ChatGPT

Le renseignement humain (HUMINT)

Introduction

Le **renseignement** désigne l'ensemble des informations jugées pertinentes pour éclairer la décision d'un État ou d'une organisation, ainsi que les activités de collecte et d'analyse de ces informations. Parmi les différentes disciplines du renseignement, le **renseignement d'origine humaine** – généralement appelé **HUMINT** (de l'anglais *Human Intelligence*) – se caractérise par le fait que la source de l'information est un individu [1]. En d'autres termes, il s'agit de recueillir des renseignements **par et auprès d'êtres humains**, par opposition aux sources techniques (écoutes électroniques, imagerie satellitaire, etc.) ou sources ouvertes (médias, Internet…). Par extension, l'HUMINT recouvre l'ensemble des activités de traitement de ces informations d'origine humaine : collecte, évaluation, analyse et diffusion [2].

Le HUMINT occupe historiquement une place centrale dans le renseignement. Même à l'ère numérique et des capteurs high-tech, il demeure un levier irremplaçable pour accéder à des données **inaccessibles par d'autres moyens**, notamment des informations **protégées ou classifiées** que les sources ouvertes ne fournissent pas [3]. Les interactions humaines permettent en outre de **contextualiser** et d'interpréter finement les données brutes collectées, en apportant des impressions, des rumeurs ou des éléments sur les **motivations profondes** des acteurs [4]. L'objectif ultime du renseignement humain est de fournir des **renseignements de haute qualité** aux décideurs (gouvernements, armées, agences), afin de prévenir les menaces, anticiper les crises et appuyer les actions diplomatiques, militaires ou de sécurité [5]. Après une définition des fondements de l'HUMINT, ce rapport passe en revue son évolution historique, ses méthodes, outils et acteurs, ainsi que les enjeux et perspectives liés à cette discipline du renseignement.

Fondements théoriques et concepts clés de l'HUMINT

L'HUMINT dans le cycle du renseignement : Comme toute discipline, le renseignement humain s'inscrit dans le **cycle du renseignement**, processus qui va de l'expression des besoins par l'autorité politique jusqu'à la diffusion du renseignement fini, en passant par la collecte et l'analyse. En pratique, l'HUMINT intervient surtout au stade de la **recherche et collecte** d'informations, mais aussi dans l'évaluation (retour sur la fiabilité des sources humaines). Sa **fiabilité** fait l'objet d'une cotation spécifique, afin de graduer la confiance dans la source et la crédibilité du renseignement obtenu [6].

Officiers traitants et agents : Le renseignement d'origine humaine implique généralement deux types d'acteurs. D'une part, les **officiers traitants** (ou officiers de renseignement opérationnels), qui sont les professionnels chargés de repérer, recruter, gérer et exploiter des sources humaines. D'autre part, les **agents** (parfois dits *sources* ou *informateurs*), c'est-à-dire les personnes extérieures au service qui fournissent les renseignements bruts [7]. Dans le jargon du renseignement français, on distingue traditionnellement les *honorables correspondants* – individus de bonne volonté collaborant **bénévolement** – des *agents* rémunérés d'une façon ou d'une autre [8]. Quel que soit leur statut, ces sources humaines sont encadrées par l'officier traitant qui les manipule et contrôle la validité de leurs informations. Notons que lorsqu'un officier de renseignement **trahit** son propre camp en livrant des informations à une puissance étrangère, il est lui-même considéré comme un **agent** du point de vue terminologique [9] (puisqu'il "fournit" du renseignement à l'ennemi).

Motivations et manipulation des sources : Convaincre un individu de livrer des informations sensibles implique de comprendre ses motivations et d'exercer sur lui certaines **pressions ou incitations** psychologiques. La théorie classique de l'HUMINT synthétise les principaux leviers de recrutement des agents par des acronymes mnémotechniques. Le plus connu est **MICE** (pour *Money, Ideology, Coercion, Ego*), traduit en français par **VICE** (Vénalité, Idéologie, Compromission/Coercition, Ego) [10] . Autrement dit, un individu peut être amené à espionner soit par appât du **gain financier**, soit par adhésion à une **cause idéologique** ou patriotique, soit par la **contrainte** (chantage, menaces…) ou l'exploitation d'une **faiblesse** (vanité, besoin de reconnaissance). D'autres acronymes existent – l'école française évoque SANSOUCIS (solitude, argent, nouveauté, sexe, orgueil, utilité, contrainte, idéologie, suffisance) – mais recouvrent des notions similaires. Le métier d'officier traitant consiste donc en partie à **identifier les motivations** d'une cible pour mieux l'amener à coopérer, ce qui requiert des compétences fines en psychologie sociale et en communication.

Clandestinité et couverture : Une grande partie des opérations HUMINT s'effectuent de manière **clandestine**, surtout lorsqu'il s'agit d'espionnage dans un pays étranger ou d'infiltration d'un groupe criminel. L'agent doit alors opérer sous **couverture**, c'est-à-dire dissimuler sa véritable identité et ses intentions derrière une fausse identité ou un statut officiel innocent (par exemple un diplomate, un homme d'affaires, un touriste…). L'élaboration d'une **légende** (biographie fictive cohérente), la fabrication de faux papiers, et le respect de règles de sécurité strictes (ne pas divulguer sa vraie fonction, changer régulièrement de pseudonyme, etc.) sont des notions clés pour protéger l'agent et son officier traitant. Par ailleurs, l'HUMINT intègre la notion d'**agent double** – individu qui joue un double jeu en fournissant des renseignements aux deux camps – et d'**agent d'influence** – source chargée non de collecter de l'information, mais d'orienter l'opinion ou les décisions au profit du service manipulateur. Autant de concepts qui montrent que le renseignement humain est un **jeu d'interactions sociales complexe**, fait de tromperies et de manipulations réciproques.

Histoire et évolution de l'HUMINT

Antiquité et Moyen Âge

L'espionnage est souvent qualifié de "deuxième plus vieux métier du monde". En effet, dès l'**Antiquité**, on trouve des traces de systèmes de renseignement organisés au sein des grandes civilisations. Les récits historiques et religieux abondent en exemples d'intrigues et d'espions : la **Bible** rapporte comment Moïse envoya des éclaireurs en terre de Canaan et comment Josué s'appuya sur Rahab à Jéricho ; l'historien grec **Hérodote** évoque des espions et messagers secrets ; l'**Arthashastra** du conseiller indien Kautilya (IVe siècle av. J.-C.) et **L'Art de la guerre** de Sun Tzu (Ve siècle av. J.-C.) consacrent des chapitres entiers aux méthodes pour recruter des agents et tromper l'ennemi. Toutes les **pratiques de l'espionnage moderne** existaient déjà dans l'Antiquité – contre-espionnage, messages chiffrés, interception de courriers, assassinats ciblés – comme en témoignent aussi bien la Bible, les inscriptions des temples égyptiens que les chroniques romaines [11] . Durant le Moyen Âge, ces activités perdurent et se structurent : royaumes et empires (de la Chine des Han aux califats musulmans, en passant par les royaumes francs) disposent d'émissaires secrets et d'informateurs. Les **réseaux d'espions** s'étoffent particulièrement dans les périodes troublées (ainsi la **Guerre de Cent Ans** entre la France et l'Angleterre voit chaque camp recourir à des agents infiltrés et messagers codés). On peut citer par exemple le **"Secret du Roi"** institué en France sous Louis XV au XVIIIe siècle, héritier des cabinets noirs de Richelieu, qui préfigure un véritable service secret royal chargé de missions clandestines parallèles à la diplomatie officielle [12] . De tout temps, la quête d'**information stratégique** – connaître les intentions et capacités de l'adversaire – a donc poussé les gouvernants à utiliser l'HUMINT, bien avant l'ère des capteurs techniques modernes.

Les guerres mondiales (XXe siècle)

L'entrée dans le XXe siècle et les **guerres mondiales** marquent un tournant dans l'organisation du renseignement. Avant 1914, peu de pays disposaient de services de renseignement structurés en temps de paix ; la Première Guerre mondiale va stimuler la création d'**agences professionnelles**. Le Royaume-Uni, par exemple, avait fondé en 1909 le Secret Service Bureau (ancêtre du MI5 et du MI6), et la guerre vit l'utilisation d'agents pour espionner l'ennemi, même si le renseignement technique (interception radio, décryptage) joua déjà un rôle crucial. La figure de **Mata Hari** illustre l'imaginaire de l'espionnage pendant la Grande Guerre : cette danseuse néerlandaise, accusée d'avoir espionné pour l'Allemagne, fut fusillée par la France en 1917, son affaire faisant grand bruit à l'époque [13]. Les historiens débattent encore de l'importance réelle de son espionnage, mais son destin symbolise l'aspect humain et trouble du renseignement en temps de guerre.

Lors de la **Seconde Guerre mondiale**, le renseignement humain prend une ampleur sans précédent, mobilisant **réseaux d'agents, résistants et services secrets militaires**. Chaque camp monta des opérations d'espionnage et de contre-espionnage sophistiquées. Du côté allié, le Royaume-Uni excella dans la guerre secrète : le Special Operations Executive (**SOE**) fut créé pour soutenir les résistances en Europe occupée et multiplia les missions d'infiltration et de sabotage [14]. Les Britanniques mirent en place le fameux système **Double Cross** qui retourna de nombreux agents allemands, transformant les espions ennemis en sources de désinformation pour le Reich. Dans le camp opposé, l'Abwehr allemande et les services japonais utilisèrent aussi des agents (mais avec moins de succès stratégique). Les Soviétiques, quant à eux, déployèrent de vastes réseaux d'espionnage : l'**Orchestre rouge** (Rote Kapelle) dirigé notamment par Léopold Trepper opéra au cœur de l'Europe occupée [15], tandis qu'à Tokyo l'officier **Richard Sorge** renseigna Moscou sur les plans germano-japonais avec une précision inouïe [16]. Sorge, espion soviétique d'origine allemande infiltré au Japon sous couverture de journaliste, fournit des renseignements de **première importance** sur l'intention d'Hitler d'attaquer l'URSS en 1941 et sur la décision du Japon de ne pas ouvrir de second front contre l'URSS – permettant à Staline de redéployer des troupes vers l'ouest [16]. Il fut démasqué et exécuté par les Japonais, entrant dans la légende du renseignement. Au sortir de la guerre, les grandes puissances disposaient ainsi de **services secrets structurés** (création en 1942 de l'OSS américain, futur CIA [17], renaissance du SDECE en France, etc.) et d'une riche expérience opérationnelle en HUMINT, ce qui allait préluder à l'intensification de la guerre de renseignement durant la période suivante.

