ChatGPT

Rapport sur le renseignement

Introduction : Le terme *renseignement* désigne à la fois une information jugée précieuse pour orienter les décisions d'une organisation (notamment un État) et l'activité consistant à produire de telles informations [1]. En pratique, il s'agit de recueillir, analyser et diffuser des données souvent sensibles afin d'éclairer les choix stratégiques des autorités. Par métonymie, le mot *renseignement* désigne aussi l'ensemble des organismes spécialisés (services de renseignement civils, militaires, intérieurs, extérieurs, etc.) consacrés à ces activités [2]. Longtemps assimilé dans la culture populaire à l'« espionnage » clandestin, le renseignement recouvre en réalité un spectre bien plus large d'actions de collecte (ouvertes ou secrètes), d'analyse et de protection. Ce rapport fait le point sur les différents aspects du renseignement, en abordant successivement le renseignement militaire, le renseignement civil, l'évolution historique du renseignement, le fonctionnement actuel des services, le cadre légal et éthique, ainsi que les technologies employées.

1. Renseignement militaire

Définitions et objectifs

Le **renseignement militaire** se concentre sur l'obtention d'informations concernant les forces adverses, leurs moyens, leurs méthodes, le terrain et, plus largement, tout élément présentant un intérêt pour la conduite des opérations militaires [3]. Son objectif fondamental est de réduire l'incertitude liée aux menaces et à l'environnement des forces armées, afin de soutenir la planification et la conduite des actions militaires du niveau tactique jusqu'au niveau stratégique [4]. En temps de paix comme en conflit, les armées s'appuient sur le renseignement pour *« anticiper et résoudre les crises [...] prévenir les menaces »* et orienter leurs stratégies de défense [5]. Comme le souligne un document de l'OTAN, aucune opération ne peut se passer d'un appui renseignement, surveillance et reconnaissance : ces activités fournissent aux décideurs une compréhension accrue de la situation sur le terrain, dans les airs, en mer, dans l'espace ou le cyberespace, et permettent des décisions éclairées [6]. Autrement dit, le renseignement militaire vise à donner aux commandements « des yeux et des oreilles » sur le champ de bataille, conformément à l'adage de Sun Tzu selon lequel *« une armée sans agents secrets est un homme sans yeux ni oreilles »* [7].

Méthodes et moyens mis en œuvre

Pour remplir ces objectifs, les forces armées mettent en œuvre une variété de **méthodes de renseignement**. Celles-ci incluent le renseignement d'origine humaine (agents, éclaireurs ou informateurs recueillant des informations directes, y compris derrière les lignes adverses), le renseignement d'origine image (reconnaissance aérienne par avions ou drones, imagerie satellite), le renseignement électromagnétique (interceptions radio, radar, communications adverses), ainsi que le renseignement cyber (surveillance et intrusion dans les réseaux informatiques ennemis). La **surveillance** et la **reconnaissance** sont deux composantes essentielles : la surveillance consiste en un suivi continu d'une cible ou d'une zone, tandis que la reconnaissance est une mission ponctuelle visant à répondre à une question précise (par exemple localiser une position ennemie) [8] [9]. Ces activités produisent des données qui sont ensuite analysées et fusionnées par les spécialistes du renseignement militaire afin de devenir du renseignement exploitable pour les états-majors [10]. Les armées organisent ces fonctions suivant le *cycle du renseignement* (orientation des besoins, recherche d'informations, analyse, diffusion aux décideurs), avec des chaînes de traitement dédiées au sein des unités. La plupart

des forces armées disposent pour cela d'unités spécialisées à chaque échelon – jusqu'au niveau du bataillon – composées d'officiers et analystes formés en recherche d'information, analyse et langues étrangères [11]. Des unités spécialisées (par exemple des escadrons de reconnaissance, des cellules d'analyse du renseignement) opèrent de manière coordonnée pour recueillir les informations par des moyens spécifiques (drones, capteurs au sol, interceptions techniques, etc.) [3] [11]. Le renseignement militaire moderne s'appuie ainsi sur un vaste éventail de capteurs et de compétences analytiques pour éclairer en continu la situation tactique et stratégique.

Acteurs principaux

Les **acteurs du renseignement militaire** sont d'abord les services spécialisés de chaque pays intégrés aux forces armées. Presque toutes les armées modernes ont créé des structures dédiées : directions ou agences de renseignement au sein du ministère de la Défense, ainsi que des départements de renseignement dans les états-majors des forces terrestres, aériennes, navales, etc. Par exemple, la France dispose de la *Direction du renseignement militaire (DRM)*, créée en 1992 après la guerre du Golfe, chargée de centraliser le renseignement d'intérêt militaire pour l'état-major des armées [12] [13]. La DRM collecte et analyse des informations sur les théâtres d'opérations (ex. Sahel, Moyen-Orient, etc.) et fournit des notes aux autorités politico-militaires, y compris sur des conflits en cours (ainsi, durant la guerre en Ukraine, la DRM décortique quotidiennement l'évolution du front et en informe les décideurs français) [14] [15]. D'autres exemples incluent la **Defense Intelligence Agency (DIA)** américaine – agence centrale du renseignement de défense aux États-Unis –, le **GRU** en Russie (renseignement militaire russe), ou encore l'**Aman** en Israël. En pratique, ces services militaires travaillent en coordination avec les unités de renseignement de chaque corps d'armée (par exemple les sections de renseignement des brigades, ou les analystes d'état-major) et avec les services de renseignement extérieurs ou intérieurs si nécessaire. Dans les opérations multinationales, ils coopèrent avec les alliés : par exemple, l'OTAN s'appuie sur un système *JISR* (*Joint Intelligence, Surveillance and Reconnaissance*) qui mutualise les capacités alliées de collecte et d'analyse pour fournir une image partagée de la situation [16] [17]. Cette coopération permet de combiner des sources variées (satellites, avions de surveillance AWACS, drones, etc.) et de partager le renseignement pertinent entre partenaires, sous réserve des impératifs de sécurité et de secret propres à chaque nation [18] [19].

Exemples historiques et contemporains

Le renseignement militaire a joué un rôle déterminant dans de nombreux conflits. Historiquement, l'une des premières théorisations de son usage remonte à l'Antiquité : dans *L'Art de la guerre*, le général chinois Sun Tzu insistait déjà (VI^e siècle av. J.-C.) sur l'importance d'entretenir des réseaux d'agents secrets pour connaître les intentions et dispositions de l'ennemi [7]. Au fil des siècles, les stratèges ont intégré le renseignement à leur art : que ce soit la **reconnaissance du terrain** pratiquée par les légions romaines (explorateurs, éclaireurs) [20] ou les réseaux d'informateurs déployés en Europe à l'époque napoléonienne. Un exemple marquant est celui de Joseph Fouché, ministre de la Police de Napoléon : il avait constitué sous le Consulat et l'Empire un vaste réseau d'indicateurs sur tout le territoire, véritable *« appareil de contrôle universel »* qui lui conférait *« plus de puissance [...] que Napoléon lui-même »* pour surveiller la population [21]. Plus tard, à la fin du XIX^e siècle, les États ont institutionnalisé le renseignement militaire : la création en France du **Deuxième Bureau** (1856) chargé du renseignement de l'état-major, ou en Prusse les services de Bismarck (fameux espion Wilhelm Stieber), marquent l'essor de structures dédiées. Durant la Première Guerre mondiale, le renseignement militaire prend une dimension inédite avec l'usage systématique de l'écoute radio, du décryptage de codes (par exemple l'interception du télégramme Zimmermann en 1917) et de la photographie aérienne. La célèbre **Mata Hari** illustre l'importance – et les risques – du renseignement en temps de guerre : accusée d'espionnage au profit de l'Allemagne, elle fut fusillée par les Français en 1917 [22], tout comme plus d'une centaine de militaires français exécutés pour trahison pendant ce conflit [23].

Au cours de la **Seconde Guerre mondiale**, les opérations de renseignement et d'intoxication furent cruciales. Par exemple, l'état-major allié monta l'*opération Fortitude* (1944) pour tromper le renseignement allemand sur le lieu du débarquement, contribuant au succès du débarquement de Normandie [24]. En parallèle, les Alliés investirent massivement dans la **cryptanalyse** : à Bletchley Park en Angleterre, les premiers ordinateurs électromécaniques (**Colossus**) aidèrent des analystes comme Alan Turing à décrypter les messages chiffrés allemands (code **Enigma**), permettant de lire environ 10 % des communications ennemies en fin de guerre [25]. Ce renseignement d'origine électromagnétique (**SIGINT**) donna aux Alliés un avantage stratégique majeur, par exemple lors de la bataille de Midway dans le Pacifique où l'interception des codes japonais permit de préparer une contre-offensive victorieuse [26].

Pendant la **Guerre froide**, le renseignement militaire et civil connut un essor sans précédent, devenant un instrument central de la rivalité Est-Ouest. Les deux blocs mirent en place de vastes appareils d'espionnage : côté occidental, les États-Unis créèrent la **CIA** en 1947 (succédant à l'OSS de la Seconde Guerre mondiale) – officiellement pour éviter une nouvelle surprise stratégique comme Pearl Harbor plutôt que pour contrer directement l'URSS [27] – et l'**NSA** en 1952 pour le renseignement d'origine électromagnétique [28], tandis que le **FBI** se chargeait du contre-espionnage intérieur [29]. Côté soviétique, le **KGB** né en 1954 (héritier de la Tchéka et du NKVD) cumulait renseignement extérieur, contre-espionnage et sécurité intérieure. Cette période est marquée par des figures célèbres d'espions et de transfuges (les « Cinq de Cambridge » recrutés par le KGB au cœur du renseignement britannique, l'agent double Oleg Penkovsky qui informa l'Ouest des plans soviétiques, etc.) et par des opérations clandestines à l'échelle mondiale. Le renseignement d'imagerie spatiale fit ses débuts avec les premiers satellites espions américains **Corona** dès 1960, révolutionnant l'observation militaire. Le rôle du renseignement fut déterminant lors de crises comme celle des missiles de Cuba en 1962, où l'analyse de photos aériennes révéla la présence de missiles nucléaires soviétiques à Cuba.

Depuis la fin de la guerre froide, le renseignement militaire a dû s'adapter à des menaces plus diffuses (**terrorisme**, guérillas, prolifération d'armes) et aux conflits asymétriques. Par exemple, lors des interventions en Afghanistan (2001-2021) et en Irak (2003-2011), les armées occidentales ont intégré le renseignement en temps réel (drones armés fournissant du renseignement d'objectif, cellules de *fusion intelligence* analysant simultanément sources humaines et techniques) pour lutter contre des insurgés difficiles à distinguer de la population civile. Plus récemment, dans le conflit en Ukraine (2022-2025), le renseignement d'intérêt militaire s'est avéré crucial tant pour les Ukrainiens que pour les pays de l'OTAN : images satellites commerciales et militaires, interceptions de communications et informations fournies par les services occidentaux ont aidé à anticiper les plans d'invasion puis à suivre l'évolution des opérations [14] [15]. Ainsi, le renseignement militaire contemporain – fort des avancées technologiques – demeure plus que jamais un **facteur décisif** pour donner aux forces armées l'avantage informationnel sur le terrain, en dépit du « brouillard de la guerre » qui rend l'ennemi souvent furtif et diffus [30] [31].

