaires et l'existence d'un cadre juridique lacunaire ont conduit à l'adoption d'une véritable politique publique du renseignement à partir de 2015.

Fort d'une volonté affirmée des services de renseignement de légitimer leur action, le législateur a adopté en quelques années plusieurs lois encadrant l'activité de ces services, et plus particulièrement la mise en œuvre de mesures de surveillance, autrement appelée les techniques de recueil de renseignement.

FOCUS 1 : LE CADRE LÉGAL GÉNÉRAL APPLICABLE À LA MISE EN ŒUVRE DES TECHNIQUES DE RECUEIL DE RENSEIGNEMENT

Historiquement, le renseignement a longtemps fait l'objet d'une certaine défiance et les activités des services de renseignement étaient caractérisées par une opacité systématique, considérées comme des « secrets d'Etat ». Seule une loi de 1991, adoptée à la suite de l'arrêt de la Cour européenne des droits de l'homme (CEDH) Kruslin et Huvig du 24 avril 1990, régissait les écoutes administratives (téléphoniques). En 2015, le législateur a consacré une véritable politique publique du renseignement, avec l'octroi de moyens, d'une protection pour les agents des services et plus globalement, d'un cadre légal encadrant strictement leurs activités, notamment en mettant en place des obligations de traçabilité.

Plusieurs lois successives sont ainsi venues encadrer la pratique des services de renseignement. La première, votée le 24 juillet 2015 et relative au renseignement, est consacrée de façon générale à la mise en œuvre des techniques de recueil de renseignement et aux règles régissant l'activité des services. Certaines dispositions de cette loi ayant fait l'objet d'une censure par le Conseil constitutionnel, une seconde loi a été votée le 30 novembre 2015 concernant les mesures de surveillance des communications électroniques internationales. Ces dispositions ont été complétées ensuite par la loi de programmation militaire du 13 juillet 2018.

En 2017, une troisième loi a été adoptée, visant à renforcer la sécurité intérieure et la lutte contre le terrorisme. Elle a notamment précisé le régime applicable à l'interception des communications électroniques empruntant exclusivement la voie hertzienne à la suite de la jurisprudence du Conseil constitutionnel ayant remis en cause le dispositif posé par la loi de 2015. Enfin, la loi du 30 juillet 2021 est venue encadrer les échanges de renseignement issus de ces techniques entre les services de renseignement, en établissant selon les cas, une autorisation préalable d'une autorité administrative indépendante, et de manière systématique la traçabilité de ces derniers.

L'ensemble de ces dispositions ont depuis été codifiées sous le Livre VIII du Code de la sécurité intérieure (CSI). Ces dispositions sont toutefois soumises à un critère d'application de la loi : le critère de territorialité. Ce critère implique que les dispositions précitées ne s'appliquent qu'aux actions menées sur ou depuis le territoire national (territoire métropolitain, départements, régions et collectivités d'outre-mer (DROM-COM), ainsi que les eaux territoriales et l'espace aérien). A l'inverse, les techniques de renseignement mises en œuvre à l'étranger, dans le cadre d'opérations extérieures, ne sont pas couvertes par ces dispositions législatives.

Ce corpus juridique vient ainsi renforcer le cadre juridique applicable aux mesures de surveillance mises en œuvre sur le territoire national, en reflétant un choix de société en adéquation avec les exigences d'une démocratie moderne et la jurisprudence des juridictions tant nationales qu'européennes. Il pose par ailleurs de réelles garanties en légitimant l'activité des services et de leurs agents, dès lors qu'ils demeurent dans le cadre juridique fixé. En contrepartie, ce cadre juridique impose un certain nombre de contrôles de la part de diverses instances (contrôle interne et des services du Premier ministre, contrôle externe d'une autorité administrative de contrôle et recours juridictionnels) et certaines limitations.

FOCUS 2 : LES PRINCIPES RÉGISSANT L'ACTIVITÉ DES SERVICES DE RENSEIGNEMENT DANS LA MISE EN ŒUVRE DES TECHNIQUES DE RECUEIL DE RENSEIGNEMENT

1. La conciliation des activités de renseignement avec la préservation des libertés publiques

En tant que mesures de police administrative, l'activité des services de renseignement consiste à prévenir les atteintes potentielles à l'ordre public. Cette mission est par nature difficilement conciliable avec le respect de la vie privée et ses déclinaisons (secret des correspondances, protection des données à caractère personnel, inviolabilité du domicile), même si celui-ci n'est pas absolu et peut faire l'objet de dérogations. Toutefois, le droit à la sécurité constitue également un droit fondamental et l'une des conditions de l'exercice des libertés individuelles et collectives, si bien que ces deux droits doivent être conciliés dans le cadre d'un équilibre global.