La guerre froide

La **guerre froide** (env. 1947-1991) fut l'âge d'or de l'espionnage classique, opposant les blocs de l'Ouest (services américains et alliés) et de l'Est (services soviétiques et satellites) dans une lutte de l'ombre planétaire. Le renseignement humain y joua un rôle majeur, quoique concurrencé par les progrès du renseignement technique. Dans les premières années, la **fermeture quasi hermétique** du bloc soviétique rendait très difficile le recrutement d'agents sur place – la CIA et le MI6 subirent de lourds échecs pour infiltrer l'URSS. Cela poussa les Occidentaux à se tourner vers des moyens techniques innovants, tels que le renseignement électromagnétique (SIGINT) et l'imagerie aérienne puis satellitaire (IMINT) [18]. Le vol du Lockheed U-2 au-dessus de l'URSS à partir de 1956, puis les satellites espions, fournirent des informations cruciales sur les armements soviétiques [19]. Néanmoins, l'HUMINT ne disparut pas pour autant : il resta indispensable pour combler les **"zones d'ombre"** laissées par la technologie et surtout pour percer les **intentions** de l'adversaire, ce que les capteurs ne peuvent deviner [20]. D'éminents responsables occidentaux soulignèrent que l'espionnage humain devenait le complément nécessaire des systèmes techniques, allant chercher ce qu'ils ne pouvaient atteindre ou vérifiant leurs résultats [20].

Au fil de la guerre froide, chaque camp réussit des coups d'éclat en HUMINT, tout en subissant des revers retentissants. Côté soviétique, le **réseau "Cambridge Five"** infiltré au cœur du renseignement britannique (Kim Philby, Donald Maclean, Guy Burgess, Anthony Blunt, John Cairncross) transmit pendant des années des secrets de première importance à Moscou, jusqu'à son démantèlement progressif dans les années 1950-60. Côté occidental, le **colonel Oleg Penkovsky** du GRU soviétique renseigna la CIA et le MI6 au début des années 1960, livrant notamment des informations capitales sur les missiles nucléaires soviétiques (ce qui aida les États-Unis pendant la crise des missiles de Cuba en 1962) [21]. Penkovsky fut arrêté et exécuté en 1963 en URSS, mais il est souvent qualifié de "l'espion qui sauva le monde" pour son rôle dans l'évitement d'une guerre nucléaire.

Les services de contre-espionnage furent également très actifs durant cette période, la **chasse aux "taupes"** devenant une obsession. Aux États-Unis, James Angleton à la CIA mena une traque intense pour débusquer un agent double supposé, tandis qu'en réalité plusieurs **officiers américains trahissaient** au profit de Moscou (par exemple **Aldrich Ames** de la CIA et **Robert Hanssen** du FBI, qui livrèrent des listes entières d'agents occidentaux, causant l'exécution de nombreuses sources en URSS) [22] [23]. En Europe, un **agent Est-allemand**, **Günter Guillaume**, infiltré comme secrétaire auprès du chancelier ouest-allemand Willy Brandt, provoqua un scandale en 1974 qui conduisit à la démission du chancelier [24]. Cet épisode illustre le **risque politique** majeur lié à l'HUMINT : un simple individu infiltré au bon endroit peut ébranler un gouvernement. Vers la fin de la guerre froide, on assista à un retournement de tendance évoqué par l'ancien officier du KGB Oleg Kalouguine : les espions idéologiques pro-soviétiques à l'Ouest (comme Philby) se raréfiaient, tandis que les **défections** depuis l'Est se multipliaient à mesure que le système communiste perdait de son attrait [25]. L'année 1985 fut ainsi surnommée aux États-Unis "l'année de l'espion" en raison des nombreuses affaires révélées (John Walker, Jonathan Pollard, Larry Wu-Tai Chin, etc.) [26]. À l'aube des années 1990, la dissolution de l'URSS marqua la fin de cette confrontation bipolaire, mais certainement pas la fin de l'espionnage humain.

Période contemporaine (1990 – années 2020)

Après la guerre froide, le renseignement humain a dû s'adapter à un nouvel environnement stratégique. Les **années 1990** ont vu diminuer la menace d'un conflit mondial entre superpuissances, mais de nouvelles problématiques ont émergé : **prolifération d'armes, terrorisme international, conflits régionaux, criminalité organisée, espionnage économique**, etc. Dans ce contexte, certains ont pu croire à un recul de l'HUMINT face à l'essor des technologies numériques. En réalité, les événements phares du début du XXIe siècle ont souligné, au contraire, son **importance cruciale**. Les attentats du **11 septembre 2001** et la "guerre contre le terrorisme" qui a suivi ont mis en évidence les limites du tout-technologique : les services occidentaux ont été critiqués pour leurs **insuffisances en renseignement humain** concernant Al-Qaïda [27]. Des commissions parlementaires aux États-Unis ont pointé le manque d'informateurs infiltrés dans les organisations terroristes et le cloisonnement excessif entre agences, appelant à renforcer l'HUMINT et la **fusion des sources** de renseignement [27]. En réponse, la CIA et d'autres services ont lancé des programmes de recrutement accélérés d'agents parlant arabe, pachto, etc., et redéployé des officiers traitants sur le terrain en Afghanistan, en Irak et ailleurs.

Durant les conflits en Afghanistan (2001-2021) et en Irak (2003-2011), l'HUMINT a été un élément clé pour débusquer les cellules terroristes et les chefs insurgés – par le biais d'**informateurs locaux**, d'interrogatoires de prisonniers, d'opérations d'infiltration ou de "leurres" destinés à attirer les combattants hors de leur cachette. Par exemple, le renseignement américain a pu localiser Oussama ben Laden en 2011 grâce en partie à un **réseau d'indicateurs humains** et à des interrogatoires, combinés bien sûr avec des moyens techniques. En Europe, la menace terroriste a également poussé les services intérieurs (DGSI en France, MI5 au Royaume-Uni, etc.) à recruter massivement des sources dans les milieux radicalisés et à renforcer leurs **équipes d'agents infiltrés** dans les filières djihadistes.

Parallèlement, la **concurrence stratégique entre États** n'a pas disparu. La Russie, la Chine, mais aussi d'autres puissances, continuent de mener des opérations d'espionnage classique. On l'a vu avec l'affaire d'**ingérence russe** dans plusieurs élections occidentales, où au-delà de la cyberguerre, Moscou a actionné des réseaux d'agents d'influence. De même, la Chine est accusée de pratiquer un espionnage économique et politique agressif, en combinant piratage informatique et recrutement d'agents au sein d'entreprises ou d'administrations étrangères. Les affaires récentes d'**"illégaux" russes** (agents dormants vivant sous de fausses identités, démantelés aux États-Unis en 2010) ou d'arrestations d'espions en Europe (par exemple un officier français du renseignement arrêté en 2020 pour avoir transmis des informations à la Russie) montrent que l'HUMINT **classique reste d'actualité**. Simplement, elle évolue et s'hybride avec les nouvelles technologies, comme nous le verrons plus loin.

Les méthodes de collecte de l'HUMINT

Un marine américain interroge une civile irakienne lors d'une patrouille à Falloujah (Irak, 2006), illustrant l'importance du renseignement humain de terrain en opération contre-insurrectionnelle.

Plusieurs méthodes permettent de **collecter du renseignement humain**, chacune adaptée à des contextes et objectifs spécifiques. Les principales techniques incluent le **recrutement d'informateurs**, l'**interrogatoire** (ou debriefing), l'**observation directe** et l'**infiltration**, sans oublier quelques approches complémentaires. Ces méthodes peuvent être **ouvertes** (légales et affichées, par exemple l'interview de témoins) ou **clandestines** (espionnage pur). Elles reposent souvent sur la **relation de confiance** entre l'agent et l'officier traitant, et exigent un savoir-faire pointu.

- **Recrutement et gestion d'informateurs :** C'est le cœur de l'espionnage classique. Un officier traitant cherche à **identifier des personnes** ayant accès à l'information recherchée (militaires ennemis, employés d'une organisation cible, membres d'un groupe criminel, etc.), puis à les recruter comme **sources régulières**. Le recrutement peut être précédé d'une longue phase d'**approche et d'évaluation** ("casting" des cibles, tests de fiabilité). Si la cible accepte de coopérer (de gré ou de force, cf. motivations MICE évoquées plus haut), elle devient un **informateur** du service. L'officier traitant la **manipule par divers moyens** – incitations financières, idéologiques, promesse de protection, chantage éventuel – et obtient des renseignements de première main [28]. Chaque rencontre avec la source (rendez-vous discrets, communications codées) permet de recueillir des informations que l'officier traitant s'empresse

de vérifier et de transmettre à sa hiérarchie. La gestion d'informateurs requiert un strict **cloisonnement** (compartimentage) : l'identité de la source doit être protégée, et son activité reste secrète. Dans certains pays, notamment en France, le statut d'informateur a été encadré juridiquement (par ex. la loi du 9 mars 2004 dite loi Perben II) afin de permettre aux policiers et agents de traiter des **indicateurs rémunérés** en toute légalité [29].

- **Interrogatoire et débriefing :** Cette méthode consiste à **questionner directement** des personnes détenant des informations, qu'il s'agisse de prisonniers de guerre, de détenus terroristes, de transfuges, d'otages libérés ou même de simples voyageurs revenant d'une zone d'intérêt. L'**interrogatoire** stricto sensu désigne plutôt les interviews de personnes capturées ou réticentes, tandis que le **débriefing** s'applique aux personnes coopératives (par exemple un ingénieur d'une entreprise revenant d'un voyage dans un pays sensible, qu'on interroge sur ses observations). L'objectif est d'**extraire des renseignements bruts** de la personne interrogée, puis de les analyser. Dans le cas d'un débriefing d'otage ou de prisonnier libéré, on cherchera par exemple à cartographier un groupe terroriste, connaître ses modes opératoires, etc. [30]. La pratique professionnelle prévoit une phase initiale de collecte tous azimuts (laisser la personne parler librement pour ne pas brider l'information) suivie d'une phase d'**analyse et de recoupement** avec d'autres sources pour en vérifier la véracité [31]. L'art de l'interrogatoire est délicat : il faut obtenir le maximum d'informations sans recourir à la coercition illégale ni compromettre la fiabilité des déclarations. Les interrogateurs efficaces sont formés pour **gagner la confiance** de la personne, établir un rapport, jouer de finesse psychologique et, si nécessaire, exercer une **pression mentale contrôlée** (par exemple en exploitant l'épuisement ou l'ego de l'interlocuteur) [32] [33]. Toute forme de **torture physique ou d'humiliation morale** est proscrite par le droit international et considérée comme contre-productive par les professionnels : ainsi, le général français Bentégeat qualifia la torture d'"acte abominable et contre-productif" et rappela son interdiction absolue lors des interrogatoires [34]. Les dérapages (tels qu'à la prison d'Abou Ghraib en 2004) ont montré que de mauvaises pratiques d'interrogatoire causent plus de tort (discrédit, informations peu fiables) que de bénéfices [35] [36]. À l'inverse, un interrogatoire mené dans le respect de l'éthique peut s'avérer extrêmement fécond en renseignement exploitable.