2. Renseignement civil (intérieur, économique, technologique, numérique)

Le **renseignement civil** regroupe l'ensemble des activités de renseignement hors du domaine strictement militaire. Il comprend notamment le renseignement intérieur (sécurité du territoire et de la population), le renseignement lié à la vie économique et technologique, la surveillance numérique des communications, ainsi que les missions de police judiciaire et de sécurité publique utilisant des méthodes de renseignement. Ces domaines sont souvent confiés à des services de sécurité intérieure ou à des agences civiles spécialisées.

Renseignement intérieur et de sécurité

Le renseignement intérieur vise à **protéger les intérêts fondamentaux de l'État** sur le territoire national. Historiquement, durant la guerre froide, les services intérieurs occidentaux se focalisaient sur la lutte contre les ingérences étrangères (espions soviétiques, subversion politique) et la surveillance de groupes extrémistes ou subversifs [32]. En France par exemple, les *Renseignements généraux (RG)*, service de police créé au début du XX^e siècle, surveillaient les milieux politiques, syndicaux et divers mouvements susceptibles de troubler l'ordre public (ce qu'on appelait le **renseignement politique** [33]). De nos jours, les priorités du renseignement intérieur se sont déplacées vers la **lutte antiterroriste**, la prévention de l'**extrémisme violent**, le démantèlement des **réseaux criminels organisés** (trafics de drogue, mafias, etc.), ainsi que la **contre-ingérence** (contre-espionnage) visant à détecter et contrer les espions étrangers sur le sol national [34]. Ainsi, un service de renseignement intérieur moderne consacrera ses efforts à repérer d'éventuelles cellules terroristes, surveiller des individus radicalisés, infiltrer des réseaux criminels internationaux ou encore déjouer les cyberattaques et opérations d'influence menées par des puissances adverses.

Les **services de sécurité intérieure** accomplissant ces missions varient selon les pays. En France, la principale agence civile chargée du renseignement intérieur est la *Direction générale de la sécurité intérieure (DGSI)*, créée en 2014 (succédant à la DCRI) et placée sous l'autorité du ministère de l'Intérieur. Elle est compétente en matière de contre-terrorisme, contre-espionnage, protection du patrimoine économique, et plus généralement de prévention des atteintes à la sûreté de l'État. Aux côtés de la DGSI opèrent d'autres entités à vocation plus ciblée, comme le *Service central du renseignement territorial (SCRT)* de la Police nationale (issu de la réorganisation des ex-RG, axé sur la veille de l'ordre public et des phénomènes de société) [35], ou encore le *Renseignement pénitentiaire* chargé du suivi des détenus radicalisés [36]. À l'étranger, on peut citer le **FBI** aux États-Unis pour le contre-espionnage et l'anti-terrorisme intérieur, le **MI5** au Royaume-Uni pour la sécurité du territoire, ou encore le **BfV** en Allemagne (Office fédéral de protection de la Constitution). Ces services de renseignement intérieur travaillent souvent en lien étroit avec les forces de police et de gendarmerie, et partagent des informations avec les services de renseignement extérieurs ou militaires lorsque les menaces dépassent les frontières.

Renseignement économique et technologique

Le **renseignement économique** consiste à collecter et analyser des informations relatives aux **secteurs économiques, industriels, scientifiques et technologiques**, dans un objectif de défense des intérêts nationaux et de compétitivité. Au niveau des États, cela inclut le soutien aux entreprises nationales face à la concurrence internationale, la veille sur les marchés étrangers, la **protection des secrets technologiques** et la **lutte contre l'espionnage industriel** mené par des puissances ou firmes adverses [37] [38]. Les gouvernements considèrent de plus en plus l'information économique comme un enjeu de souveraineté, parlant parfois de *« guerre économique »* [38]. Concrètement, les services spécialisés peuvent surveiller les investissements étrangers stratégiques, détecter des tentatives d'ingérence économique (par exemple des cyberattaques visant des entreprises nationales ou des vols de brevets) et informer les décideurs des risques (pénuries, manipulations de cours, etc.). Ils mènent aussi des **opérations d'influence économique** (par exemple pour appuyer l'obtention de contrats à l'étranger par des entreprises nationales) ou, inversement, des contre-mesures pour empêcher des États rivaux d'obtenir des technologies sensibles.

Dans le secteur privé, on parle d'**intelligence économique** pour désigner les activités légales de collecte d'informations ouvertes au profit des entreprises [39]. Celles-ci recoupent la veille technologique, la veille concurrentielle et l'analyse de l'environnement (réglementation, nouveaux acteurs, innovations) afin d'éclairer la stratégie de l'entreprise. Des sociétés spécialisées se sont

développées depuis les années 1990 pour fournir ce type de renseignement commercial et industriel aux entreprises, de façon licite (analyse de sources publiques, bases de données, etc.) [40]. Néanmoins, la frontière est parfois mince entre l'intelligence économique légale et l'espionnage industriel illégal (vol de secrets de fabrication, de données sensibles, etc.). Des affaires retentissantes ont mis en lumière la compétition acharnée dans des domaines comme l'aéronautique, l'informatique ou l'énergie – par exemple l'affaire d'espionnage entre Airbus et Boeing, ou des cyberintrusions attribuées à des hackers liés à des États cherchant à voler des technologies (comme le piratage de laboratoires pharmaceutiques ou de startups innovantes). Les services de renseignement d'État jouent ici un double rôle : offensif (espionner pour le compte de son économie) et défensif (protéger ses entreprises des espions étrangers). Ainsi, la France a mis en place depuis 2016 une *Coordination nationale du renseignement et de la lutte contre les ingérences économiques* pour renforcer la protection du patrimoine scientifique et industriel. De même, des cellules spécialisées au sein de services intérieurs (par exemple le département *« sécurité économique »* de la DGSI) traquent les tentatives d'ingérence économique étrangère (rachats hostiles, agents infiltrés dans des filiales, etc.).

Surveillance numérique et renseignement technologique

La **surveillance numérique** désigne l'ensemble des techniques permettant de surveiller les communications et activités dans le cyberespace. Avec la généralisation d'Internet, des smartphones et des réseaux sociaux, le renseignement a dû investir massivement le champ numérique. Les services de renseignement interceptent désormais des volumes colossaux de données transitant par les câbles sous-marins, les serveurs ou les ondes hertziennes, dans le but d'y détecter des menaces pour la sécurité (préparation d'attentats, propagande terroriste, cyberespionnage, etc.). On distingue généralement la **surveillance de masse** (collecte indiscriminée de métadonnées téléphoniques, de paquets Internet, etc., afin d'y appliquer des filtres et algorithmes) de la **surveillance ciblée** (mise sur écoute d'individus ou de groupes précis, après autorisation légale) [41] [42]. Les révélations d'Edward Snowden en 2013 ont mis en lumière l'ampleur planétaire de ces surveillances : la NSA américaine et ses partenaires avaient mis en place des programmes comme **PRISM** (accès aux données des géants du web tels que Google, Facebook, Microsoft, Apple…) et **XKeyscore** (analyse large du trafic Internet mondial) pour espionner les communications à une échelle sans précédent [43]. Ces pratiques ont suscité un vaste débat public et conduit à certaines réformes (voir section Cadre légal), mais elles n'ont pas fondamentalement cessé [44] [45]. En effet, les agences continuent de considérer l'exploitation du renseignement numérique comme essentielle : *« il n'est pas utile d'avoir un service de renseignement s'il se limite à ce qu'on peut lire dans le journal »*, déclarait en 2014 le président américain Barack Obama pour justifier la poursuite de ces interceptions, rappelant que par définition *« le travail du renseignement est de découvrir ce que pensent et font [les acteurs étrangers] »* [46].

Plusieurs services sont spécifiquement dédiés à la surveillance technologique. Par exemple, au Royaume-Uni le **GCHQ** (Government Communications Headquarters) est l'agence technique chargée du renseignement d'origine électromagnétique et cyber, équivalent de la NSA aux États-Unis. En France, la DGSE possède une importante direction technique responsable des interceptions électroniques dans le cadre du renseignement extérieur, tandis qu'au niveau intérieur la DGSI et les services de police disposent d'unités spécialisées en cybersurveillance (suivi des activités criminelles en ligne, infiltration des réseaux de cybercriminalité, etc.). Par ailleurs, des *plates-formes nationales de captation* ont été mises en place (écoute des communications téléphoniques, balayage du web) avec l'autorisation du Premier ministre sous le contrôle d'une autorité administrative indépendante (voir cadre légal).

La **surveillance numérique** comporte aussi un volet offensif : les services de renseignement développent des capacités de **lutte informatique offensive (LIO)**, c'est-à-dire de cyberattaque. Celles-ci peuvent servir à neutraliser des infrastructures adverses (radars, réseaux de communication) en cas de conflit, ou à infiltrer discrètement les ordinateurs d'une cible pour en extraire des informations (*hacking*

d'un ministère étranger, implantation de logiciels espions type **Pegasus** sur les téléphones de suspects, etc.). De plus, le renseignement technologique englobe la surveillance des systèmes de communication chiffrés. Les avancées en cryptographie (messageries chiffrées de bout en bout, VPN…) compliquent la tâche des agences, qui investissent en contrepartie dans la **cryptanalyse** (briser ou contourner les codes de chiffrement) et la **surveillance technique** (exploiter des vulnérabilités zero-day, mettre des *backdoors* avec l'aide éventuellement des fabricants). On se souvient que pendant des décennies, la CIA et la BND allemande ont discrètement vendu à de nombreux pays des machines de chiffrement truquées (affaire **Crypto AG** dévoilée en 2020), ce qui leur a permis de lire des flots de communications diplomatiques et militaires étrangères sans résistance. Aujourd'hui, la cryptanalyse s'appuie sur des **supercalculateurs** et des mathématiciens de haut niveau, ainsi que sur l'essor potentiel de l'**informatique quantique** qui fait peser une menace à moyen terme sur les algorithmes de chiffrement actuels.

En somme, le renseignement civil couvre un périmètre très étendu allant de la lutte antiterroriste intérieure à la guerre économique, en passant par la maîtrise des nouvelles technologies de l'information. Les services de sécurité intérieure, les cellules de renseignement financier (telles que *TRACFIN* en France, chargé de suivre les circuits financiers clandestins [47]), les unités de renseignement criminel dans la police et la gendarmerie, ou encore les antennes locales de renseignement territorial, contribuent tous à collecter du renseignement civil. Leur action préventive a permis de déjouer des attentats, démanteler des réseaux criminels ou espionner des organisations extrémistes. Toutefois, la puissance des outils de surveillance numérique qu'ils utilisent soulève des enjeux de libertés publiques qui seront abordés plus loin.