La mise en place d'un régime juridique applicable aux services de renseignement visait donc à concilier les impératifs de respect des libertés publiques et la protection des droits des citoyens susceptibles de faire l'objet d'une surveillance, avec la nécessité de ne pas obérer les capacités d'action des services. Cet équilibre entre les mesures par natures intrusives prises dans le cadre des nécessités d'intérêt public, notamment des besoins en renseignement des services, et le principe de respect de la vie privée est posé dès l'article chapeau du Livre VIII, à l'article L. 801-1 du CSI.

2. La protection renforcée de certaines professions dites « protégées »

En 2015, le législateur, conscient que certaines professions ou activités sont considérées comme d'une importance telle pour l'exercice de la vie démocratique qu'elles devaient faire l'objet de mesures particulières, a décidé de restreindre les possibilités de surveillance de membres de certaines professions. Aussi les magistrats, avocats, parlementaires et journalistes bénéficient d'une protection renforcée, dans la mesure où chacune de ces professions renvoie à des grands principes directeurs tels que la liberté de la presse, la protection des sources, le respect des droits de la défense (incluant la confidentialité des échanges entre l'avocat et son client) et le principe de séparation des pouvoirs (législatif, exécutif et judiciaire).

Il en résulte que la surveillance de ces professions n'est pas interdite par la loi, mais s'effectue dans des conditions plus restrictives. La surveillance n'est ainsi possible que dans le cadre des communications détachables de l'activité professionnelle de ces catégories, et fait l'objet d'un contrôle renforcé de l'autorité de contrôle. Cette limitation relève également d'un choix de société, qui se fonde sur notre histoire politique.

3. Le respect des principes de proportionnalité et de subsidiarité

Le code de la sécurité intérieure offre aux six services spécialisés de renseignement la possibilité de mettre en œuvre des mesures de surveillance individuelle. Outre le nombre de services limitativement énuméré, le code pose deux principes cardinaux régissant la mise en œuvre de ces techniques de recueil de renseignement : la proportionnalité de la mesure mise en œuvre (autrement dit la mesure doit obligatoirement être proportionnée au besoin en renseignement recherché) et la subsidiarité entre les techniques susceptibles d'être mises en œuvre (ce qui implique que la moins intrusive pour atteindre l'objectif recherché doit impérativement être sollicitée en première approche).

Par ailleurs, aux fins de mettre en œuvre une technique de recueil de renseignement, les services doivent systématiquement se fonder sur une ou plusieurs des sept finalités légales posées par la loi (article L. 811-3 du CSI) et dénommées « intérêts fondamentaux de la Nation ». A ce titre, le recueil n'est permis qu'aux fins de la défense et de la promotion de ces intérêts fondamentaux de la Nation.

FOCUS 3 : LE RÉGIME D'AUTORISATION ET DE CONTRÔLE APPLICABLE À LA MISE EN ŒUVRE D'UNE SURVEILLANCE INDIVIDUELLE PAR LES SERVICES

Au-delà des principes directeurs et fondements de mise en œuvre d'une mesure de surveillance, celle-ci repose sur deux régimes : un régime d'autorisation a priori et un régime de contrôle a posteriori.

1. Une autorisation par une autorité administrative indépendante

Toute demande de mise en œuvre d'une technique de renseignement doit faire l'objet d'une autorisation préalable du Premier ministre, après avis d'une autorité administrative indépendante, la Commission nationale de contrôle des techniques de renseignement (CNCTR). Cette Commission est chargée d'exercer un contrôle externe de la légalité de l'activité des services de renseignement et d'apprécier l'atteinte portée à la vie privée des personnes concernées, au regard des menaces invoquées.

La Commission rend ainsi un avis au Premier ministre sur la légalité de toutes les demandes tendant à la mise en œuvre de techniques de renseignement sur le territoire national. Son contrôle porte notamment sur le respect des principes de proportionnalité et de subsidiarité.