- **Observation directe sur le terrain :** C'est la forme la plus **basique et immédiate** de renseignement humain : l'observation visuelle ou auditive par un **capteur humain** se trouvant physiquement sur le terrain, sans contact nécessaire avec la cible. Cela recouvre la **surveillance discrète** (filatures, planques) d'individus ou de sites, les missions de **reconnaissance** menées par des soldats ou agents en zone hostile, voire l'observation participante (l'agent se fond dans la foule pour noter l'ambiance, etc.). L'observation directe est un **outil précieux et incontournable** du renseignement humain : rien ne remplace le fait d'aller constater par soi-même la réalité du terrain [37]. En étant **présent physiquement**, l'observateur humain peut saisir une foule de détails contextuels et dynamiques (comportements, atmosphère, éléments non retransmis par les capteurs techniques) et en tirer des **données fiables et authentiques** [38]. Par exemple, une équipe de forces spéciales en reconnaissance pourra identifier la présence de combattants ennemis dans un village et évaluer leur attitude, là où un drone n'aurait vu que des silhouettes indistinctes. Ce type de collecte exige évidemment que l'observateur **s'expose** aux mêmes risques que sa cible (risques qui, nous le verrons, sont propres à l'HUMINT). La doctrine française distingue à ce titre le renseignement humain *conversationnel* (ROHUM-C, par interrogatoire) du renseignement humain de *reconnaissance* (ROHUM-R, par observation sans contact direct) [39].

- **Infiltration et espionnage clandestin :** Il s'agit là de la méthode la plus **emblématique** de l'HUMINT, souvent romancée dans les fictions – et pour cause, elle implique qu'un agent opère **sous couverture prolongée** au sein du camp adverse ou d'un milieu fermé afin d'y recueillir du renseignement de l'intérieur. L'**agent infiltré** peut agir seul ou être membre d'un réseau

clandestin. Le processus est long et difficile : il faut d'abord **introduire** l'agent dans l'environnement cible (par exemple en le faisant recruter dans l'organisme visé, ou en l'insérant comme « nouveau membre » d'un groupe terroriste), puis lui laisser le temps de **gagner la confiance** de ceux qui l'entourent, tout en **communiquant discrètement** ses informations à son service d'origine. Historiquement, l'infiltration a donné lieu à des exploits fameux (par ex. **Marthe Richard** infiltrant les milieux anarchistes au début du XXe siècle, **Eli Cohen** s'infiltrant dans les cercles du pouvoir syrien dans les années 1960, etc.). De nos jours, l'infiltration demeure une technique de pointe, utilisée notamment par les services de police contre le crime organisé ou le terrorisme (agents se faisant passer pour des trafiquants, des convertis radicalisés…). C'est une opération risquée – en cas de **démasquage**, l'agent infiltré peut payer de sa vie – et très coûteuse en ressources (construire une couverture robuste, prévoir des soutiens, etc.). Souvent, l'infiltration s'appuie sur une **légende** soignée (identité fictive), des moyens techniques (documents falsifiés, appareils de communication secrets) et une surveillance rapprochée pour protéger l'agent. Lorsqu'elle réussit, elle offre un **accès direct au cœur** du dispositif adverse, permettant de recueillir les renseignements les plus sensibles.

- **Autres méthodes complémentaires :** On peut mentionner également le renseignement obtenu par **liaison** avec des services partenaires (échange de renseignements entre alliés, ce qui peut inclure des informations HUMINT fournies par l'un à l'autre), ou encore la technique du **« fouille de documents sur humains »** (l'exploitation des documents capturés sur une personne : carnets, téléphones, ordinateurs – appelée parfois DOMEX, *Document and Media Exploitation*, bien que cela flirte avec le TECHINT). Par ailleurs, la **recherche de renseignement** via des interactions humaines peut inclure des actions non clandestines : par exemple, un attaché d'ambassade qui discute avec les élites locales collecte de l'information **ouvertement** (HUMINT *overt*), tout comme un officier de renseignement peut interviewer des réfugiés pour mieux connaître la situation d'un pays. Ces activités "grises" complètent les méthodes plus clandestines décrites ci-dessus. En somme, l'HUMINT offre un **arsenal varié de techniques**, allant du simple entretien au long effort d'infiltration, chacune mobilisant des compétences spécifiques mais poursuivant le même but : **obtenir de l'humain ce que l'on ne trouve pas ailleurs**.

Outils et techniques utilisés en HUMINT

La mise en œuvre des méthodes ci-dessus s'appuie sur un ensemble de **techniques opérationnelles**, souvent appelées en anglais *tradecraft*. Il s'agit de tout ce qui permet à l'agent humain de **communiquer, se cacher, transmettre ou extraire** l'information en sécurité. Ces outils et techniques ont évolué au fil du temps, mais certains principes restent constants.

- **Techniques de communication secrète :** Une fois qu'un agent a recueilli un renseignement, il doit pouvoir le transmettre à son service sans se faire détecter. Historiquement, cela passait par des **"boîtes aux lettres mortes"** (lieux de dépôt dissimulés où l'agent laisse un message que récupère plus tard son officier traitant), des **rendez-vous discrets** dans des endroits sûrs, ou l'utilisation de **codes** dans une correspondance apparemment anodine. Au XXe siècle, l'usage de la **radio chiffrée** a été courant : par ex. un espion émettait à heures fixes de brefs messages en morse vers une station distante (beaucoup d'agents soviétiques en Occident utilisaient des postes émetteurs-récepteurs miniatures). Pour la sécurité des transmissions, on recourait à des systèmes de **cryptographie** comme les *one-time pads* (carnets de codes à usage unique pratiquement incassables). De nos jours, les agents peuvent utiliser des moyens plus modernes : communications chiffrées via Internet (stéganographie dans des images, messageries sécurisées), téléphones jetables, etc. Néanmoins, la **discrétion** reste le maître-mot : un agent se trahira s'il communique trop ou de façon suspecte. C'est pourquoi les rencontres physiques dans

des **safe houses** (planques) ou les livraisons sur cachette restent des techniques robustes à l'ère numérique.

- **Couverture et surveillance anti-filature :** Un espion qui opère clandestinement en territoire hostile doit constamment protéger sa **légende** (fausse identité) et déjouer d'éventuelles surveillances ennemies. Les manuels de renseignement regorgent de techniques pour **passer inaperçu** : changer fréquemment de trajets et d'apparence, utiliser des "boîtes aux lettres" (adresses fictives) pour sa couverture, éviter les routines. Les fameuses *règles de Moscou* (ensemble de principes élaborés par les agents occidentaux en URSS) conseillaient par exemple de ne **jamais affirmer qu'on n'est pas surveillé** – c'est quand on se croit seul qu'on est vulnérable. Des accessoires spécialisés existent aussi : kits de **déguisement** (postiches, maquillage) fournis par des services comme la CIA, ou appareils pour vérifier si l'on est suivi (miroirs, etc.). L'agent doit également connaître les techniques de **filature** utilisées par la contre-intelligence adverse afin de les repérer et s'en affranchir (par des "gazouillis" – tests pour voir si quelqu'un le suit en voiture, etc.). La moindre erreur (par exemple rencontrer sa source sans s'assurer qu'on n'est pas filé) peut compromettre toute l'opération.

- **Techniques de recueil et de copie d'informations :** Souvent, un agent humain a pour mission d'**obtenir des documents** ou des preuves tangibles. Cela peut impliquer de **photographier** furtivement des plans, de copier des fichiers informatiques, de subtiliser du courrier, etc. Les services ont développé pour cela une panoplie de **gadgets** : micro-appareils photo (célèbre *Minox* utilisé pendant la guerre froide pour copier des documents), clés USB furtives, caméras dissimulées (dans un stylo, un bouton de veste…), micros discrets pour enregistrer des conversations, etc. Dès la Seconde Guerre mondiale, l'OSS distribuait à ses agents des kits contenant par exemple des **encres sympathiques** (pour écrire des messages invisibles), des limes pour s'évader, ou des faux paquets de cigarettes abritant des compartiments secrets. Aujourd'hui, la miniaturisation électronique permet à un agent de stocker des giga-octets de données sur une carte mémoire cachée dans une boutonnière. Mais quelle que soit la technologie, l'essentiel reste le **savoir-faire humain** pour s'en servir au bon moment sans éveiller les soupçons.

- **Manipulation et techniques d'influence :** Dans le cas du recrutement d'agents ou de l'interrogatoire, l'officier traitant utilise des techniques psychologiques pour **amener sa cible à coopérer**. Au-delà du choix des "leviers" de motivation (MICE/VICE), cela inclut l'établissement d'un **rapport de confiance** (par exemple jouer sur l'empathie, le patriotisme partagé, ou se poser en protecteur), l'**entretien dirigé** par questions ouvertes ou fermées selon l'effet recherché, l'utilisation du **mensonge** (feindre de connaître déjà certaines informations pour pousser la source à parler plus), ou encore le **good cop/bad cop** (alternance d'attitudes conciliantes et intimidantes). Des méthodes plus controversées existent, comme la création de **scénarios fictifs** (faire croire à la source que son camp l'a abandonnée, afin qu'elle change d'allégeance) ou l'exploitation de la **fatigue et du stress** (dits interrogatoires "musclés", sans aller jusqu'à la torture prohibée). Dans tous les cas, ces techniques demandent une formation approfondie en **communication et psychologie**. Un bon officier traitant sait "lire" le langage corporel, détecter un mensonge, calibrer son discours pour influencer sans braquer. Ces compétences *"soft"* sont de véritables **outils immatériels** de l'HUMINT, souvent décisifs dans l'obtention d'un renseignement humain de qualité [40] [41].

En synthèse, l'HUMINT mobilise un ensemble diversifié d'outils – à la fois **technologiques, logistiques et humains** – destinés à surmonter les obstacles inhérents au travail clandestin. Qu'il s'agisse de chiffrer une communication, de rencontrer une source en secret ou de convaincre un individu de livrer ses secrets, chaque geste est planifié avec minutie. Les progrès techniques offrent sans cesse de

nouveaux gadgets, mais l'essentiel de l'HUMINT demeure une affaire de **maîtrise technique ET de créativité** de la part des agents sur le terrain.

Enjeux éthiques, juridiques et politiques

Le recours au renseignement humain soulève d'importantes questions **éthiques, juridiques et politiques**, car il implique des actes souvent situés aux marges de la légalité et de la morale.