3. Histoire du renseignement : des origines à nos jours

Antiquité et Moyen Âge

Le **renseignement** est souvent décrit comme *« le second plus vieux métier du monde »*. En effet, dès qu'il y a eu des rivalités politiques ou militaires, l'espionnage et la recherche d'informations sensibles ont existé. Des textes anciens attestent de ces pratiques : le traité militaire chinois de Sun Tzu (VI^e s. av. J.-C.) consacre un chapitre entier aux agents secrets et à l'importance de connaître l'ennemi [7]. Dans la Bible ou *L'Iliade* d'Homère, on trouve également des récits d'espionnage, de reconnaissance furtive ou d'intoxication de l'ennemi [48]. Dans l'Empire romain, les généraux employaient des éclaireurs (*speculatores*, *exploratores*) pour obtenir des renseignements militaires [20], et des services de poste impérial (*frumentarii*) servaient parfois de réseau d'information à l'empereur. Au Moyen Âge, le renseignement restait artisanal : les princes et rois utilisaient des émissaires, des marchands ou des religieux comme informateurs. Certaines cités italiennes de la Renaissance avaient développé un véritable système de courriers cryptés et de maîtres de poste interceptant le courrier (prémices du *cabinet noir*). À la fin du XV^e siècle, Louis XI en France était réputé pour son réseau d'« hommes de confiance » à travers l'Europe, préférant la ruse et la subversion à l'affrontement direct [49]. De même, la reine Élisabeth I^re d'Angleterre s'appuyait sur son secrétaire d'État Francis Walsingham, souvent considéré comme l'un des premiers « maîtres espions » modernes, qui déjoua entre autres les complots catholiques grâce à un réseau d'agents et à la lecture de correspondances chiffrées.

Époque moderne (XVII^e–XIX^e siècles)

L'époque moderne voit la **professionnalisation du renseignement**. En France, le Cardinal de Richelieu (XVII^e s.) mit sur pied un *cabinet noir* chargé d'ouvrir et de décrypter le courrier pour le compte du roi. Plus tard, sous Louis XV, un autre *cabinet noir* opérait à la Poste aux lettres de Paris pour intercepter secrètement les missives d'ambassadeurs ou de suspects. Sous la Révolution et l'Empire, la figure de Joseph Fouché illustre l'efficacité – et l'opacité – d'un service de renseignement intérieur tentaculaire

(voir section précédente). Napoléon I^er créa également en 1804 un *Bureau des secrets d'État* consacré à l'espionnage extérieur. Au XIX^e siècle, l'émergence des États-nations et des armées de conscription s'accompagne de la création des premiers véritables **services de renseignement modernes** : la *Section de Statistique* autrichienne (créée en 1850), le *Deuxième Bureau* français (1856) au sein de l'état-major, ou l'**Intelligence Branch** britannique (1873) posent les bases d'organismes permanents dédiés au recueil d'informations militaires et diplomatiques. Ces bureaux sont encore de petite taille, souvent subordonnés aux opérations militaires. Néanmoins, leur influence apparaît lors de conflits comme la guerre franco-prussienne de 1870 où le renseignement prussien fut jugé supérieur (grâce au réseau d'agents de Wilhelm Stieber, souvent qualifié d'« espion de Bismarck ») [50] . Cette époque voit aussi les premiers scandales d'espionnage publics : en France, *l'affaire Schnaebelé* (1887) – du nom d'un officier français arrêté pour espionnage par les Allemands – ou surtout *l'affaire Dreyfus* (1894) qui débuta par l'identification d'une fuite de renseignements vers l'Allemagne au sein de l'état-major français [50] [51] . L'affaire Dreyfus, bien qu'elle fût une tragique erreur judiciaire, démontra l'impact du renseignement sur la sphère publique et la raison d'État. Elle entraîna en outre une modernisation du **contre-espionnage** français (avec la création en 1899 d'une *Section de Statistique* bis dédiée à la surveillance des espions internes).

Guerres mondiales et entre-deux-guerres

Le **XX^e siècle** catapulte le renseignement sur le devant de la scène internationale. Durant la Première Guerre mondiale (1914-1918), on assiste à l'institutionnalisation de grandes unités de renseignement dans les armées belligérantes : en France, le *Deuxième Bureau* du général Dubail coordonne espionnage et contre-espionnage, tandis que le Royaume-Uni développe le *MI5* (1909, contre-espionnage intérieur) et le *MI6* (1909, renseignement extérieur). L'usage intensif de la télégraphie sans fil conduit à la création de centres d'écoute radio (la *Room 40* de l'Amirauté britannique excella dans le déchiffrage des codes navals allemands). Les exploits des services secrets pendant la Grande Guerre alimentèrent la littérature d'espionnage (le personnage de **James Bond** s'inspirera plus tard de ces figures héroïques ou romanesques). L'entre-deux-guerres voit se structurer les grandes agences : l'URSS crée le **NKVD** (qui mènera des opérations d'infiltration en Occident dans les années 1930), les États-Unis tardent à se doter d'un service civil centralisé et s'appuient surtout sur les attachés militaires à l'étranger. La montée des périls dans les années 1930 accélère tout de même la coopération entre services alliés, notamment en matière de cryptographie (les Polonais réussissent à percer la version initiale de la machine Enigma allemande dès 1932, exploit transmis aux Français et Britanniques).

Pendant la **Seconde Guerre mondiale (1939-1945)**, le renseignement joue un rôle capital dans l'issue des hostilités. Chaque camp dispose de multiples branches : l'Allemagne nazie a l'**Abwehr** (renseignement militaire, sous l'amiral Canaris) et le **RSHA** (services secrets SS de Himmler), qui affrontent le **MI5** britannique sur le terrain du contre-espionnage [24] . Les Alliés montent des opérations d'intoxication pour tromper l'ennemi (citons encore l'opération Fortitude et l'utilisation d'agents doubles comme Juan Pujol, alias *Garbo*, qui trompa les Allemands sur le débarquement). Sur le front du renseignement technologique, la lutte anti-sous-marine dans l'Atlantique dépendit en partie de la capacité à décoder les messages Enigma de la Kriegsmarine, ce que parvinrent à faire les cryptanalystes de Bletchley Park en améliorant constamment leurs techniques [25] . Dans le Pacifique, l'écoute radio de la US Navy permit de préparer l'embuscade victorieuse de Midway en 1942 [26] , en décodant les communications navales japonaises. La résistance intérieure dans les pays occupés fournit également du renseignement précieux (sabotages, rapports sur les mouvements de troupes, etc.), souvent coordonné par les services secrets alliés (le **SOE** britannique ou le **BCRA** de la France libre). En 1945, l'ampleur et l'efficacité des services de renseignement sortent considérablement renforcées de la guerre, tout comme le prestige de certaines figures du renseignement (les « casseurs de codes » de Bletchley, les agents du SOE, etc.).

Guerre froide (1947-1991)

L'après-guerre se caractérise par la structuration durable des **grandes agences de renseignement** et leur expansion au cœur de la rivalité bipolaire. En 1947, les États-Unis fondent la **CIA** via le National Security Act, dotant ainsi l'exécutif d'un service de renseignement extérieur pérenne, chargé aussi de conduire des **opérations clandestines** à l'étranger (covert operations) pour contrer l'influence soviétique [27]. La même loi crée le **National Security Council** et amorce la coordination de la « Communauté du renseignement » américaine, qui finira par regrouper des dizaines d'agences civiles et militaires (DIA, NSA, services des armées, etc.). L'URSS, de son côté, réforme ses services plusieurs fois : après la Tchéka de l'époque révolutionnaire puis le NKVD de Staline, elle établit en 1954 le **KGB** qui concentre un pouvoir immense sur le renseignement extérieur, le contre-espionnage et la surveillance interne [52]. La guerre froide voit aussi l'essor d'agences dans les pays alliés : création du **BND** (service extérieur ouest-allemand) en 1956, du **DGSE** français en 1982 (héritier du SDECE), etc.

Les méthodes de renseignement pendant la guerre froide englobent tout le spectre : infiltration d'agents (les espions soviétiques réussissent à pénétrer le programme nucléaire occidental, cas de Klaus Fuchs en 1950 ; à l'inverse, la CIA obtient des informations cruciales via des hauts gradés du bloc de l'Est comme le colonel Penkovsky en 1961), usage intensif des **satellites espions** (le programme CORONA et ses successeurs fournissent aux Américains des photographies détaillées du territoire soviétique dès les années 1960), interceptions planétaires avec le réseau **ECHELON** mis en place par les pays anglo-saxons (Five Eyes) pour capter les communications internationales, sans oublier les **opérations clandestines** et coups tordus (renversement de gouvernements, soutien secret à des mouvements armés, assassinats ciblés de leaders communistes ou, côté soviétique, exécutions d'opposants exilés, etc.). Les affrontements indirects de la guerre froide – par services interposés – se manifestent à travers des crises retentissantes comme l'affaire de l'**U-2** (un avion espion américain abattu au-dessus de l'URSS en 1960, révélant au monde les activités d'espionnage aérien), l'**affaire Farewell** (1981, recrutement par la DST française d'un officier du KGB qui dévoila l'ampleur de l'espionnage industriel soviétique en Occident), ou encore l'expulsion réciproque de dizaines d'agents sous couverture diplomatique (le *jeu des expulsions* récurrent entre Est et Ouest). C'est aussi l'âge d'or des romans et films d'espionnage, qui popularisent les figures de l'agent secret – souvent idéalisées – mais aussi du transfuge et de la taupe infiltrée (John le Carré dépeint magistralement ces conflits de l'ombre).

En 1991, l'effondrement de l'URSS ne fait pas disparaître les services secrets, bien au contraire. Comme l'observe le vice-président du Conseil d'État français, *« la fin de la guerre froide et la disparition de l'URSS en 1991 ont maintenu ou replacé le renseignement sur le devant de la scène, car [elles] ont fait émerger un monde encore plus instable et incertain »* avec des menaces multiples [53] [54]. Les années 1990 voient les agences se redéployer vers de nouveaux enjeux : prolifération nucléaire (suivi du programme atomique nord-coréen ou iranien), criminalité organisée transnationale (drogue, blanchiment), et surtout terrorisme islamiste montante (déjà illustré par des attentats comme celui du World Trade Center en 1993). Cette période est également marquée par la révélation au grand jour de certaines pratiques illégales des services pendant la guerre froide : en 1975, aux États-Unis, la Commission Church du Sénat avait mis au jour des abus de la CIA (écoutes sans mandat, complots d'assassinat contre Castro et autres dirigeants, surveillance de militants civils) conduisant à une première vague de réformes et à la mise en place d'un contrôle parlementaire renforcé. De même, divers scandales éclatent en Europe, comme l'affaire **Gladio** (réseaux stay-behind de l'OTAN impliqués dans la politique intérieure italienne) ou, en France, l'affaire du **Rainbow Warrior** (le sabotage par les agents de la DGSE d'un navire de Greenpeace en 1985, qui entraîne une crise diplomatique avec la Nouvelle-Zélande). Ces événements ont nourri une demande de transparence et de contrôle démocratique du renseignement, préparant les évolutions législatives ultérieures.

Époque contemporaine (années 2000-2020)

Les attentats du **11 septembre 2001** marquent un tournant majeur et une **remobilisation massive** du renseignement à l'échelle mondiale. Face au terrorisme djihadiste transnational (Al-Qaïda, puis Daech), les gouvernements investissent d'énormes moyens pour renforcer leurs capacités de renseignement : aux États-Unis, une refonte de la communauté du renseignement crée le poste de *Director of National Intelligence* (2004) pour mieux coordonner la multitude d'agences, tandis que le **Patriot Act** (2001) élargit drastiquement les pouvoirs de surveillance et de perquisition du FBI et de la NSA. En Europe, les services intérieurs et extérieurs accroissent leurs échanges d'informations sur les réseaux terroristes, et de nouvelles structures voient le jour (par exemple, le Royaume-Uni crée en 2006 le **JTAC** – Joint Terrorism Analysis Centre – pour centraliser l'analyse de la menace terroriste). Malgré cela, les années 2000 et 2010 sont endeuillées par de nombreux attentats, ce qui conduit à *institutionnaliser* encore davantage la coopération renseignement-police-armée (cellules communes, fusions de bases de données) et à développer les méthodes de surveillance de masse déjà évoquées.