2. Un encadrement a posteriori, administratif, politique et juridictionnel

La CNCTR exerce également un contrôle a posteriori en veillant à ce que toutes les techniques mises en œuvre sur le territoire national soient autorisées et respectent le cadre légal qui les régit. A cet effet, elle dispose d'un accès permanent, complet et direct aux renseignements élaborés par les services bénéficiaires. Cette modalité de contrôle inclut en particulier des vérifications sur pièces et sur place au sein des services de renseignement.

Si la CNCTR est un véritable organe de contrôle indépendant, d'autres entités peuvent également être amenées à encadrer l'activité des services de renseignement. La délégation parlementaire au renseignement et la Cour des comptes contribuent ainsi à l'évaluation de l'application des politiques publiques et constituent un encadrement de nature politique pour les services de renseignement. L'inspection des services de renseignement et la commission nationale informatique et libertés sont également amenés à effectuer des contrôles au sein des services.

L'ensemble de ces organismes contribuent au contrôle administratif et juridique de l'activité des services. Les activités de renseignement sont ainsi largement encadrées.

Par ailleurs, conformément à l'article L 841-1 du code de la sécurité intérieure, toute personne souhaitant vérifier qu'aucune technique n'est irrégulièrement mise en œuvre à son encontre dispose de la possibilité de saisir la formation spécialisée du Conseil d'Etat. Avant 2015, les procédures contentieuses relatives aux activités de renseignement étaient presque systématiquement vouées à l'échec en l'absence de compétence juridictionnelle et face à l'obstacle que représentait la protection du secret de la défense nationale. La loi de 2015 a renforcé le contrôle juridictionnel des activités de renseignement en offrant au Conseil d'Etat une nouvelle compétence exclusive. Cet encadrement juridictionnel se retrouve également en cas d'avis défavorable de la CNCTR pour une demande de mise en œuvre de technique de renseignement, auquel cas le Conseil d'Etat est obligatoirement saisi. C'est une section spécialisée du Conseil d'Etat, composée de magistrats habilités à connaître de documents relevant du secret de la défense nationale, qui est compétente.

Au bilan, les activités des services de renseignement sont donc strictement encadrées par le code de la sécurité intérieure et font l'objet d'un contrôle renforcé de plusieurs autorités externes, qu'il soit administratif, politique ou juridictionnel. Le renseignement étant par principe une matière mouvante en constante évolution, les principes immuables qui fondent notre modèle démocratique sont le gage d'un cadre juridique effectif. Pour l'avenir, la multiplication exponentielle des données numériques et leur encadrement constitue un enjeu majeur pour l'ensemble de la communauté du renseignement, qui se doit d'adapter ses outils pour faire face, demain, au « mur de la donnée », tout en étant consciente que de nouveaux principes se feront jour.

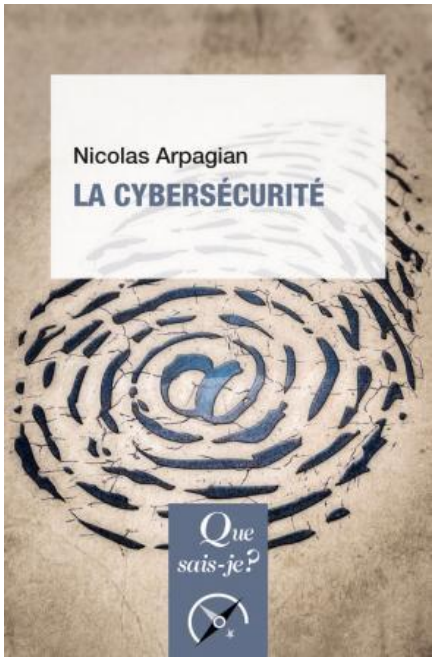
- ***Snowden***, Oliver Stone, film germano-franco-américain, 2h14, 2016

Le film revient sur les révélations faites par Edward Snowden sur la collecte illégale d'informations par la National Security Agency (NSA) sous prétexte de lutte antiterroriste.

- ***Le cyber : un nouvel espace géopolitique***, Le dessous des cartes, Arte, documentaire, 15 minutes, 2018

Au cœur de l'actualité politique et militaire, le cyber est un instrument nouveau qu'il faut savoir manier, parfois pour s'en défendre. Les cyberattaques menacent aujourd'hui indifféremment les individus, les entreprises ou les États. Quelles sont les formes de cybercriminalité ? Quels en sont les enjeux politiques internationaux ? État des lieux cartographique, à l'aide d'exemples aux quatre coins du monde.