Enjeux juridiques et souveraineté : Sur le plan du **droit international**, l'espionnage bénéficie d'un statut pour le moins ambigu. En temps de **guerre**, le droit des conflits armés (Conventions de La Haye et de Genève) prévoit qu'un combattant capturé en espionnage (c'est-à-dire en civil derrière les lignes ennemies) **perd son statut de prisonnier de guerre** et peut être traité comme un criminel par l'ennemi. En revanche, en temps de **paix**, il n'existe pas de traité international régissant l'espionnage – c'est en général considéré comme un acte **contraire à la souveraineté** de l'État ciblé, mais toléré comme pratique universelle officieuse. En clair, chaque pays espionne, tout en protestant officiellement lorsqu'il est espionné. Les affaires d'espionnage peuvent cependant déclencher des **crises diplomatiques** retentissantes lorsque dévoilées. Par exemple, l'arrestation d'un espion américain à Moscou en 2000, l'incident de l'avion-espion américain contraint d'atterrir en Chine en 2001, ou les expulsions réciproques de diplomates russo-américains la même année, ont montré que l'espionnage touche directement à la **responsabilité des États et au droit diplomatique** [42] [43]. Souvent, la réaction classique consiste à expulser l'"espion-diplomate" (couvert par l'immunité) ou à engager des poursuites pour "espionnage" contre un agent sans couverture diplomatique. Sur le plan **national**, la plupart des pays criminalisent l'espionnage au profit d'une puissance étrangère (haute trahison) ainsi que certaines méthodes de renseignement (par ex. en France, la loi encadre strictement les interceptions de sécurité, les perquisitions clandestines, etc.). Mais symétriquement, ils dotent leurs propres services de renseignement de **pouvoirs spéciaux** les autorisant à déroger à la loi commune (intrusions, surveillances, etc.) sous contrôle de l'État [44] [45]. La difficulté est de concilier ces dérogations avec le respect de l'État de droit, d'où la mise en place d'organismes de contrôle (commissions parlementaires, autorités administratives comme la CNCTR en France) pour s'assurer que les services ne franchissent pas certaines lignes rouges, même au nom de la sécurité nationale [46] [47].

Enjeux éthiques : L'HUMINT confronte les services et les agents à des dilemmes moraux. **Mentir, manipuler, trahir** sont au cœur du métier d'espion – ce qui pose la question de la frontière entre moyen acceptable et moyen intolérable. Par exemple, est-il éthique de faire chanter quelqu'un (sur la base de sa vie privée, de fraudes commises, etc.) pour le contraindre à devenir agent ? De s'appuyer sur des individus moralement douteux (criminels, tortionnaires repentis) pour obtenir des infos ? Les services de renseignement élaborent des **codes de conduite** et des formations en éthique pour guider leurs agents, mais le terrain présente d'innombrables zones grises. L'un des débats les plus vifs concerne l'usage de la **torture** ou traitements cruels en interrogatoire. À la suite des attentats de 2001, certains ont défendu la notion de "torture justifiable" en cas de "bombe à retardement" (pour sauver des vies imminentes). Cependant, la grande majorité de la communauté internationale et des professionnels du renseignement rejette cette idée. Les **droits de l'homme** et le droit international interdisent formellement de tels actes (Convention de l'ONU contre la torture, CEDH, etc.), et l'expérience a montré qu'un interrogé torturé fournit souvent n'importe quelle information pour faire cesser la douleur – au risque de **fausses pistes**. L'affaire de la CIA et des prisons secrètes (programme de "renditions" et interrogatoires musclés de 2002-2006) a entaché gravement l'image des États-Unis sans apporter de résultats probants. À l'inverse, l'armée française, échaudée par les exactions de la guerre d'Algérie, a mis en place dans les années 2000 une unité spécialisée (le GRI) formée à des techniques d'interrogatoire **respectueuses de l'intégrité** des détenus, considérant que l'obtention de renseignement exploitable doit se faire **dans le respect de la loi** [48] [34]. Plus largement, l'éthique du renseignement questionne la **finalité** des opérations HUMINT : toutes les actions sont-elles permises

dès lors qu'elles servent l'"intérêt supérieur" ? Par exemple, fomenter un coup d'État en soutenant des agents locaux (ingérence politique), manipuler l'opinion publique d'un pays via des agents d'influence, est-ce légitime ou abusif ? La réponse dépend souvent du prisme national – ce qui est "défense de la liberté" pour les uns peut être "subversion" pour les autres. Les services doivent donc naviguer entre **efficacité et principes**.

Enjeux politiques et responsabilité : L'HUMINT, lorsqu'il est découvert, peut avoir des conséquences politiques sensibles. Une affaire d'espionnage révélée publiquement est toujours un **camouflet diplomatique**. L'État victime se doit de protester, l'État pris la main dans le sac peut nier ou sacrifier l'agent compromis. Par exemple, lorsque la France a découvert en 2014 qu'un de ses hauts responsables (Pierre-Martin Wiener) espionnait pour le compte de la DGSE – affaire rare d'espionnage interne –, cela a créé un malaise politique. De même, la révélation des écoutes de la NSA sur des alliés (comme le portable d'Angela Merkel) par les documents Snowden a provoqué des crises de confiance entre partenaires. Ces exemples montrent que même entre amis, "**on n'espionne pas les amis**" reste la règle… de façade seulement. Politiquement, les gouvernements doivent gérer le **scandale public** si des méthodes d'HUMINT illégales ou amorales sont dévoilées (d'où l'importance du secret et du **"plausible deniability"** – pouvoir nier officiellement toute implication). Enfin, sur le plan de la responsabilité démocratique, il est essentiel que les services de renseignement soient placés sous un **contrôle approprié** pour éviter les dérives. Les pays démocratiques instaurent un contrôle parlementaire ou exécutif sur les opérations sensibles, afin que l'HUMINT ne devienne pas un **"État dans l'État"** échappant aux lois. L'équilibre est délicat : trop brider les agents par des considérations éthiques ou légales strictes pourrait nuire à l'efficacité du renseignement – mais leur donner carte blanche risquerait d'éroder les valeurs mêmes qu'ils sont censés défendre. En définitive, l'HUMINT confronte à cette tension permanente entre **nécessité de la fin et moralité des moyens**, un sujet de réflexion constant dans la communauté du renseignement.

Principaux acteurs de l'HUMINT

Le renseignement humain est pratiqué par une multitude d'acteurs à travers le monde, qu'il s'agisse de services de renseignement **civils**, **militaires**, d'organismes de coopération internationale ou même de certains acteurs privés. Voici un panorama des principaux acteurs impliqués dans l'HUMINT :

- **Services de renseignement nationaux (civils)** : Chaque grande puissance dispose d'une ou plusieurs agences civiles spécialisées dans le renseignement, qui intègrent une composante HUMINT importante. Par exemple, aux **États-Unis**, la CIA (Central Intelligence Agency) est chargée du renseignement extérieur et mène des opérations HUMINT clandestines à travers le globe (recrutement de sources, missions d'espionnage, etc.). En **Russie**, le SVR (Service des renseignements extérieurs, héritier de la Première Direction générale du KGB) joue un rôle comparable, tout comme le faisait le KGB à l'époque soviétique. En **Chine**, c'est le MSS (Ministry of State Security) qui pilote l'espionnage humain à l'étranger. En **Royaume-Uni**, le MI6 (Secret Intelligence Service) est l'agence extérieure, rendue célèbre par la figure de James Bond – bien que la réalité de ses opérations soit autrement plus discrète. La **France** dispose de la DGSE (Direction Générale de la Sécurité Extérieure) pour l'espionnage à l'étranger, laquelle est explicitement chargée du renseignement **humain** et technique hors des frontières [49] . Nombre d'autres pays ont leurs homologues (BND allemand, Mossad israélien, ASIS australien, etc.). Ces services civils opèrent souvent sous la couverture de leurs ambassades (officiers traitants se faisant passer pour diplomates) ou via des réseaux clandestins, et travaillent en temps de paix comme en temps de guerre.

- **Services de renseignement militaires** : En parallèle des structures civiles, les armées possèdent leurs propres unités de renseignement, focalisées sur le soutien aux opérations militaires. L'HUMINT militaire consiste en la collecte de renseignements tactiques sur le terrain et stratégiques en zone de conflit. Par exemple, aux États-Unis, la **DIA** (Defense Intelligence Agency) coordonne l'HUMINT pour le Département de la Défense, avec des officiers déployés dans les zones d'intérêt [50]. En **Russie**, le GRU (Direction du renseignement de l'état-major) a longtemps eu un vaste réseau d'espions militaires à travers le monde (incluant les fameux "illégaux"). La **France** a la DRM (Direction du Renseignement Militaire) et des unités dédiées dans l'armée de Terre (par exemple le 13e RDP pour les reconnaissances spéciales ou le 2e RH) qui déploient des équipes de recherche humaines. En milieu militaire, l'HUMINT prend la forme d'interrogatoires de prisonniers de guerre, de patrouilles de renseignement, d'agents de terrain insérés derrière les lignes ennemies, etc. Ces acteurs opèrent surtout en temps de guerre ou de crises extérieures, et collaborent souvent avec les services civils lorsque les missions se chevauchent.

- **Services de sécurité intérieure et contre-espionnage** : La dimension HUMINT est tout aussi présente dans le renseignement **intérieur**, c'est-à-dire la surveillance du territoire national pour prévenir espionnage et menaces internes. Ici, on parle plutôt d'agents infiltrés dans des groupes terroristes ou criminels, de réseaux d'indicateurs dans les milieux à risque, etc. Des agences comme le **FBI** (États-Unis) ou le **MI5** (Royaume-Uni) ont longtemps géré un important maillage d'informateurs pour traquer espions étrangers et extrémistes. En **France**, la DGSI (Direction Générale de la Sécurité Intérieure) recrute et rémunère des informateurs dans divers secteurs (communautés sensibles, mouvances radicales, crime organisé) via le **SCRT** (Service central du renseignement territorial, héritier des Renseignements Généraux) [51]. Ces structures conjuguent souvent des techniques de police classique et de renseignement clandestin. Leur rôle HUMINT est crucial par exemple pour **déjouer des attentats** grâce aux indications fournies par une source infiltrée, ou pour **identifier des espions étrangers** opérant sur le sol national.