Le renseignement contemporain fait face à deux facteurs déterminants : la **révolution numérique** et l'**évolution du cadre juridique et éthique**. D'une part, l'explosion des communications électroniques, du volume de données disponibles (Big Data) et des outils d'IA a fourni au renseignement de nouveaux outils puissants, mais a aussi complexifié la tâche (masse d'informations à trier, chiffrement répandu, etc.). D'autre part, la société civile et les instances démocratiques exigent davantage de garanties contre les abus. En 2013, les révélations d'Edward **Snowden** sur la surveillance à grande échelle menée par la NSA et ses alliés occidentaux ont provoqué un choc planétaire [44]. Des chefs d'États (dont Angela Merkel, dont le téléphone avait été surveillé) ont protesté, des associations de défense des libertés ont saisi les tribunaux, et plusieurs pays ont dû adapter leurs lois : aux USA, le *Freedom Act* de 2015 a mis fin à certains programmes de collecte massive de métadonnées téléphoniques, et en France la **loi relative au renseignement de 2015** a pour la première fois encadré légalement les techniques de surveillance des services (voir section suivante) [55]. En parallèle, l'Union européenne a adopté le **RGPD** (Règlement général sur la protection des données) en 2016, qui renforce la protection de la vie privée, y compris face aux ingérences éventuelles des États [55].

Ces évolutions montrent que le renseignement est dans un **processus constant de légitimation et de contestation**. À chaque scandale ou « affaire » (Dreyfus, Watergate, écoutes de la NSA…), succède une phase de réforme ou de justification de l'action des services, sans que ceux-ci disparaissent – au contraire, ils voient souvent leurs moyens renforcés après coup, la menace ayant entre-temps évolué [56] [57]. Aujourd'hui, au milieu des années 2020, les services de renseignement doivent faire face simultanément au **retour de menaces étatiques classiques** (tensions géopolitiques avec des puissances rivales, comme le montrent les crises en Ukraine ou autour de Taïwan) et à la **persistance de menaces diffuses** (terrorisme, extrémismes violents, cyberattaques par des acteurs non étatiques). Cette conjonction conduit à un maintien – voire une augmentation – des budgets et effectifs du renseignement un peu partout dans le monde [57]. Par exemple, en France, le budget de la DGSE (renseignement extérieur) a plus que doublé depuis 2008 et dépassera 1 milliard d'euros en 2025 [58] [59], traduisant l'importance accordée à la fonction renseignement dans la défense nationale. Le renseignement reste ainsi *« en première ligne de la défense de notre sécurité et de nos intérêts »*, comme l'affirmait le Livre Blanc sur la défense de 2008 [60].

4. Fonctionnement actuel des services de renseignement

Structure et organisation générale

La plupart des États disposent aujourd'hui de **plusieurs services de renseignement spécialisés**, chacun ayant son domaine de prédilection. On distingue généralement les services de renseignement

intérieur (sécurité du territoire national), *extérieur* (espionnage à l'étranger), *militaire* (renseignement au profit des forces armées), et parfois d'autres branches thématiques (renseignement financier, criminel, technique…). Par exemple, la France identifie officiellement dix services de renseignement dans sa « Communauté du renseignement », dont la DGSE (extérieur), la DGSI (intérieur), la DRM (militaire), la DRSD (sécurité militaire), la DNRED (douanes), Tracfin (financier) et quelques unités spécialisées de police et gendarmerie [61] [62]. Cette pluralité permet de couvrir un large spectre de menaces en spécialisant les compétences, mais elle pose des défis de coordination. En effet, chaque service dispose de ses propres bases de données, de sa culture institutionnelle et de sa chaîne hiérarchique, ce qui peut engendrer cloisonnement ou rivalités. Inversement, certains pays à plus petite échelle choisissent de regrouper le renseignement dans une structure unique multi-missions, ce qui facilite le pilotage mais risque de concentrer excessivement le pouvoir et de limiter la diversité d'analyse [63].

Pour assurer la cohérence, de nombreux États ont mis en place des mécanismes de **coordination et de pilotage central**. Aux États-Unis, le *Director of National Intelligence (DNI)* coiffe depuis 2005 l'ensemble des 17 agences fédérales de renseignement, fixant les priorités et arbitrant le partage d'informations. En France, un *Conseiller national du renseignement* à l'Élysée (fonction créée en 2008) et depuis 2017 un *Coordonnateur national du renseignement et de la lutte contre le terrorisme (CNRLT)* rattaché au Président de la République veillent à la bonne synergie entre services. Des *unités interservices* ont également vu le jour pour des thématiques transverses comme l'antiterrorisme ou la contre-prolifération, réunissant des agents de plusieurs services dans un même centre opérationnel afin de partager leurs renseignements. Par exemple, l'Unité de Coordination de la Lutte Antiterroriste (UCLAT) en France (remplacée en 2017 par le Centre national du contre-terrorisme) était un organe de ce type. Au niveau gouvernemental, les services de renseignement sont généralement rattachés soit au ministère de l'Intérieur (pour les services de sécurité intérieure), soit au ministère de la Défense/Armées (pour les services militaires ou extérieurs), à quelques exceptions près. Ils relèvent directement du pouvoir exécutif, souvent du chef du gouvernement ou du chef de l'État dans le cas des services les plus sensibles. Par exemple, le directeur de la CIA aux États-Unis rend compte au Président et siège au Conseil de sécurité nationale, tandis qu'au Royaume-Uni les chefs du MI5, MI6 et GCHQ reportent au Premier ministre via le Joint Intelligence Committee.

Chaîne de commandement et contrôle

La **chaîne de commandement** des services de renseignement est typiquement pyramidale, avec à son sommet une autorité politique (ministre ou Premier ministre) validant les grandes orientations. En France, les services sont sous l'autorité de leur ministre de tutelle mais certaines opérations particulièrement sensibles doivent être autorisées par le cabinet du Premier ministre (c'est le cas des interceptions de communications, autorisées par le Premier ministre sur avis de la CNCTR – voir section légale). La réforme de la gouvernance du renseignement entreprise après 2008 a d'ailleurs renforcé le rôle du Premier ministre dans le pilotage de la communauté du renseignement [64]. Au quotidien, chaque service est dirigé par un haut fonctionnaire (directeur ou directeur général) généralement issu du sérail (haut gradé militaire pour la DRM, préfet ou policier haut gradé pour la DGSI, diplomate ou militaire pour la DGSE…). Ce directeur fixe les priorités internes en fonction des *directives nationales du renseignement* édictées au plus haut niveau de l'État. Il doit arbitrer l'allocation des ressources entre les différentes missions (par exemple, consacrer plus de moyens au contre-terrorisme si la menace est élevée, ou au renseignement économique selon les orientations du gouvernement). Le **processus de décision** dans le renseignement suit en principe le schéma "demande – recueil – analyse – diffusion" : les *demandes de renseignement* (requirements) sont exprimées par les décideurs politiques ou militaires, elles sont traduites en plans de recherche par les services, qui collectent et analysent, puis restituent des notes et rapports en réponse. Ces notes peuvent servir à la décision stratégique (par exemple, informer le président de la République de la situation d'un conflit) ou à l'action opérationnelle (par exemple, guider une unité antiterroriste vers une cible).

Pour éviter les dérives et garantir l'efficacité, certains pays ont établi des **principes de coordination et de contrôle interne**. Par exemple, aux États-Unis, la CIA n'a pas le droit d'opérer sur le sol national – rôle réservé au FBI – afin de cloisonner renseignement extérieur et intérieur et prévenir les abus domestiques [29]. En pratique cependant, ces frontières peuvent être floues (une agence extérieure coopère avec l'intérieure si une menace étrangère se manifeste sur le territoire). D'où la nécessité de *"ponts"* institutionnels : cellules mixtes, officiers de liaison détachés dans d'autres services, bases de données partagées. L'un des défis actuels est de favoriser le **partage d'information** entre agences sans compromettre la sécurité des sources. Des concepts comme la *"communauté du renseignement"* (intelligence community) encouragent la circulation de l'information pertinente vers tous ceux qui en ont le besoin, plutôt qu'une rétention selon le principe du *"besoin d'en connaître"* uniquement [19]. L'OTAN par exemple promeut l'approche *"responsibility to share"* pour ses membres, bien qu'en pratique chaque pays conserve ses réticences à tout partager systématiquement [19].

Coopération internationale

Le **renseignement est par nature transnational**, car les menaces (terrorisme, prolifération, espionnage, crime organisé) dépassent souvent les frontières. De ce fait, les services de renseignement entretiennent entre eux des réseaux de coopération plus ou moins formalisés. L'alliance la plus connue est celle des *Five Eyes* (États-Unis, Royaume-Uni, Canada, Australie, Nouvelle-Zélande) formée dès 1946 pour le partage du renseignement d'interception SIGINT, qui demeure extrêmement étroite encore aujourd'hui. Dans le cadre de l'OTAN, des échanges de renseignement se font couramment lors des opérations conjointes : ainsi en Afghanistan (2001-2014), les officiers de renseignement de différents pays alliés travaillaient côte à côte au sein d'un même QG. L'OTAN a d'ailleurs mis en place une structure permanente de renseignement (le **NATO Intelligence Fusion Centre** et la division renseignement du SHAPE) pour consolider les informations sur les zones d'intérêt de l'Alliance. Au niveau européen, la coopération reste plus intergouvernementale : les services de l'UE se rencontrent dans des forums comme le *Club de Berne* (forum informel des chefs de services européens) ou s'échangent des données via Europol pour le contre-terrorisme et la criminalité. L'UE a toutefois créé une petite unité d'analyse, le *Intelligence and Situation Centre (IntCen)*, pour fournir aux instances européennes une synthèse de renseignements civils (fournis volontairement par les États membres).

La coopération bilatérale est également cruciale : par exemple, la France entretient des liens de renseignement privilégiés avec des pays africains pour le suivi des groupes terroristes au Sahel, ou avec l'Allemagne et l'Espagne en matière antiterroriste en Europe. De même, des services historiquement concurrents peuvent collaborer ponctuellement sur un enjeu commun – on a vu par exemple les services russes et occidentaux coopérer brièvement après le 11 septembre 2001 contre Al-Qaïda, ou plus récemment échanger des informations sur des combattants de Daech. Cependant, cette coopération internationale se heurte parfois à la *realpolitik* : un service allié dans un contexte peut être rival dans un autre. Les affaires d'espionnage entre pays amis (comme l'écoute par la NSA de dirigeants européens révélée en 2013 [65]) rappellent que les services de renseignement n'hésitent pas à cibler également des partenaires, ce qui peut créer des tensions diplomatiques. Pour cette raison, la confiance et la réciprocité sont des maîtres-mots dans les échanges de renseignement : la règle tacite est souvent *"pas de service, pas de renseignement"*, signifiant qu'un service étranger ne partagera ses informations sensibles qu'en échange d'une contribution équivalente ou d'un partenariat stable.