- ***La cybersécurité,*** Nicolas Arpagian, Que sais-je ?, PUF, 128 pages, 2022



Nous vivons dans des sociétés de plus en plus numérisées où presque toutes les activités humaines dépendent du bon fonctionnement des technologies de l'information, en particulier d'Internet. Les États, les entreprises, les forces armées, les activistes, le crime organisé et même les particuliers apprécient l'avantage stratégique de l'arme numérique pour capter des données ou de l'argent, déstabiliser une organisation ou attenter à sa réputation. Tous sont ainsi irrigués par une informatique vulnérable aux cyberattaques.

Nos vies personnelles et professionnelles se trouvent dorénavant menacées par ces nouvelles formes d'affrontement et dépendent de la cybersécurité. Laissée sans contraintes, celle-ci peut néanmoins aboutir au cauchemar d'une société de la surveillance totale. À chacun le devoir de s'informer sur les enjeux de la sécurité numérique.

- ***Cyber espionnage : mon nom est Geek, James Geek***, La méthode scientifique, France culture, podcast, 58 minutes, 2018

Quels sont les nouveaux types d'espionnage ? Comment les espions travaillent-ils aujourd'hui ? Quelles sont les menaces qui résultent des nouvelles technologies ? Qu'est-ce qu'une cyberattaque et quelles en sont les conséquences ? Quels organismes utilisent le cyber espionnage ?

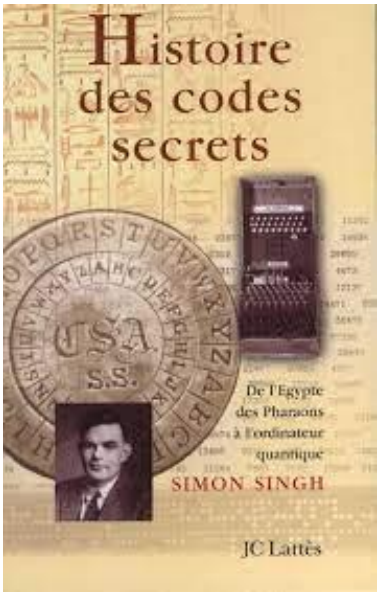
Avec Nicolas Arpagian, maître de conférences à l'Ecole nationale supérieure de la police (ENSP) et directeur scientifique au sein de l'Institut national des hautes études de la sécurité et de la justice (INHESJ), rédacteur en chef de la revue Prospective stratégique, et Gérald Arboit, historien, directeur de l'équipe Renseignement au Centre national des Arts et Métiers.

- ***Mécaniques de la cybermenace***, Maxime Tellier, France culture, podcast réalisé en 5 épisodes, 55 minutes, 2022

Piratage par des individus ou des États, manipulations numériques… ce podcast nous plonge en immersion dans les services qui luttent contre la cybermenace, pour comprendre comment la France se défend et s'arme dans le cyberespace.

1 - La guerre cyber
2 - La démocratie dans le viseur
3 - Les victimes de cyberattaques
4 - La justice face aux cybercriminels
5 - Hackeurs au service de la société

- ***Histoire des codes secrets***, titre original en anglais : ***The Code Book***, Simon Singh, 504 pages, 1999 (pour la 1re édition)



De tous temps, les codes secrets ont été un outil indispensable dans les affaires d'ordre politique, diplomatique, militaire. Ils ont décidé du sort des peuples, des armées, quelquefois des amants…

De l'arrestation de Marie Stuart à l'entrée en guerre des Etats-Unis pendant la Seconde Guerre mondiale, des messages cachés dans la chevelure des émissaires grecs aux salles de calcul de la National Security Agency, ce livre, aussi excitant qu'un roman policier, déploie une véritable fresque historique.

- ***Histoire mondiale des services secrets***, Rémi Kauffer, Tempus Perrin, 2017

Une histoire totale des services secrets de l'Antiquité à nos jours.

En couvrant plus de vingt siècles d'histoire du renseignement dans plus de vingt pays, Rémi Kauffer fait la lumière sur le milieu ô combien opaque et captivant des services secrets. On y découvre les grands services de renseignement, les moins connus aussi, les agents secrets, les taupes et leurs techniques, ainsi que les succès et échecs des opérations qui rythment l'Histoire. Pas moins de trente-cinq années d'investigation auront été nécessaires à l'auteur pour livrer cette somme sans égale.