- **Coopération et agences internationales :** Si chaque nation a ses services, l'HUMINT est aussi au cœur de la **coopération internationale** en matière de renseignement. Dans les alliances militaires (OTAN) ou les partenariats stratégiques (ex : le réseau **Five Eyes** anglo-saxon), les pays échangent des informations y compris issues de sources humaines. Par exemple, un agent recruté par le MI6 au Moyen-Orient pourra fournir des renseignements qui seront partagés avec la CIA et vice-versa. Il existe également des **cellules de renseignement internationales** dans certaines opérations de maintien de la paix, où des officiers de différents pays mettent en commun leurs informations (dans le cadre d'opérations de l'ONU ou de l'UE par exemple). Toutefois, la dimension humaine du renseignement, très liée à la **confiance** entre l'agent et son officier traitant, rend les échanges parfois délicats – les services ne révèlent pas aisément l'identité de leurs sources à des tiers. Notons qu'en **temps de guerre**, des structures unifiées peuvent émerger : durant la guerre froide, le Pacte de Varsovie coordonnait partiellement les activités de ses services (via le KGB), et de nos jours, la lutte antiterroriste mondiale a vu l'émergence de **task-forces** transnationales où l'HUMINT joue un rôle (agents de plusieurs pays collaborant pour infiltrer une même nébuleuse terroriste).

- **Acteurs privés et milieu industriel :** Enfin, bien que l'espionnage soit historiquement affaire d'États, on assiste à l'implication croissante d'**acteurs privés**. D'une part, des **sociétés militaires privées** ou sociétés de sécurité proposent aux États des prestations de renseignement (certaines embauchent d'anciens espions pour mener des enquêtes dans des zones risquées, par exemple). D'autre part, dans le domaine de l'**intelligence économique**, de grandes entreprises n'hésitent pas à recourir à l'HUMINT pour collecter des informations sur leurs concurrents ou sur les marchés (ce qui flirte parfois avec l'illégalité si on parle d'espionnage industriel). On voit émerger

des cabinets d'intelligence économique qui recrutent des informateurs dans des entreprises cibles, ou encore des **opérations d'infiltration industrielle** – par exemple, un ingénieur envoyé "en mission" dans une société rivale pour en soutirer des secrets. Ces pratiques soulèvent des enjeux juridiques sérieux (violation de secrets d'affaires) et sont généralement condamnées si découvertes. Néanmoins, les **États eux-mêmes pratiquent l'espionnage économique** via leurs services officiels, justifiant cela par la protection des intérêts nationaux (la DGSE française, par exemple, a été accusée dans les années 1990 d'espionner des entreprises américaines pour aider l'économie française, ce qui provoqua des critiques [52]). Ainsi, l'HUMINT dépasse le cadre purement étatique et s'étend à quiconque a besoin d'informations exclusives – mais les agences étatiques restent de loin les principaux employeurs de cette "main d'œuvre" spéciale que sont les espions et leurs agents.

Études de cas et exemples historiques célèbres

Pour illustrer concrètement le rôle du renseignement humain, voici quelques **cas marquants** d'opérations ou d'agents ayant marqué l'histoire de l'espionnage :

- **Mata Hari (1876-1917)** : Danseuse néerlandaise devenue **agent double** pendant la Première Guerre mondiale. Recrutée par les services allemands, elle fournit aussi des informations aux Français, mais ces derniers l'accusent d'avoir causé la mort de milliers de soldats par ses révélations à l'ennemi. Son **procès retentissant** se solde par son exécution en octobre 1917. Symbole de l'espionne vénéneuse, Mata Hari reste une figure controversée : on pense aujourd'hui qu'elle n'avait en réalité transmis que peu de renseignements décisifs, mais son histoire demeure emblématique de la suspicion extrême en temps de guerre [13].

- **L'"Orchestre Rouge" (1940-1944)** : Nom de code donné par la Gestapo à un réseau de renseignement soviétique actif en Europe occupée durant la Seconde Guerre mondiale. Dirigé notamment par **Leopold Trepper**, ce réseau parvient à infiltrer l'administration nazie en France, en Belgique et même en Allemagne. Il transmet à Moscou des informations cruciales sur les plans militaires allemands. Le réseau sera progressivement démantelé par les nazis, mais son existence a démontré la capacité des Soviétiques à mener une **guerre secrète** efficace au cœur du dispositif ennemi [15].

- **Kim Philby (1912-1988)** et le **Groupe de Cambridge** : Philby fut un officier supérieur du MI6 britannique, tout en étant un **agent du KGB** depuis ses années universitaires à Cambridge. Avec quatre complices également issus de Cambridge (Maclean, Burgess, Blunt, Cairncross), ils forment un redoutable **réseau d'agents doubles** qui, des années 1930 aux années 1950, livrent à l'Union soviétique d'innombrables secrets (plans alliés, identité d'agents occidentaux infiltrés à l'Est, etc.). Philby, devenu chef de la section anti-soviétique du MI6, a ainsi pu saboter de l'intérieur de nombreuses opérations britanniques. Il fera défection à Moscou en 1963 pour échapper à l'arrestation. L'affaire Cambridge Five a constitué l'un des plus grands **couacs du contre-espionnage** occidental, révélant l'ampleur des infiltrations soviétiques au cœur même des élites de renseignement alliées.

- **Richard Sorge (1895-1944)** : Espion soviétique opérant au Japon pendant la Seconde Guerre mondiale. D'origine allemande, journaliste de profession, Sorge parvient à gagner la confiance des milieux diplomatiques et militaires allemands à Tokyo tout en dirigeant un réseau clandestin pour l'URSS. Il transmet en 1941 deux informations capitales : la date exacte de l'attaque allemande contre l'URSS (22 juin 1941) et le fait que le Japon ne déclarera pas la guerre à l'URSS tant que la guerre contre les États-Unis n'est pas décidée. Ces renseignements permettent à

Staline de redéployer des troupes sibériennes vers Moscou à l'automne 1941, contribuant à stopper l'avance nazie. **Arrêté par les Japonais**, Sorge est exécuté en 1944, et n'a été officiellement reconnu Héros de l'Union soviétique qu'en 1964. Il reste l'un des espions les plus célébrés pour la **qualité inestimable de son renseignement** obtenu à très haut risque [16].

- **Günter Guillaume (1927-1995)** : Agent de la Stasi est-allemande, infiltré en RFA auprès du chancelier Willy Brandt. Immigré en Allemagne de l'Ouest dans les années 1950 sur instruction de la Stasi, Guillaume gravit les échelons au sein du parti social-démocrate jusqu'à devenir un collaborateur très proche du chancelier fédéral Brandt au début des années 1970. Son **exfiltration en 1974** provoque un choc : Brandt démissionne, assumant la responsabilité politique de s'être laissé infiltrer. L'affaire Guillaume a été un coup de maître du renseignement est-allemand (HVA dirigé par Markus Wolf), illustrant comment un seul agent bien placé peut avoir un **impact politique majeur** [24].

- **Oleg Penkovsky (1919-1963)** : Colonel du renseignement militaire soviétique (GRU) qui contacta l'Ouest en 1960 et devint une **source clé** pour la CIA et le MI6. Durant deux ans, il fournit des renseignements très détaillés sur les missiles nucléaires soviétiques, les plans militaires de l'URSS et l'organisation du GRU [21]. Ses informations ont joué un rôle crucial pendant la **crise des missiles de Cuba** (1962) en confirmant l'état de faiblesse relative de l'arsenal soviétique, ce qui a aidé les Américains à négocier avec fermeté. Démasqué en 1963, Penkovsky est arrêté et exécuté en URSS après un procès à huis clos. En Occident, il fut surnommé *"l'espion qui sauva le monde"* pour avoir potentiellement évité une guerre nucléaire. Son cas est emblématique du **transfuge idéaliste** (Penkovsky était déçu du régime soviétique et a choisi de le trahir) qui offre à l'ennemi un trésor de renseignements.

- **Aldrich Ames (né en 1941)** et **Robert Hanssen (1944-2021)** : Deux des plus célèbres **"taupes"** ayant sévi au cœur du renseignement américain pendant la guerre froide tardive. Aldrich Ames, cadre de la CIA endetté, commence en 1985 à vendre des informations au KGB contre de l'argent. En près de 9 ans, il livre l'identité de **dizaines de sources** américaines en URSS, entraînant l'arrestation et l'exécution de nombre d'entre elles [22]. Arrêté en 1994, il purge une peine de prison à vie. Robert Hanssen, quant à lui, était agent du FBI chargé du contre-espionnage : de 1979 à 2001, motivé lui aussi par l'argent (et un sentiment de supériorité intellectuelle), il renseigne d'abord le renseignement soviétique puis russe sur les opérations américaines, compromettant là encore des opérations sensibles et des informateurs clés [23]. Son arrestation en 2001 a mis fin à l'une des plus longues trahisons de l'histoire du FBI. Ces deux affaires ont eu un retentissement énorme aux États-Unis, et ont conduit à un renforcement drastique des procédures de **sécurité interne** dans les agences (surveillance financière des employés, détection des comportements à risque, etc.). Elles illustrent les **dangers de la contre-ingérence** : la réussite d'un service de renseignement peut être sapée de l'intérieur par l'infidélité de ses propres officiers.

(D'autres cas célèbres pourraient être cités, comme l'affaire Jonathan Pollard – analyste US ayant espionné pour Israël, Eli Cohen – infiltré israélien en Syrie dans les années 60, Claus Fuchs – physicien ayant transmis à l'URSS les secrets de la bombe atomique américaine [53], etc. Chacun éclaire un aspect particulier de l'HUMINT, qu'il s'agisse de son efficacité, de ses risques ou de ses enjeux moraux.)

Comparaison avec les autres formes de renseignement (SIGINT, OSINT, IMINT, etc.)

Le renseignement humain (HUMINT) s'inscrit dans un écosystème plus large de **disciplines du renseignement**, souvent désignées par des sigles en -INT. Les principales sont :

- **SIGINT** (*Signals Intelligence*) : renseignement d'origine électromagnétique, c'est-à-dire l'interception de communications (téléphonie, radio, internet) et d'émissions radar ou autres. Par exemple, les écoutes téléphoniques, le déchiffrement de messages radio, l'espionnage des communications par satellite font partie du SIGINT. C'est le domaine d'agences comme la NSA américaine ou le GCHQ britannique.

- **IMINT** (*Imagery Intelligence*) : renseignement d'origine image, obtenu par des capteurs optiques, infra-rouges ou radar, embarqués sur des avions, drones ou satellites. Il fournit des **photographies aériennes ou satellites** permettant d'observer des sites militaires, des mouvements de troupe, etc. L'IMINT s'est développé à fond pendant la guerre froide (avions U-2, satellites espions…).

- **OSINT** (*Open Source Intelligence*) : renseignement obtenu à partir de **sources ouvertes**, c'est-à-dire publiques et accessibles librement (médias, publications, réseaux sociaux, bases de données ouvertes). C'est un domaine en plein essor à l'ère d'Internet, où une masse énorme d'informations est disponible publiquement pour qui sait la trier.