Ressources, budgets et effectifs

Le **budget des services de renseignement** est généralement couvert par le secret défense, mais on observe depuis quelques années davantage de transparence sur les grandes tendances. Dans les démocraties occidentales, les dépenses de renseignement ont connu une nette hausse depuis le début des années 2000 sous l'effet de la menace terroriste puis des nouveaux défis technologiques. Par

exemple, aux États-Unis, le budget total de la communauté du renseignement (National Intelligence Program) avoisinait 80 milliards de dollars en 2019 (chiffres non classifiés) – en forte progression par rapport aux années 1990. En France, le budget cumulé des services de renseignement est en croissance continue depuis le Livre blanc de 2008 : la DGSE, principal service extérieur, a vu ses moyens passer de 440 millions € en 2008 à plus d'1 milliard € en 2025 [59]. Cette hausse soutient des investissements dans le **cyber** et l'**intelligence artificielle**, domaines jugés prioritaires, ainsi que le renforcement des capacités d'interception technique et de traitement de données [66] [67]. Les effectifs des services augmentent en conséquence : la DGSE par exemple est passée de ~4400 agents en 2008 à plus de 6100 prévus en 2025 [68], et continue de recruter chaque année des centaines de profils qualifiés (ingénieurs informaticiens, linguistes, analystes, etc.). D'autres pays comparables affichent des niveaux de ressources similaires voire supérieurs : le BND allemand disposera d'environ 1,19 milliard € en 2025, et les agences britanniques MI6 et GCHQ emploient davantage d'agents que leurs homologues français, selon les auditions parlementaires [69] [70].

Une part significative du budget finance les **technologies spécialisées** (supercalculateurs, satellites, réseaux sécurisés) et les projets immobiliers ultra-sécurisés (nouveaux sièges, centres de données). Par exemple, la France a lancé le chantier d'un nouveau siège de la DGSE à Vincennes pour 2030, évalué à 1,34 milliard € [71], afin de regrouper sur un même campus ses milliers d'agents. Outre les dotations officielles, certains services bénéficient de **fonds spéciaux** ou fonds secrets, non détaillés publiquement, souvent utilisés pour les opérations sensibles (financer des informateurs, des actions clandestines, etc.). En France, le budget 2025 prévoit 72 millions € de fonds spéciaux destinés à l'ensemble des services, gérés directement par le Premier ministre [72].

La question des ressources est doublement sensible : **trop peu de moyens** risque de priver un service de capacités indispensables (par exemple, ne pas pouvoir renouveler un satellite d'observation vieillissant, c'est perdre du renseignement), tandis que **des moyens abondants mais mal contrôlés** peuvent conduire à des gaspillages ou des velléités d'échapper à l'encadrement légal. C'est pourquoi la plupart des pays soumettent désormais les budgets du renseignement à un *contrôle parlementaire* restreint et secret (voir plus loin), afin d'équilibrer efficacité et responsabilité.

Transparence, contrôle et réformes récentes

Traditionnellement, les services de renseignement opèrent dans le **secret** et sont peu enclins à la transparence. Cependant, pour conserver la confiance du public dans un État de droit, des mécanismes de contrôle démocratique ont été instaurés ou renforcés ces dernières années. Dans nombre de démocraties, il existe une **délégation parlementaire** ou une commission spécialisée chargée de superviser l'action des services, sans en révéler les détails opérationnels. Par exemple, le Parlement britannique dispose de l'*Intelligence and Security Committee* (ISC) qui examine à huis clos les politiques et dépenses du MI5, MI6, GCHQ et publie des rapports expurgés. En France, la *Délégation parlementaire au renseignement (DPR)*, créée en 2007, rassemble députés et sénateurs habilités Secret-Défense qui reçoivent des rapports d'activité annuels des services et peuvent formuler des recommandations [73]. Ces organes contribuent à une **meilleure transparence** sur l'organisation et la stratégie des services, sans compromettre le secret des opérations.

En complément, des **autorités administratives indépendantes** veillent au respect du cadre légal par les agences. Dans le cas français, la loi de 2015 a institué la **Commission nationale de contrôle des techniques de renseignement (CNCTR)**, qui doit être consultée avant toute mise en œuvre de techniques intrusives (écoutes, balises, etc.) et peut en contrôler la conformité ex post. De même, des **juges** peuvent être impliqués (en Allemagne, une cour fédérale autorise certaines surveillances ; aux États-Unis, la Foreign Intelligence Surveillance Court – FISC – approuve les demandes de surveillance électronique visant des cibles liées à l'étranger).

Les **réformes récentes** du secteur du renseignement ont souvent visé à l'inscrire dans un cadre légal clair et respectueux des libertés. En France, avant 2015, paradoxalement *« les activités de renseignement obéissaient à un no man's land juridique »* : il n'y avait pas de loi spécifique encadrant les pratiques comme les écoutes ou la géolocalisation par services spéciaux [74] [75]. La **loi du 24 juillet 2015 relative au renseignement** a comblé ce vide en définissant les finalités légitimes justifiant le recours aux techniques de renseignement (sécurité nationale, préservation des intérêts fondamentaux de la Nation limitativement énumérés : lutte contre le terrorisme, prolifération, ingérence étrangère, criminalité organisée, etc.) [76]. Elle a autorisé un éventail de techniques (écoutes téléphoniques, accès aux données de connexion, captation de paroles ou d'images, IMSI-catchers, etc.) sous réserve d'une procédure d'autorisation stricte (demande motivée par les services, accord du Premier ministre après avis de la CNCTR, durée limitée, données détruites au bout d'un certain temps) [77]. Cette loi a en outre **sanctuarisé le respect de la vie privée** en tête du Code de la sécurité intérieure, tout en reconnaissant que le renseignement reste un domaine d'exception par rapport au droit commun [78] [79]. Le Conseil constitutionnel français a validé l'essentiel du texte, n'en censurant que quelques dispositions trop floues et exigeant notamment l'intervention d'une autorité indépendante (CNCTR) pour autoriser l'exploitation de certaines données sensibles [80].

D'autres pays ont vécu des évolutions similaires après les scandales de surveillance de masse. Le *USA Freedom Act* de 2015 a mis fin à la collecte globale par la NSA des métadonnées téléphoniques domestiques (révélée par Snowden), la remplaçant par un système de réquisitions ciblées auprès des opérateurs. Au Royaume-Uni, l'**Investigatory Powers Act** 2016 (surnommé *« Charte des fouineurs »*) a légalement encadré – et en partie étendu – les capacités d'interception des agences, tout en instaurant des mécanismes de double validation (par un commissaire judiciaire) pour les opérations les plus intrusives. L'effet conjugué de ces lois est d'assurer que le renseignement s'exerce *« dans l'État de droit »* : la Cour européenne des droits de l'homme exige en effet que toute ingérence dans la vie privée soit *« précisément prévue par la loi »* et assortie de garanties pour éviter l'arbitraire [81].

Scandales et controverses

Malgré ces garde-fous, les **controverses** liées au renseignement demeurent nombreuses, signe des tensions inhérentes entre **sécurité** et **libertés**. Chaque révélation d'abus ou d'opération illégale suscite un débat sur la légitimité des méthodes utilisées. Parmi les grands scandales historiques, on cite évidemment le **Watergate** (1972-74) : l'utilisation des services de renseignement et de police par le président Nixon pour espionner ses opposants politiques a conduit à sa démission et à une profonde remise en cause du fonctionnement du FBI et de la CIA (avec les commissions Church et Pike). Dans les années 1980, l'affaire **Iran-Contra** dévoile que la CIA a contourné le Congrès pour financer clandestinement des rebelles au Nicaragua, ce qui entache la confiance dans le contrôle démocratique du renseignement américain. En France, les *« écoutes de l'Élysée »* sous François Mitterrand (où une cellule parallèle espionnait journalistes et personnalités) ont provoqué un scandale dans les années 1990, menant à des poursuites judiciaires contre les responsables de cette dérive.

Plus récemment, les **programmes de surveillance de masse** mis au jour par Snowden en 2013 ont déclenché une onde de choc mondiale. Non seulement ils ont révélé l'ampleur de la collecte de données sur des citoyens lambda (par exemple via PRISM), mais également l'espionnage de dirigeants alliés (téléphone de la chancelière Merkel, institutions européennes écoutées) [65]. Cela a sérieusement affecté la confiance entre partenaires occidentaux pendant un temps et relancé les revendications d'asile pour les lanceurs d'alerte. D'autres polémiques portent sur l'**usage des nouvelles technologies** : par exemple, l'utilisation du logiciel espion israélien **Pegasus** par certains États pour surveiller des journalistes, opposants ou défenseurs des droits humains a fait scandale en 2021-2022, illustrant le risque de détournement des outils de renseignement à des fins de répression politique.

Les **assassinats ciblés** menés par des services de renseignement posent également un défi éthique et juridique. Durant la « guerre contre le terrorisme », la CIA a eu recours à des frappes de drones armés pour éliminer des membres d'Al-Qaïda ou de groupes affiliés, y compris des ressortissants occidentaux comme l'américano-yéménite Anwar al-Aulaqi (tué par drone en 2011). Cette pratique de *targeted killing* soulève la question du respect du droit international et du droit à un procès équitable pour les cibles, et fut critiquée par des ONG et l'ONU. De même, l'élimination sur le sol étranger d'opposants ou d'ex-agents (cas d'Alexandre Litvinenko empoisonné au polonium à Londres en 2006 par des agents russes, ou de Jamal Khashoggi assassiné dans un consulat en 2018 par des agents saoudiens) choque l'opinion et entraîne des condamnations diplomatiques, mais témoigne hélas de pratiques loin d'être abandonnées par certains services.

Enfin, un enjeu persistant est la **surveillance politique interne** illégitime : dans les États autoritaires, les services de renseignement sont souvent instrumentalisés pour maintenir le régime en place en muselant l'opposition (on l'a vu récemment en Biélorussie ou à Hong Kong). Dans les démocraties, si les services s'écartent de leur mission pour surveiller des mouvements citoyens légaux ou pour servir les intérêts partisans d'un gouvernement, cela constitue une dérive grave. Des révélations comme le fichage illégal de syndicalistes par la DCRI française dans les années 2000, ou l'espionnage de journalistes aux États-Unis dans le cadre de fuites, ont alimenté des *affaires* qui, là encore, obligent à renforcer les garde-fous.

En conclusion de cette partie, on constate que le fonctionnement actuel des services de renseignement est un **équilibre délicat** : d'une part, doter ces services de l'organisation, des moyens et de la liberté d'action suffisants pour parer des menaces complexes et protéger efficacement la nation ; d'autre part, s'assurer qu'ils opèrent sous le contrôle de l'État de droit, sans empiéter indûment sur les libertés individuelles ni échapper à toute forme de redevabilité. Les réformes entreprises depuis une quinzaine d'années dans de nombreux pays vont dans le sens d'une professionnalisation accrue et d'un encadrement légal plus strict – deux conditions nécessaires pour légitimer durablement l'action de ces *« services secrets »* au sein de nos démocraties.