- **MASINT** (*Measurement and Signature Intelligence*) : renseignement de mesures et signatures, englobant la collecte de données techniques (nucléaires, acoustiques, chimiques, etc.) pour détecter des phénomènes d'intérêt (par ex. détection d'un essai nucléaire par des capteurs sismiques). C'est plus confidentiel et lié aux capteurs scientifiques.

Le **renseignement humain se distingue de ces formes techniques et ouvertes** par le fait qu'il implique une **interaction avec un être humain** [6]. Là où un satellite IMINT prendra automatiquement des clichés et où un système SIGINT enregistrera des ondes, l'HUMINT nécessite de **gagner la confiance** d'une source, ou d'analyser le comportement d'un interlocuteur, etc. Cette singularité fait sa **force** et sa **faiblesse**.

Forces complémentaires : L'HUMINT peut accéder à des informations que ni les capteurs techniques ni les sources ouvertes ne peuvent fournir. Par exemple, les **intentions stratégiques** d'un dirigeant ennemi (ses plans secrets, sa volonté réelle de paix ou de guerre) ne transparaissent pas forcément dans les communications interceptées ou les images satellites, mais un **agent humain** bien introduit peut les apprendre de première main [20]. De même, un capteur technique peut rater une information parce qu'elle n'est pas émise (un document sur papier non numérisé, une réunion à huis clos non sonorisée), alors qu'une source humaine présente dans la pièce pourra la rapporter. L'HUMINT apporte aussi du **contexte et de l'interprétation** : une image ou un signal brut nécessite une analyse pour lui donner du sens, alors qu'un informateur peut fournir directement une analyse en même temps que l'information ("Untel prépare un coup d'État, je le sais car j'ai senti telle dynamique au sein du groupe dirigeant"). Enfin, le coût financier de l'HUMINT est souvent bien moindre que celui des grands systèmes techniques : recruter quelques informateurs coûte moins cher que lancer un satellite ou déployer un avion-espion [54]. À l'heure où les budgets de renseignement explosent pour la technologie, l'HUMINT reste un **investissement modéré** qui peut rapporter gros.

Faiblesses et limites : En contrepartie, l'HUMINT souffre d'inconvénients spécifiques par rapport aux autres disciplines. D'abord une **lenteur et une inertie** : développer une source humaine fiable prend du temps (des mois, parfois des années), et un agent infiltré ne peut pas changer de cible rapidement comme un satellite qui redirige son capteur [55]. C'est donc un capteur moins flexible, moins "pilotable à loisir". Ensuite, l'HUMINT est vulnérable car **humainement exposé** : un espion peut être arrêté, retourné, tué, ce qui représente un risque politique énorme en cas d'incident [56]. Un satellite abattu ou un câble sous-marin coupé, c'est un incident technique ; un espion arrêté, c'est un **casus belli diplomatique** presque à coup sûr. L'HUMINT est aussi sujette aux **tromperies** : une source humaine peut mentir, exagérer, être manipulée par l'adversaire (cas d'un agent double ou d'un "**fabricant**" qui fournit de faux renseignements pour de l'argent) [57]. L'exemple tristement célèbre est celui de la source code-nommée *Curveball* qui, au début des années 2000, a fourni de fausses informations sur les armes de destruction massive irakiennes conduisant les Occidentaux à se fourvoyer [58]. Ce **risque de contamination** du renseignement par de fausses informations est un talon d'Achille de l'HUMINT – on doit toujours recouper avec d'autres sources. Par ailleurs, la **couverture géographique** de l'HUMINT est limitée : on ne peut pas avoir des espions partout, alors qu'un satellite peut survoler n'importe quel point du globe. Le renseignement technique offre souvent une **vue d'ensemble** (par ex. imagerie d'une zone entière) là où l'HUMINT donne une **vue de l'intérieur** très pointue mais étroite.

Nécessaire complémentarité : En réalité, les différentes disciplines de renseignement sont mieux vues comme **complémentaires** que rivales. Chaque type comble les lacunes de l'autre. Stansfield Turner, directeur de la CIA à la fin des années 1970, écrivait que l'espionnage humain était devenu un **complément** des systèmes techniques : il "va chercher dans les trous que la technique ne peut sonder, ou revérifie les résultats de la collecte technique" [20]. De l'autre côté, beaucoup soulignent que **seules les sources humaines** peuvent éclairer les intentions ou les pensées d'une cible, ce qu'aucun capteur ne détectera [20]. Les retours d'expérience, notamment après le 11 septembre 2001, ont mis en lumière la nécessité de **croiser les sources** (*"all-source intelligence"*) pour obtenir le tableau le plus fiable : par exemple, un rapport parlementaire américain a critiqué la CIA pour ses insuffisances en HUMINT sur le terrorisme, tout en soulignant le besoin d'**intégration** du renseignement humain, technique, image, etc., afin que chaque pièce du puzzle soit analysée en conjonction des autres [27]. Aujourd'hui, la plupart des centres de fusion du renseignement (dans les grandes agences ou au niveau interarmées) travaillent à partir de **produits mixtes**, par exemple : l'analyse d'un site suspect combinera les images satellites (IMINT) pour le repérage des bâtiments, les interceptions (SIGINT) pour connaître les communications, et les informations d'un informateur local (HUMINT) décrivant ce qui se trame à l'intérieur. Aucun **"INT"** pris isolément n'est parfait, mais leur combinaison augmente considérablement la fiabilité du renseignement final. Ainsi, l'HUMINT n'est ni dépassé ni infaillible : il est l'un des piliers, avec ses atouts uniques et ses défauts, d'une **communauté du renseignement interconnectée** où chaque source enrichit les autres [59].

Limites et risques de l'HUMINT

Comme évoqué plus haut, le renseignement humain présente des **limites structurelles** et expose à des **risques** particuliers. Les principaux inconvénients identifiés par les spécialistes (par exemple l'ambassadeur Jean-Claude Cousseran et le chercheur Philippe Hayez en France) sont au nombre de quatre [60] :

- **Lenteur et réactivité limitée :** Contrairement aux capteurs techniques instantanés, une **source humaine** ne se crée pas en un jour. Il faut du temps pour infiltrer un milieu ou recruter un agent, et l'en extraire en sécurité. L'HUMINT est donc peu adapté aux informations urgentes ou aux changements rapides. Par exemple, infiltrer un groupe terroriste peut prendre des mois, alors que la menace peut évoluer en semaines. De plus, un agent sur le terrain ne peut pas être

redéployé facilement d'une cible à une autre : il est "inertiel". Cette **manque de flexibilité** fait que l'HUMINT répond parfois moins bien aux besoins immédiats du décideur [55].

- **Risques physiques pour les personnels :** C'est sans doute le point le plus évident : **espionner est dangereux**. Un espion pris en flagrant délit dans un pays étranger hostile encourt l'arrestation, la prison, voire la torture ou la peine de mort. Même un informateur local court de grands risques s'il est découvert par son camp (lynchage par un groupe terroriste, exécution pour trahison…). Quant aux officiers traitants opérant clandestinement, ils ne sont pas à l'abri d'un coup de filet policier. De nombreux épisodes l'ont montré, depuis les **exécutions d'agents doubles** pendant les guerres jusqu'aux empoisonnements d'anciens espions (par ex. le cas de Sergueï Skripal empoisonné en 2018 au Royaume-Uni). À l'échelle politique, la perte d'un agent expose aussi le commanditaire à un scandale. En somme, l'HUMINT implique de **mettre des vies en jeu**, ce qui le distingue là encore des moyens techniques sans âme [56].

- **Risques diplomatiques et politiques :** Quand une affaire d'espionnage éclate, les conséquences peuvent aller d'un simple **recadrage diplomatique** (expulsion de quelques diplomates) à une crise majeure. Par exemple, la révélation d'espionnage entre pays alliés peut gravement détériorer la confiance politique (cf. l'affaire des écoutes de la NSA sur ses alliés). Dans des contextes plus tendus, la capture d'un espion peut servir de **monnaie d'échange** ou d'outil de propagande. Sur le plan intérieur, l'utilisation de méthodes contraires aux valeurs proclamées (torture, manipulation d'opinion) peut provoquer des polémiques publiques et affaiblir la légitimité du gouvernement. Les dirigeants doivent donc peser le **coût politique** potentiel de chaque opération HUMINT clandestine. Ainsi, toute entreprise d'espionnage comporte une part de **risque diplomatique** que les décideurs doivent accepter en connaissance de cause [61].

- **Risque de contamination et de tromperie :** C'est le talon d'Achille de l'HUMINT en matière de fiabilité. Une source humaine peut **se tromper ou mentir**, volontairement ou non. Elle peut être dès le départ un **agent double** au service de l'ennemi, qui transmet de fausses informations pour induire en erreur (par ex. un service adverse peut "lâcher" un agent en lui faisant jouer le rôle d'un transfuge, alors qu'il continue à travailler pour eux, afin de distiller des mensonges crédibles). Une source peut aussi **changer de camp** en cours de route (cas des officiers traitants occidentaux qui ont trahi pour Moscou – devenant en quelque sorte les "agents" de l'Est). Il y a aussi les **mythomanes** ou **fabricants** : des individus qui, pour de l'argent ou de la reconnaissance, inventent des renseignements plausibles. *Curveball* en est l'exemple typique : ce transfuge irakien a fourni aux occidentaux un récit détaillé mais fictif sur les armes biologiques de Saddam Hussein, contribuant à justifier l'invasion de 2003, alors que tout était faux [57]. Enfin, une source fiable peut **flancher sous la pression** – si elle est arrêtée et interrogée, elle peut divulguer de mauvaises informations ou se faire retourner. En somme, l'HUMINT comporte un **risque de désinformation** plus élevé que les capteurs techniques (qui n'enregistrent que des signaux bruts), d'où la nécessité de toujours recouper avec d'autres sources et de **vérifier la loyauté** des agents en permanence.

Outre ces quatre inconvénients majeurs, on peut ajouter la **capacité limitée** en volume : recruter 1000 espions est illusoire, alors qu'on peut lancer des milliers d'interceptions électroniques automatisées. L'HUMINT est donc précieux mais rare, et il faut l'employer là où il apporte la plus-value la plus grande. Par ailleurs, l'HUMINT dépend beaucoup de la **qualité humaine** des agents : un officier traitant médiocre ou peu expérimenté pourra mal exploiter une source, ou ne pas percevoir qu'il est manipulé, etc. La **formation** est donc un enjeu vital.

Enfin, l'HUMINT doit composer avec l'environnement moderne : la **surveillance généralisée** (caméras de rue, traçage numérique) complique la clandestinité ; l'**évolution des valeurs** fait que certaines

pratiques jadis acceptées (corrompre, piéger par des “honey traps” – pièges sexuels) sont aujourd’hui plus contrôlées. Malgré ces limites, il convient de rappeler que nombre de ces risques peuvent être **atténués** par des mesures adéquates (contre-contre-espionnage pour surveiller ses propres troupes, échanges de sources avec alliés de confiance pour recoupement, etc.). Surtout, les **avantages de l’HUMINT** – déjà évoqués dans la section précédente – font que les services sont prêts à prendre ces risques lorsque l’enjeu en vaut la chandelle. Sans l’HUMINT, **pas d’espionnage possible**, mais avec l’HUMINT vient la **zone grise de l’incertain et du danger**.

Applications actuelles de l’HUMINT

Dans le monde d’aujourd’hui, le renseignement humain est mis à profit dans **de multiples domaines** stratégiques et de sécurité. En voici quelques illustrations sectorielles :

- **Domaine militaire et opérations extérieures :** Les forces armées s’appuient largement sur l’HUMINT pour les besoins tactiques et stratégiques. Sur le terrain, les **unités de renseignement militaire** déploient des patrouilles de renseignement, collectent des infos auprès de la population locale (par ex. via des **équipes CIMIC** ou des interprètes servant de capteurs humains), et interrogent les **prisonniers de guerre ou ennemis capturés** pour obtenir des informations immédiates sur l’ordre de bataille adverse. Par exemple, durant les guerres d’Irak et d’Afghanistan, l’armée américaine a constitué des réseaux d’**informateurs locaux** (chefs tribaux, civils) fournissant des renseignements sur les caches d’armes, les mouvements des insurgés, etc. Les forces spéciales utilisent également l’HUMINT pour préparer leurs raids (contact dissimulé avec des informateurs à l’intérieur d’un camp ennemi, etc.). Au niveau stratégique, le renseignement humain militaire vise à évaluer les intentions et capacités des armées étrangères : recruter un officier dans l’état-major d’un pays rival peut offrir un éclairage direct sur ses plans de défense ou ses nouveaux armements. L’HUMINT fournit donc aux militaires un **avantage informationnel** décisif, en complément des drones et satellites, surtout dans les **conflits asymétriques** où la population locale est l’enjeu central (contrebande d’information, contre-insurrection).

- **Lutte antiterroriste et sécurité intérieure :** Dans le domaine de la sécurité nationale, l’HUMINT est un **outil clé pour déjouer les menaces diffuses** telles que le terrorisme, l’extrémisme violent, le crime organisé. Les services de renseignement intérieur (ou de sécurité d’État) investissent beaucoup dans la **surveillance humaine des milieux à risque**. Concrètement, cela passe par l’**infiltration de cellules terroristes** (placer un agent ou retourner un membre pour qu’il renseigne de l’intérieur), le recrutement d’**“indics”** dans la criminalité organisée (par exemple, un trafiquant qui devient informateur de la police sur un cartel), ou la mise en place d’opérations de **leurre** (un agent se fait passer pour un complice afin de mieux identifier le réseau). Les réussites en la matière sont souvent confidentielles, mais on sait que de nombreux attentats ont pu être évités grâce à une **source humaine anonyme** ayant averti les autorités. Par exemple, en France, plusieurs plans d’attaque jihadiste ont été déjoués dans les années 2010 grâce à des renseignements fournis par des **infiltrés** ou des repentis. La sécurité intérieure recourt aussi à l’HUMINT pour la **contre-ingérence** : identifier et surveiller les espions étrangers opérant sur le sol national. Cela peut impliquer de **retourner** un espion ennemi (le convaincre de travailler en double jeu) ou de mettre sur écoute/clairement filature ses contacts. En matière de **cyber-sécurité**, qui est un champ nouveau, l’HUMINT intervient également – par exemple en infiltrant des forums du Dark Web où échangent des cybercriminels [62], ou en retournant un hacker repenti pour qu’il guide les autorités à travers les cercles fermés du cybercrime. En somme, police, gendarmerie, douanes et services spécialisés combinent leurs moyens techniques de surveillance avec des **sources humaines de renseignement** pour assurer la sûreté du territoire face à des menaces internes souvent furtives.

- **Diplomatie et renseignement politique :** Historiquement, diplomates et espions sont intimement liés (beaucoup d'espions opèrent sous **couverture diplomatique**). L'HUMINT a donc naturellement sa place dans les **ambassades et consulats**, où les attachés de défense, les conseillers politiques, etc., passent une partie de leur temps à **collecter de l'information** sur le pays hôte en discutant avec les élites locales, en assistant à des événements, en posant des questions ciblées. Cette collecte **"à ciel ouvert"** fait partie du jeu diplomatique et n'a rien d'illégal (c'est de l'OSINT amélioré par du contact humain), mais certains diplomates vont plus loin et entrent dans le champ de l'espionnage classique. Par exemple, un diplomate peut **recruter un employé ministériel** du pays hôte pour qu'il lui transmette des documents confidentiels – c'est de l'HUMINT clandestin mené sous immunité diplomatique. Bien sûr, si cela est découvert, le diplomate-espion est expulsé manu militari. Au-delà des ambassades, la diplomatie secrète fait parfois appel à des émissaires "non officiels" disposant d'un réseau personnel. L'HUMINT sert aussi dans les **négociations internationales** : avoir une source qui renseigne en temps réel votre délégation sur la position réelle (et non celle affichée) de l'autre camp peut donner un atout majeur pour conclure un accord. Dans le renseignement dit "politique", l'objectif est de **prévoir les évolutions** d'un pays, les jeux de pouvoir internes, et les **intentions des dirigeants étrangers**. Cela peut passer par l'entretien de **"contacts privilégiés"** – hauts fonctionnaires, opposants, journalistes influents – qui partagent officieusement leurs analyses. Par exemple, pendant la Guerre froide, la CIA disposait en France d'un vaste réseau d'informateurs dans les milieux politiques et syndicaux, ce qui lui permettait de suivre l'influence communiste et les tendances politiques du pays. Aujourd'hui, de même, comprendre la politique interne chinoise ou russe nécessite non seulement de lire la presse (OSINT) mais aussi d'écouter des confidences de personnes bien placées – c'est du HUMINT diplomatique et politique de haut niveau.

- **Renseignement économique et technologique :** La compétition mondiale se joue aussi sur le terrain économique, et l'HUMINT y trouve des applications spécifiques. Le **renseignement économique** vise à acquérir des informations sur les négociations commerciales, les avancées technologiques d'un concurrent, les intentions industrielles d'un pays, etc. Parfois, ces informations sont publiques, mais souvent elles sont gardées secrètes par les entreprises ou les gouvernements. Les États, soucieux de préserver leur avantage économique, déploient donc des efforts de renseignement ciblés. Par exemple, un service de renseignement peut chercher à **recruter un cadre** dans une entreprise étrangère stratégique (aéronautique, énergie…) pour être tenu informé de ses programmes de recherche – on parlera d'espionnage industriel s'il s'agit de voler des secrets, ou d'**intelligence économique grise** s'il s'agit de veille borderline. La France a été à la pointe de cette démarche dans les années 1980-90 en déclarant vouloir utiliser ses services pour aider ses industries nationales (ce qui a valu quelques frictions avec des pays alliés). Plus récemment, la Chine est régulièrement accusée de mener un **espionnage économique systématique**, en s'appuyant sur des milliers de ressortissants (scientifiques, étudiants, ingénieurs) encouragés à recueillir des infos sensibles lors de leurs séjours à l'étranger. Du côté des entreprises elles-mêmes, l'appel à des sociétés privées d'intelligence économique s'est banalisé : ces sociétés emploient parfois d'anciens espions capables de **obtenir des renseignements concurrents** par des méthodes HUMINT (par exemple, interviewer des employés rivaux sous un faux prétexte pour soutirer des informations, ou s'introduire dans une conférence privée). Si ces pratiques dépassent la légalité, elles tombent sous le coup de la justice (il y a eu des affaires retentissantes d'espionnage industriel, ex : Uber vs Google, Renault suspectant ses cadres, etc.). Néanmoins, beaucoup d'informations stratégiques ne sont pas protégées pénalement, et l'HUMINT trouve là un vaste champ "gris" : connaître les intentions d'investissement d'un pays, les négociations d'un contrat d'armement, les futurs appels d'offres – autant de renseignements convoités obtenus en discutant avec les bonnes personnes. En somme, sur le front économique, l'HUMINT est devenu un outil de

compétitivité et d'**anticipation**, utilisé tant par les services étatiques que par les grandes entreprises dans la limite (élastique) du cadre légal.

Chaque domaine ci-dessus illustre que l'HUMINT reste **au cœur de la décision** en fournissant cet ingrédient particulier : la **compréhension humaine** fine derrière les faits bruts. Qu'il s'agisse de remporter une bataille, de prévenir un attentat, de négocier un traité ou de gagner un marché, le renseignement humain apporte souvent le petit plus déterminant qui fait pencher la balance.

Évolutions récentes et perspectives d'avenir

À l'ère des **nouvelles technologies** et de l'**intelligence artificielle (IA)**, le renseignement humain est confronté à de nouveaux défis mais aussi de nouvelles opportunités. Contrairement à certaines prophéties annonçant son déclin face aux machines, l'HUMINT tend plutôt à **s'adapter et se réinventer** en intégrant les apports technologiques tout en conservant son noyau humain irremplaçable.

Impact du numérique et de l'IA sur l'HUMINT : L'omniprésence du numérique a deux conséquences majeures. D'une part, l'**abondance de données ouvertes** (Open Data, réseaux sociaux) offre énormément d'informations disponibles sans espion traditionnel – ce qui a renforcé le poids de l'OSINT. Certaines tâches jadis confiées à des agents peuvent être accomplies par des analystes derrière leur écran (pister les relations d'une cible via Facebook plutôt qu'en filature physique, par ex.). D'autre part, la **surveillance électronique généralisée** rend la vie dure aux espions : caméras de vidéosurveillance en ville, traçage des communications, reconnaissance faciale, tout cela augmente le risque de détection d'un agent clandestin. Un espion voyageant sous une fausse identité laisse des traces numériques (réservations, paiements) qui peuvent être analysées par l'IA pour détecter des anomalies. Ainsi, paradoxalement, la même technologie qui fournit plus de données aux services sert aussi les contre-mesures adverses pour **débusquer les intrus**. On a vu par exemple en 2018 l'arrestation d'agents russes aux Pays-Bas qui avaient laissé des indices numériques de leur passage. Les espions doivent donc se former aux **opérations dans le cyberespace** : utiliser le Dark Web de manière anonyme, chiffrer toutes leurs communications, éviter les gadgets électroniques susceptibles d'être pistés.