5. Cadre légal et éthique du renseignement

Lois encadrant le renseignement dans les démocraties

Longtemps, le renseignement a opéré dans l'ombre des textes juridiques, considéré comme un domaine régalien échappant au droit commun. Ce n'est plus le cas aujourd'hui dans la plupart des démocraties, où l'on a cherché à **formaliser légalement** l'activité de renseignement pour la soumettre au principe de légalité et à un contrôle équilibré. Un principe fondamental rappelé par la Cour européenne des droits de l'homme est que toute intrusion du renseignement dans la vie privée ou les libertés doit être *« précisément prévue par la loi »* et accompagnée de garanties appropriées [81]. En pratique, cela s'est traduit par l'adoption de lois spécifiques ou l'intégration d'un *cadre légal du renseignement* dans le droit national.

Aux États-Unis, le tournant fut l'après-Watergate : le Foreign Intelligence Surveillance Act (**FISA**) de 1978 a instauré un régime d'autorisation judiciaire pour les interceptions de communications sur le sol américain visant des puissances étrangères ou leurs agents. Ce texte a créé la FISA Court, qui siège à huis clos pour valider (ou refuser) les demandes de la NSA ou du FBI concernant la surveillance électronique de cibles liées à l'étranger. Par la suite, d'autres lois ont affiné le cadre (USA Patriot Act 2001 élargissant temporairement certaines prérogatives, puis USA Freedom Act 2015 restreignant la collecte en vrac des données domestiques). En outre, plusieurs **Executive Orders** (décrets présidentiels) précisent les missions et limites des agences – le fameux EO 12333 de 1981 définit les rôles de la CIA,

NSA, etc., et interdit par exemple formellement l'assassinat ciblé de personnes par des agents américains, même si cette interdiction a été contournée dans le cadre des opérations militaires anti-terroristes.

En Europe, beaucoup de pays ont attendu les années 2010 pour légiférer explicitement sur le renseignement. Au **Royaume-Uni**, après des scandales d'écoutes illégales dans les années 1980, une loi de 1989 a officialisé l'existence du MI5, du MI6 et du GCHQ et créé des commissaires indépendants pour surveiller leurs activités. Plus récemment, l'Investigatory Powers Act 2016 (IPA) a rationalisé l'ensemble des pouvoirs de surveillance (interceptions, piratage informatique, rétention de données) et mis en place un *Investigatory Powers Commissioner* chargé de superviser les agences et d'approuver en second regard les mandats délivrés par les ministres. L'IPA a ainsi fourni une base légale consolidée à des techniques comme la *bulk collection* (collecte massive de données) qui, auparavant, se faisaient sous des bases juridiques partielles contestées en justice. Le **Conseil de l'Europe** a de son côté souligné en 2015 la nécessité pour les États de fixer *« au niveau international la portée autorisée de la surveillance exercée par les services de renseignement, les conditions dans lesquelles elle s'exerce et les garanties, incluant un contrôle effectif et indépendant »* [82] [83]. Cet appel a débouché sur l'ouverture à la signature en 2018 de la *Convention 108+* sur la protection des données, qui vise à inclure des garde-fous contre la surveillance de masse dans un traité international contraignant [84] [85].

En **France**, comme mentionné, la première grande loi dédiée est celle de 2015. Celle-ci insère dans le Code de la sécurité intérieure un Livre VIII « Du renseignement » qui détaille : les finalités justifiant le recours aux techniques (par exemple prévention du terrorisme, des ingérences étrangères, de la criminalité organisée…), la liste des **techniques de renseignement autorisées** (interception de correspondances téléphoniques et hertziennes, accès administratifs aux données de connexion, surveillance audiovisuelle, keyloggers pour capturer les frappes au clavier, IMSI-catchers pour capter les téléphones dans une zone, etc.), la procédure d'autorisation (demande écrite du service, avis de la CNCTR, décision du Premier ministre) et la **durée de conservation des données** collectées [75] [77]. Elle prévoit également des régimes spécifiques pour des dispositifs nouveaux comme les *« boîtes noires »* algorithmiques insérées chez les fournisseurs d'accès Internet pour détecter des schémas de connexion terroristes – dispositif très controversé à l'époque, expérimenté puis pérennisé par une loi de 2021. Globalement, la loi de 2015 a *légalisé* ce qui se faisait auparavant de manière occulte, donnant aux agents une sécurité juridique dans leur action tout en créant la CNCTR pour éviter les abus. Elle a été en grande partie validée par le Conseil constitutionnel, hormis certains points (par exemple l'usage de techniques de surveillance internationale a dû être revu par une loi de 2017 pour mieux encadrer l'espionnage hors du territoire national après une censure partielle du Conseil d'État). Désormais, la France dispose d'un *« droit du renseignement »* complet, certes d'exception, mais qui *« offre une base légale claire et stable aux activités des services, répondant à la nécessité de sécuriser l'action des agents et aux attentes de transparence de la société »* [77].

Dans d'autres démocraties, on observe des évolutions similaires : l'Allemagne a réformé en 2016 la loi régissant le BND après que la Cour constitutionnelle de Karlsruhe a exigé plus de protections pour les étrangers surveillés depuis l'Allemagne (notamment pour les journalistes et avocats) ; le Canada a adopté en 2019 la Loi sur la sécurité nationale (NSICOPA) instaurant un comité parlementaire de surveillance et clarifiant les pouvoirs du SCRS (Service canadien de renseignement de sécurité) et du CST (Centre de la sécurité des télécommunications) ; l'Australie en 2018 a passé une loi obligant les entreprises technologiques à aider les agences à accéder aux communications chiffrées (loi très controversée concernant le chiffrement de bout en bout). En somme, le mouvement de fond est que les activités de renseignement, autrefois furtives et juridiquement floues, sont désormais **inscrites dans la loi** – du moins dans les États de droit – afin de concilier efficacité opérationnelle et respect des valeurs démocratiques.

Limites posées par les droits de l'homme et principes éthiques

Les **droits de l'homme** forment le socle des limites éthiques imposées aux services de renseignement dans les démocraties. Le droit à la **vie privée** (protection des données personnelles, secret des correspondances), la **liberté d'expression** et la **liberté d'association** sont autant de biens juridiques que les services peuvent affecter par leurs surveillances, et qu'il s'agit donc de préserver autant que possible. Les principes directeurs incluent la **nécessité** et la **proportionnalité** : une mesure de renseignement ne devrait être entreprise que si elle est nécessaire pour atteindre un but légitime (par ex. prévenir un danger grave) et doit être proportionnée, c'est-à-dire l'atteinte aux droits doit être minimisée et équilibrée par rapport au bénéfice attendu en termes de sécurité. Par exemple, placer sur écoute l'ensemble d'une population pour trouver quelques suspects serait disproportionné, là où cibler spécifiquement les communications d'un individu suspecté sur des indices sérieux peut être jugé acceptable. Ces critères de nécessité/proportionnalité sont inscrits dans la jurisprudence de la Cour européenne des droits de l'homme (arrêt *Klass c. Allemagne* dès 1978) et repris dans les législations nationales (en France, le Conseil constitutionnel y veille aussi).

Un autre principe clé est celui de la **finalité déterminée** : les services doivent opérer dans le cadre de missions définies par la loi (par exemple la défense de la sécurité nationale, la prévention du terrorisme, etc.) et ne pas détourner leurs moyens à d'autres fins. Si un service de renseignement interne se met à surveiller des adversaires politiques du gouvernement sans lien avec la sécurité nationale, il outrepasse sa mission légale et viole les droits civils (ce fut le cas dans le passé de certaines sections des RG en France, ou du FBI sous Hoover qui fichait des militants pour des motifs idéologiques). Les cadres légaux actuels s'efforcent de borner les finalités : la loi française liste limitativement les objectifs légitimes des techniques de renseignement [76], la loi britannique impose que les mandats de surveillance précisent le motif (sécurité nationale, prévention du crime grave, etc.).

Il existe en outre des **lignes rouges éthiques** que même les exigences de sécurité ne sauraient franchir dans un État de droit. Par exemple, la **torture** ou les traitements inhumains sont prohibés de manière absolue par les conventions internationales : un service de renseignement ne peut légitimement recourir à la torture pour faire parler un captif, quel que soit l'enjeu (après le 11-Septembre, la CIA a pratiqué des techniques assimilables à la torture – waterboarding, etc. – lors d'interrogatoires de terroristes, ce qui a été largement condamné et a conduit à l'interdiction de ces méthodes par le président Obama en 2009). De même, l'**assassinat politique** de ressortissants sur le territoire national serait illégal et anticonstitutionnel (en démocratie, seuls des cas de légitime défense immédiate pourraient justifier de tuer, par exemple un terroriste sur le point de commettre une tuerie, mais un assassinat planifié extra-judiciaire est proscrit). L'exemple extrême inverse est celui des régimes autoritaires où les services éliminent des opposants exilés à l'étranger (empoisonnements d'ex-espions russes au Royaume-Uni, etc.) : de tels actes violent clairement le droit international et les droits humains.

Une limite souvent soulignée est la **protection des sources journalistiques et du libre exercice du journalisme**. Les services de renseignement peuvent être tentés de surveiller des journalistes pour identifier leurs informateurs (notamment lorsqu'il y a des fuites d'informations classifiées). Toutefois, les tribunaux et instances comme la Cour européenne des droits de l'homme insistent sur le fait que la liberté de la presse est fondamentale et que les journalistes ne devraient pas faire l'objet de surveillance à moins d'être eux-mêmes impliqués dans une menace sérieuse. Des scandales récents – par exemple en 2021, la découverte que des journalistes français avaient été espionnés via le logiciel Pegasus par un service étranger, ou qu'aux États-Unis le département de la Justice avait saisi discrètement les relevés téléphoniques de journalistes pour trouver l'origine de fuites – ont ravivé l'attention sur ce point. En France, la loi *« Secret des affaires »* (2018) et la loi de 2015 sur le renseignement prévoient des

dispositions pour protéger, dans une certaine mesure, les communications des parlementaires, magistrats et journalistes (avec un régime d'autorisation renforcé s'ils devaient être surveillés).

Scandales et dérives ayant questionné l'éthique du renseignement

Comme évoqué, l'histoire du renseignement est jalonnée de **scandales** qui ont mis en cause l'équilibre entre sécurité et libertés. On a mentionné plus haut l'affaire Dreyfus (symbole de l'erreur judiciaire sur fond de renseignement faussé) et le Watergate (abus politique des services). D'autres affaires notables incluent : le **scandale des « fiches »** en France (1904) où il fut révélé que le ministère de la Guerre fichait les opinions politiques et religieuses des officiers – entraînant la démission du gouvernement de l'époque ; l'**Opération CHAOS** de la CIA (années 1960) qui espionnait illégalement des citoyens américains militants contre la guerre du Vietnam ; ou encore plus récemment le scandale dit **« NSO Pegasus »** (2021) révélant que le logiciel espion Pegasus, vendu à des gouvernements pour lutter contre le crime, avait servi à cibler des centaines de téléphones de journalistes, d'avocats ou d'opposants dans plusieurs pays. Ces dérives ont en commun de déclencher une **perte de légitimité** du renseignement aux yeux du public, du moins temporairement, et d'appeler une réaction institutionnelle : commissions d'enquête, nouvelles lois, sanctions de responsables. Par exemple, après Snowden, on a vu naître un **mouvement global pour la protection de la vie privée** : multiplication des applications chiffrées (Signal, etc.), renforcement des législations de data privacy (RGPD en Europe), et un débat de société sur le juste milieu entre surveillance et vie privée.

Un enjeu éthique actuel est aussi la question de la **surveillance de masse permise par l'IA** : la Chine, par exemple, déploie un système orwellien de crédit social en s'appuyant sur la reconnaissance faciale de masse et l'agrégation de données, ce qui heurte profondément les conceptions occidentales des libertés. Les démocraties devront se positionner clairement sur ce qu'elles s'autorisent ou non en la matière (ex : les villes américaines comme San Francisco ont banni la reconnaissance faciale policière pour éviter une dérive vers un État panoptique).

En synthèse, le cadre légal et éthique du renseignement dans les pays démocratiques cherche à **mettre des limites claires** : limites dans les finalités (pas d'espionnage pour des intérêts purement privés ou politiques), limites dans les moyens (pas de torture, pas de traitements inhumains, pas de surveillance sans autorisation ni contrôle), et limites dans la durée (les données collectées doivent être détruites passé un certain délai pour éviter la constitution de fichiers liberticides). Il s'agit de permettre au renseignement de remplir son rôle de *« bouclier invisible »* de la nation sans pour autant devenir une menace pour l'État de droit qu'il est censé défendre.

6. Technologies utilisées dans le renseignement moderne

Les services de renseignement modernes s'appuient sur un **arsenal technologique** de pointe pour mener à bien leurs missions. Parmi les technologies clés figurent la cybersurveillance, la cryptanalyse, les satellites espions, l'intelligence artificielle, le *big data* et l'interception des communications. Voici un tour d'horizon de ces outils et de leur emploi concret :

- **Cybersurveillance :** Ce terme recouvre l'ensemble des techniques permettant de surveiller l'activité sur les réseaux informatiques et Internet. Il s'agit aussi bien de la capacité à **collecter des données en ligne** (navigation Web, messageries, réseaux sociaux) qu'à **infiltrer des systèmes informatiques** cibles pour en extraire des informations ou y implanter des mouchards. Par exemple, les agences peuvent utiliser des logiciels espions (*spyware*) ultra-sophistiqués – tel **Pegasus** développé par la société NSO – pour pénétrer le smartphone d'une cible et accéder à ses messages, micro et caméra. D'autres outils consistent à analyser le trafic

Internet mondial : la NSA a ainsi conçu des programmes comme XKeyscore, qui permet de filtrer en temps quasi réel une part du trafic Internet international pour repérer des mots-clés ou des comportements suspects [43]. La cybersurveillance comprend également la veille sur le *Dark Web* où s'échangent des informations illicites (forums djihadistes, places de marché de la cybercriminalité). Face à la masse de données, les services développent des techniques d'analyse automatisée pour détecter, par exemple, une recrudescence soudaine de conversations violentes sur un forum – signe avant-coureur potentiel d'émeutes ou d'attentats [86] [87]. Ils exploitent aussi les fuites de données (par ex. bases de mots de passe piratées) pour leurs investigations. La cybersurveillance est devenue un pilier du renseignement intérieur et extérieur, car une énorme partie des activités humaines (y compris criminelles ou terroristes) laissent désormais des traces numériques.

- **Cryptanalyse :** C'est l'art de déchiffrer les communications codées de l'adversaire. Historiquement, la cryptanalyse a eu des succès éclatants (déchiffrement d'Enigma par les Alliés durant la 2GM, interception de codes diplomatiques). Aujourd'hui, face à des algorithmes de chiffrement modernes très robustes (AES, RSA…), la tâche est complexe. Cependant, les agences disposent de moyens considérables : des **supercalculateurs** capables de tester des milliards de combinaisons par seconde, des équipes de mathématiciens et informaticiens spécialistes de la théorie des nombres, et parfois l'accès à des faiblesses implantées dans les systèmes. Par exemple, la NSA a travaillé avec certains éditeurs pour implanter des **failles secrètes** (backdoors) dans des logiciels de chiffrement commerciaux, afin de s'en réserver l'accès. La cryptanalyse s'intéresse aussi aux méthodes de **cryptographie post-quantique**, anticipant l'arrivée dans peut-être une décennie d'ordinateurs quantiques capables de briser certaines protections actuelles. En attendant, une approche consiste à **contourner le chiffrement** plutôt que le casser : c'est l'objet de l'initiative dite *« lawful access »* où les gouvernements font pression sur les entreprises (Apple, WhatsApp…) pour obtenir des solutions d'accès aux contenus chiffrés en cas de besoin judiciaire ou de sécurité nationale. Cette demande se heurte aux résistances des défenseurs de la vie privée et des entreprises elles-mêmes, car affaiblir le chiffrement pour les uns revient à l'affaiblir pour tous (porte ouverte aux pirates). Malgré cela, les services comme la DGSE investissent massivement dans des centres de calcul capables d'absorber et de tester des clés de chiffrement sur d'énormes volumes, et dans la mise au point d'**algorithmes de cassage** améliorés. Durant la Seconde Guerre mondiale, les efforts conjugués de l'électromécanique et de l'intelligence humaine avaient permis de craquer l'Enigma pourtant dotée de 150 trillions de possibilités [25] ; l'espoir des cryptanalystes actuels est que de nouvelles percées mathématiques ou technologiques reproduisent de tels exploits face aux chiffrements modernes.

Exemple historique de cryptanalyse : une machine de chiffrement Enigma utilisée par l'Allemagne durant la Seconde Guerre mondiale. Les Alliés réussirent à casser son code malgré ~!150 quintillions de combinaisons possibles, grâce aux travaux de cryptanalystes comme Alan Turing et à l'emploi des premiers ordinateurs [25]. Ceci illustre l'importance du décryptage des communications ennemies dans le renseignement, hier comme aujourd'hui.

- **Satellites espions :** Les satellites d'observation et d'écoute sont des **pièces maîtresses du renseignement technique**. En orbite à quelques centaines de kilomètres d'altitude, les satellites d'imagerie (IMINT) peuvent fournir des photographies d'une précision étonnante (résolution de l'ordre de 30 cm voire mieux pour les plus récents), permettant de détecter par exemple le déploiement de missiles ou la construction de sites militaires clandestins. Il existe aussi des satellites radar pouvant *voir* de nuit et à travers la couverture nuageuse. Les États-Unis, la Russie, la Chine, la France, entre autres, exploitent des constellations de tels satellites. Un exemple célèbre est l'analyse par les Américains de photos satellites en 1962 qui révéla la présence de

missiles nucléaires soviétiques à Cuba, déclenchant la crise des missiles. Outre l'imagerie, les satellites de renseignement peuvent être dédiés à l'écoute électromagnétique (SIGINT) : ils captent depuis l'espace les émissions radio et micro-ondes (communications militaires, téléphones satellite, signaux radar) survolant des zones d'intérêt. Par exemple, le réseau **Orion** de la DGSE (ex- programme *CERES*) lancé en 2021 consiste en plusieurs satellites d'écoute capables d'intercepter depuis l'orbite des communications sur toute la planète. Ces outils offrent l'avantage d'accéder à des zones inaccessibles (pays fermés, océans) sans violer techniquement la frontière aérienne (les satellites évoluant dans l'espace extra-atmosphérique). Cependant, ils sont coûteux et ont leurs limites (passages intermittents, vulnérabilité à des mesures de camouflage ou à l'aveuglement laser). Avec la démocratisation de l'accès à l'espace, de plus en plus d'acteurs utilisent l'imagerie satellite y compris dans un but de renseignement ouvert : ainsi, lors de l'invasion de l'Ukraine en 2022, des images commerciales de sociétés privées ont permis de documenter les mouvements de troupes russes et d'en informer quasi en temps réel le grand public. Les services, eux, bénéficient de capacités bien supérieures en temps réel et résolution, gardant une avance significative.

- **Intelligence artificielle (IA) :** L'IA constitue pour le renseignement un outil à la fois prometteur et nécessaire étant donné l'**explosion des données** à traiter. Les algorithmes d'apprentissage automatique peuvent aider à détecter des **schémas cachés** dans des masses d'informations que l'analyste humain ne pourrait trier manuellement. Par exemple, des systèmes d'IA peuvent scruter les médias sociaux et détecter une soudaine montée de discours violents ou de fausses rumeurs ciblées sur une communauté [86] [87] – un signal d'alerte pour prévenir des troubles ou identifier une campagne de désinformation orchestrée par un acteur étatique. L'IA est aussi utilisée pour le **traitement automatisé d'images** : dans des flux vidéos de drones ou de caméras, un algorithme de vision peut identifier la présence d'un véhicule suspect ou reconnaître un visage particulier au milieu d'une foule, accélérant le travail de surveillance. De même, en cybersécurité, des outils IA apprennent à repérer des comportements anormaux sur un réseau qui pourraient révéler une intrusion. Les armées explorent l'IA pour le renseignement géospatial (par exemple, l'analyse en temps quasi réel des images de satellites pour détecter des changements sur le terrain). La **DGSE française** indique investir dans ces technologies, notamment via des supercalculateurs capables de traiter des flux massifs de données avec des algorithmes sophistiqués [66] [67]. Cependant, l'IA reste un *assistant* : les responsables du renseignement soulignent qu'elle ne remplacera pas le facteur humain, car l'analyse du contexte, la compréhension fine des intentions adverses, nécessitent du jugement et de l'expertise. L'IA peut fournir des *alertes* et dégrossir l'information, mais c'est à l'analyste qu'il incombe de valider et d'interpréter. Par ailleurs, l'usage de l'IA pose ses propres questions éthiques (biais algorithmiques pouvant mener à de fausses alertes sur certains groupes, risque d'une confiance excessive dans des décisions automatisées). Néanmoins, bien employée, l'IA est un **formidable multiplicateur d'efficacité** : par exemple, un tri intelligent des interceptions de la NSA via des algorithmes a été indispensable pour isoler quelques communications pertinentes au milieu de milliards interceptées. De même, l'IA est exploitée en traduction automatique, pour traiter des volumes de messages dans des langues rares et les rendre compréhensibles aux analystes humains.