Dans le même temps, les services explorent comment utiliser l'IA pour améliorer l'HUMINT. L'IA peut aider à **identifier des cibles potentielles** en fouillant des masses de données (repérer qu'un officier étranger semble mécontent de son régime via ses posts sur les réseaux sociaux, donc cible de recrutement possible). Elle peut aussi assister les officiers dans l'**analyse comportementale** : certaines solutions logicielles promettent de détecter les micro-expressions de mensonge lors d'un entretien filmé, ou de prévoir les réactions d'une personne. Toutefois, l'IA ne remplace pas le **jugement humain** dans la conduite d'un recrutement ou d'un interrogatoire – du moins pas encore. Un autre sujet brûlant est celui des **deepfakes** (trucages audio/vidéo générés par IA) : ils représentent à la fois une menace et un outil potentiellement. Côté menace, des deepfakes pourraient servir à **piéger des agents** (par ex. un agent reçoit un appel vidéo de son supposé officier traitant lui demandant de faire X, mais c'est un deepfake généré par l'ennemi – la *synthetic media* brouille la confiance). Côté outil, les services pourraient créer de faux profils en ligne ultra-réalistes (avec photos, vidéos crédibles générées par IA) pour faciliter les approches sur les réseaux sociaux (*catfishing* amélioré). L'éthique et l'efficacité de telles méthodes restent discutées.

HUMINT et cyberespionnage : La frontière entre HUMINT et renseignement technique tend à s'estomper dans le domaine du cyber. On parle par exemple de **SOCMINT** (Social Media Intelligence) pour désigner le recueil d'infos sur les réseaux sociaux – qui peut être passif (OSINT) ou actif (HUMINT si on interagit avec des personnes en se faisant passer pour un autre). Les cyber-espions (hackers) eux-mêmes deviennent des cibles de recrutement HUMINT : infiltrer une communauté de hackers peut

permettre de prévenir des attaques, mais cela nécessite d'agir sous couverture virtuelle. Les **opérations offensives** dans le cyberespace peuvent aussi bénéficier d'un renseignement humain : par ex., recruter un administrateur système d'une cible pour obtenir ses identifiants facilitera grandement un hack. Ainsi, on observe une convergence des approches : *« derrière chaque clavier, il y a un homme »*, rappellent les partisans de l'HUMINT dans le cyber. Et inversement, la réussite d'une opération humaine peut dépendre de moyens techniques (ex : exfiltrer en urgence un agent en danger grâce à sa balise de détresse GPS reliée par satellite). Le futur proche va sans doute accentuer cette **complémentarité inter-domaines** : les officiers HUMINT recevront des formations en cyber-sécurité, tandis que les cyber-analystes intégreront des éléments comportementaux dans leurs algorithmes.

Évolutions sociétales et HUMINT : Sur un plan plus humain, le métier d'espion évolue aussi avec la société. Les services cherchent à diversifier leurs recrues, intégrant plus de **femmes** et de personnes aux profils variés, dans l'idée que l'accès à certaines cibles peut être facilité par des agents reflétant cette diversité. Les femmes, par exemple, ont prouvé qu'elles pouvaient exceller dans le renseignement humain (par leur capacité d'écoute, leur moindre visibilité dans certains contextes machistes, etc.). La série française "Le Bureau des Légendes" a popularisé le concept d'**"illégaux"** – des agents français formés à vivre sous une identité fabriquée à l'étranger pendant des années. Ce concept, hérité du KGB, montre la volonté des services de s'adapter aux terrains difficiles (pays fermés, surveillance électronique) en investissant dans des **agents longue durée** particulièrement bien préparés. Dans un autre registre, les services intègrent les préoccupations éthiques modernes : ils forment leurs agents aux enjeux **déontologiques** (ne pas franchir certaines lignes, signaler les ordres illégaux) afin d'éviter les scandales type Snowden où un analyste choqué par des programmes de surveillance de masse a tout révélé. L'idée est de concilier l'efficacité opérationnelle avec la **confiance du public** dans le renseignement – un équilibre délicat.

L'HUMINT à l'horizon futur : À moyen et long terme, on peut spéculer sur l'impact des technologies comme l'**IA avancée** ou la **biotechnologie**. Peut-être verra-t-on émerger un **"HUMINT augmenté"** où l'agent sur le terrain sera assisté en temps réel par une IA qui lui soufflera des informations (par exemple via des lunettes connectées affichant les profils des personnes rencontrées en direct grâce à la reconnaissance faciale). Les avancées en **traduction automatique** abolissent déjà partiellement la barrière de la langue, ce qui aide les espions à opérer dans des pays dont ils ne maîtrisent pas parfaitement l'idiome. L'IA pourrait également aider à détecter plus rapidement qu'un agent a été compromis (en surveillant des paramètres inhabituels dans son comportement en ligne, etc.). À l'inverse, la lutte contre l'HUMINT adverse fera peut-être appel à des **IA contre-espionnes** scrutant les mégadonnées pour repérer des schémas suspects (par ex. *« qui, dans nos employés, semble vivre au-dessus de ses moyens ? »* – potentiellement indicateur qu'il est payé par une puissance étrangère).

Cependant, la quintessence de l'HUMINT reste la relation humaine, l'élément **psychologique** qu'aucune machine ne peut totalement reproduire. La **confiance mutuelle**, la **trahison**, la **conviction intime** sont des moteurs de l'espionnage qui relèvent de la nature humaine. Tant que la politique, la guerre et la stratégie impliqueront des êtres humains, il y aura besoin d'HUMINT pour comprendre et influencer ces êtres humains. En 2008, le Livre blanc français sur la défense notait déjà : *« Une attention particulière sera portée au renseignement humain »*, insistant sur la nécessité d'améliorer le recrutement et la formation dans ce domaine [63]. Depuis, les événements n'ont fait que confirmer cette orientation : face à des menaces asymétriques, dispersées et souvent furtives, l'HUMINT redevient un **atout primordial** là où la technologie atteint ses limites.

En conclusion, loin de disparaître, l'HUMINT se voit plutôt **renforcé et redéfini**. Il travaille main dans la main avec les outils technologiques, s'aventure sur de nouveaux terrains (virtuel, économique, sociétal), tout en préservant le cœur de sa valeur : la capacité d'**empathie** et d'**ingéniosité humaine** pour obtenir l'information là où personne d'autre ne peut aller la chercher. L'avenir de l'HUMINT sera ce que les

femmes et hommes du renseignement en feront – nul doute qu'ils sauront continuer à innover pour que, dans la bataille sans fin de l'information, **l'élément humain** fasse toujours la différence.

Bibliographie indicative

- **Wikipédia (fr)** – *Renseignement d'origine humaine (HUMINT)* [2] [60] . Article offrant une synthèse des concepts et enjeux du HUMINT, avec références académiques.
- **Ecole de Guerre Économique (EGE)** – *5 types de sources de renseignement humain (HUMINT)* [3] [37] (février 2024). Article en ligne détaillant les catégories de sources HUMINT et leur importance à l'ère numérique.
- **T. Yégavian**, « *Renseignement et espionnage pendant l'Antiquité et le Moyen-Âge* » [11] , *Le Monde diplomatique*, août 2020. Compte-rendu d'ouvrage montrant l'existence de l'espionnage organisé dès l'Antiquité.
- **J.-C. Cousseran & Ph. Hayez**, *Manuel du renseignement*, Presses de Sciences Po, 2016. (Ouvrage de référence en français, avec une analyse fine des avantages/inconvénients de l'HUMINT [64]).
- **M. Klen**, « *Éthique et déontologie militaire – L'interrogatoire des prisonniers de guerre* », *Revue Défense Nationale* n°733, 2010 [34] . (Analyse du cadre légal et moral de l'interrogatoire, exemples contemporains).
- **Fabien Lafouasse**, « *L'espionnage en droit international* », *Annuaire français de droit international*, vol.47, 2001 [42] . (Étude juridique sur le statut de l'espionnage et ses implications en temps de paix/guerre).
- **DCAF Genève** – *Les services de renseignement : document d'information SSR* (2015) [45] . (Rapport d'information avec définitions des différentes disciplines de renseignement et enjeux de gouvernance).
- **Pascal Martin**, *Human Intelligence in the age of new information and communication technologies*, Note recherche CREOGN n°91, Gendarmerie (sept. 2023) [65] [59] . (Analyse de l'impact des nouvelles technologies sur l'HUMINT, complémentarité des capteurs).
- **Central Intelligence Agency (CIA)** – *Studies in Intelligence – Selected Articles*. (Divers articles déclassifiés en anglais sur des opérations HUMINT historiques et leçons apprises).
- **Site du Musée du Renseignement (Intelligence Museum)** – (Ressources en ligne sur l'histoire de l'espionnage, biographies d'espions célèbres, gadgets et anecdotes).

Les références ci-dessus permettent d'approfondir chacun des aspects abordés dans ce rapport, qu'il s'agisse de l'histoire ancienne de l'HUMINT, de ses théories modernes, de cas concrets ou des problématiques contemporaines d'éthique et de technologie.

---

[1] [2] [6] [8] [10] [18] [19] [20] [25] [26] [27] [39] [54] [55] [56] [57] [58] [60] [61] [64] Renseignement d'origine humaine — Wikipédia
https://fr.wikipedia.org/wiki/Renseignement_d%27origine_humaine

[3] [4] [5] [28] [29] [30] [31] [37] [38] [40] [41] [51] [62] 5 types de sources de renseignement humain (HUMINT) | Ecole de Guerre Economique
https://www.ege.fr/infoguerre/5-types-de-sources-de-renseignement-humain-humint

[7] [9] [13] [15] [16] [21] [22] [23] [24] [53] Liste d'espions — Wikipédia
https://fr.wikipedia.org/wiki/Liste_d%27espions

[11] Renseignement et espionnage pendant l'Antiquité et le Moyen-Âge, par Tigrane Yégavian (Le Monde diplomatique, août 2020)
https://www.monde-diplomatique.fr/2020/08/YEGAVIAN/62095

12 Le culte de la transparence - Les billes de culture générale
https://lerevolver.blog/2018/12/07/le-culte-de-la-transparence/

14 17 49 52 Renseignement — Wikipédia
https://fr.wikipedia.org/wiki/Renseignement

32 33 34 35 36 48 Éthique et déontologie militaire - L'interrogatoire des prisonniers de guerre
https://www.defnat.com/e-RDN/vue-article.php?carticle=8101

42 43 L'espionnage en droit international - Persée
https://www.persee.fr/doc/afdi_0066-3085_2001_num_47_1_3655

44 45 46 47 dcaf.ch
https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_12_Les%20services%20de%20renseignement_0.pdf

50 HUMINT - Defense Intelligence Agency
https://www.dia.mil/Careers/Career-Fields/Human-Intelligence/

59 63 65 gendarmerie.interieur.gouv.fr
https://www.gendarmerie.interieur.gouv.fr/crgn/content/download/40754/file/Research_Note_CREOGN_91_human-intelligence-ntic_2023.pdf