- **Big Data et analyse de données massives :** Lié à l'IA, le *big data* désigne la capacité à stocker et exploiter d'immenses quantités de données hétérogènes. Le renseignement actuel collecte des **traces numériques** en quantités faramineuses : historiques téléphoniques, déplacements via GPS, transactions bancaires, enregistrements de caméras de surveillance, etc. Par exemple, pour suivre un réseau terroriste, il peut être utile d'analyser des millions de métadonnées télécom (qui a appelé qui, quand, où) afin de faire émerger un **graphe de connexions** révélant une cellule clandestine. C'est précisément ce qu'ont fait les agences américaines après le 11-Septembre avec

la collecte de métadonnées téléphoniques (programme *Stellarwind* de la NSA) – pratique controversée mais dont elles défendaient l'utilité pour *« reconstituer la toile »* entourant un suspect. Le *big data* appliqué au renseignement, c'est aussi par exemple de croiser des bases de données de voyageurs aériens, de passeports, de contrôles frontaliers, pour repérer qu'un individu a transité par tel pays à risque ou a des connexions indirectes avec d'autres personnes surveillées. Les services investissent dans des centres de données sécurisés et des capacités de calcul pour faire tourner ce genre de traitements lourds. Un document budgétaire indique qu'en 2025 la DGSE disposera de supercalculateurs dans les sous-sols de son siège pour analyser les flux massifs de données interceptées [67] . L'analyse big data est souvent couplée à des **outils de visualisation** afin de permettre aux analystes de comprendre les tendances (tableaux de bord, graphes dynamiques de réseaux, cartes interactives des incidents géolocalisés…). Par exemple, la surveillance des réseaux sociaux dans un pays instable pourrait donner lieu à une carte en temps réel des *hotspots* de tensions via l'agrégation de posts ou de tweets géolocalisés – utile pour anticiper des émeutes. Encore une fois, le défi du big data est de **filtrer l'utile de l'inutile** sans noyer le renseignement sous des faux positifs. Les techniques d'exploration de données (data mining) doivent être calibrées finement, et surtout le respect de la vie privée impose de ne pas tout conserver indéfiniment. La loi française impose d'ailleurs des durées maximales de conservation pour les données recueillies par les services (par exemple, les enregistrements d'écoutes doivent être détruits après x mois si non exploités).

Infrastructure de renseignement électromagnétique : photographie de radômes abritant des antennes d'écoute à la station de Menwith Hill (Royaume-Uni). Ce site exploité par les États-Unis est un nœud du réseau ECHELON, capable d'intercepter des communications satellites et micro-ondes à très longue distance [88] [89] . Les radômes protègent des paraboles qui "espionnent" le ciel en continu. Ce type d'installation illustre les moyens technologiques déployés pour l'interception planétaire des communications.

- **Interceptions des communications :** Il s'agit d'une des missions historiques des services de renseignement technique (SIGINT) : intercepter les **communications électroniques** (téléphoniques, radios, Internet) afin d'en extraire du renseignement. À l'ère analogique, cela signifiait placer des **écoutes téléphoniques** sur les lignes, capter des émissions radio chiffrées, etc. Aujourd'hui, l'écrasante majorité des communications empruntent des réseaux numériques (fibre optique, satellites, cellulaires). Les agences ont donc adapté leurs méthodes. Elles peuvent opérer des **points d'accès** chez les opérateurs télécom (par exemple la NSA avait des partenariats avec AT&T pour aspirer le trafic transitant par certaines dorsales Internet, nom de code **UPSTREAM**). Elles exploitent les stations terrestres écoutant les satellites de télécommunications (c'est le rôle de stations comme Menwith Hill, qui capte les liaisons satellite d'une bonne partie de l'hémisphère nord pour le compte des Five Eyes [88] [89]). Elles posent des **capteurs sous-marins** sur des câbles optiques (la capacité à se brancher sur des câbles sous-marins a été démontrée dès les années 1970 par l'US Navy dans l'opération Ivy Bells sous un câble soviétique en mer d'Okhotsk). Désormais, nombre de grandes stations d'écoutes comportent de vastes fermes de serveurs pour stocker temporairement et trier le flot intercepté. Les interceptions peuvent aussi cibler des communications chiffrées : les agences collectent des messages chiffrés qu'elles ne peuvent lire dans l'immédiat, mais qu'elles conservent dans l'éventualité de les déchiffrer plus tard (notamment si des avancées en cryptanalyse ou en informatique quantique surviennent).

L'**interception ciblée** reste tout aussi importante : cela inclut la pose de micros ou de *keyloggers* chez un individu (par ex. grâce à une perquisition clandestine autorisée par le politique), l'écoute d'une ligne téléphonique spécifique via une réquisition à l'opérateur, ou l'exploitation des ondes radio Wi-Fi émises par une cible. Par exemple, la **DGSI** a pu, dans certaines affaires terroristes, capter des discussions de

suspects en infiltrant leurs téléphones ou en utilisant des dispositifs discrets placés dans leurs domiciles, le tout sous contrôle du cadre légal.

Des programmes d'interception automatique comme **PRISM** (révélé par Snowden) ont permis à la NSA d'obtenir directement auprès des géants du Web le contenu de comptes de messagerie ou de cloud de cibles étrangères, via un cadre juridique secret (FISA 702) [90]. L'existence de PRISM a montré que même sans casser le chiffrement, les services pouvaient accéder aux données en s'insérant dans la chaîne (les données étant en clair sur les serveurs des entreprises). En réponse, plusieurs firmes ont renforcé le chiffrement de leurs services, rendant plus complexe l'accès direct. C'est un jeu du chat et de la souris entre les services cherchant des portes d'entrée et les technologies se blindant.

Enfin, les interceptions de communications englobent aussi la **surveillance des fréquences radio** non conventionnelles. Par exemple, en contre-espionnage, on traque les signaux d'émetteurs clandestins (les *transmissions clandestines* de satellites ou de postes radio utilisés par un espion). Dans le domaine militaire, on intercepte les communications des radars, des liaisons de données adverses, afin de connaître en temps réel leurs dispositifs (guerre électronique).

En résumé, les techniques d'interception actuelles sont omniprésentes, depuis le câble sous-marin jusqu'au smartphone local, et constituent une **source primordiale** de renseignement. Leur usage pose cependant des défis de **tri** (on collecte beaucoup plus qu'on ne peut analyser manuellement) et de **légalité** (trouver un équilibre entre surveillance et respect de la vie privée). Les États démocratiques, via leurs nouvelles lois, tentent d'encadrer cela en imposant par exemple que les interceptions en masse soient anonymisées et exploitées uniquement via des requêtes ciblées validées (c'est ce que prévoit la loi française de 2015 pour les données techniques de connexion, traitées d'abord de façon indifférenciée puis pouvant être examinées si un critère d'alerte se déclenche, avec autorisation). À l'international, des discussions ont lieu pour établir des normes communes de protection malgré la surveillance (par ex. la convention de protection des données du Conseil de l'Europe évoquée plus haut, Convention 108+).

Conclusion générale : Le renseignement, qu'il soit militaire ou civil, s'avère un **enjeu stratégique** majeur pour la sécurité des États et la conduite de leurs politiques. De l'Antiquité où Sun Tzu posait ses principes, jusqu'à l'ère du numérique et de l'intelligence artificielle, son rôle n'a cessé d'évoluer en s'adaptant aux menaces du moment – qu'il s'agisse d'armées ennemies, de terroristes cachés ou de cyberguerre silencieuse. Les services de renseignement actuels disposent d'**organisations complexes**, d'une **légitimité renforcée par la loi**, mais aussi de **responsabilités accrues** vis-à-vis de la démocratie. À l'aube de défis futurs (menaces hybrides mêlant propagande, sabotages cyber et interventions indirectes), le renseignement restera probablement la *« première ligne »* invisible qui permet aux États d'anticiper les crises et de protéger leurs citoyens. Il devra pour cela maintenir un difficile équilibre entre efficacité opérationnelle et respect des valeurs de l'État de droit – équilibre dont l'importance est soulignée par chaque controverse et chaque réforme. Le sujet du renseignement demeure ainsi, par essence, un domaine où se rencontrent l'ombre et la lumière, le secret nécessaire et la transparence exigée, au service de la sûreté commune.

Sources : Les informations de ce rapport s'appuient sur des publications spécialisées et officielles, notamment des documents du DCAF sur les services de renseignement [91] [5], des articles de l'encyclopédie Wikipédia pour les définitions et l'historique [3] [24], des analyses d'organismes comme l'OTAN [6] et le Conseil d'État français [54] [76], ainsi que sur des rapports journalistiques récents (budget de la DGSE en 2025) [58] et des travaux de recherche académiques (dossier *Cultures & Conflits* sur Snowden et la légitimation du renseignement) [44] [56]. Des exemples concrets et contemporains (guerre en Ukraine, affaires Snowden, Pegasus, etc.) ont été intégrés pour illustrer chaque point.

1 2 3 4 7 11 20 22 23 24 26 27 28 29 32 33 34 37 38 39 40 43 48 49 50 51 52 65 90 Renseignement — Wikipédia
https://fr.wikipedia.org/wiki/Renseignement

5 63 91 dcaf.ch
https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_12_Les%20services%20de%20renseignement.pdf

6 8 9 10 16 17 18 19 Renseignement, surveillance et reconnaissance interarmées (JISR) | OTAN Sujet
https://www.nato.int/fr/what-we-do/deterrence-and-defence/joint-intelligence-surveillance-and-reconnaissance

12 13 14 15 Calaméo - Esprit défense 17 - Au coeur du renseignement
https://www.calameo.com/books/007889324a240e667d492

21 53 54 60 64 74 75 76 77 78 79 80 81 Le renseignement et son contrôle - Conseil d'État
https://www.conseil-etat.fr/publications-colloques/discours-et-contributions/le-renseignement-et-son-controle

25 File:Enigma-Machine.jpg - Wikimedia Commons
https://commons.wikimedia.org/wiki/File:Enigma-Machine.jpg

30 31 Les mutations du renseignement militaire : dissiper le brouillard de la guerre ? | Ifri
http://www.ifri.org/fr/etudes/les-mutations-du-renseignement-militaire-dissiper-le-brouillard-de-la-guerre

35 36 47 61 62 Les services de renseignement | L'Académie du Renseignement
https://www.academie-renseignement.gouv.fr/services-renseignement

41 Enquêter sur le paysage de la surveillance numérique
https://gijn.org/fr/ressource/enqueter-menace-numerique-surveillance/

42 Surveillance numérique ciblée - Amnesty International France
https://www.amnesty.fr/militants-surveillance-numerique-ciblee

44 45 46 55 56 57 Contestations et (re)légitimations du renseignement en démocratie
https://journals.openedition.org/conflits/20889

58 59 66 67 68 69 70 71 72 La DGSE dépasse le milliard d’euros de budget en 2025, une hausse historique pour les espions français
https://www.challenges.fr/entreprise/defense/la-dgse-depasse-le-milliard-d-euros-de-budget-en-2025-une-hausse-historique-pour-les-espions-francais_908528

73 La délégation parlementaire au renseignement publie son rapport d ...
https://www.senat.fr/travaux-parlementaires/office-et-delegations/delegation-parlementaire-au-renseignement/actualite/la-delegation-parlementaire-au-renseignement-publie-son-rapport-dactivite-2023-2024-5051.html

82 83 84 85 La surveillance numérique par les services de renseignement : les États doivent prendre des mesures pour mieux protéger les individus - Portal
https://www.coe.int/fr/web/portal/-/digital-surveillance-by-intelligence-services-states-must-take-action-to-better-protect-individuals

86 L'utilisation de l'IA dans l'espionnage militaire : avantages et défis
https://cyberveille.ch/posts/2025-04-23-l-utilisation-de-l-ia-dans-l-espionnage-militaire-avantages-et-defis/

87 [PDF] Application de l'Intelligence Artificielle dans le Domaine Militaire
https://docs-library.unoda.org/General_Assembly_First_Committee_-Eightieth_session_(2025)/79-239-Morocco-FR.pdf

88 89 File:RAF Menwith Hill 2.jpg - Wikimedia Commons
https://commons.wikimedia.org/wiki/File:RAF_Menwith_Hill_2.jpg