

NUMÉRO 20 – MARS 2025

STRATÉGIE ET SÉCURITÉ



LE RENSEIGNEMENT

LES MONDES DU
RENSEIGNEMENT

HUMINT, OSINT,
GEINT, IMINT,
SIGINT...

OPÉRATIONS SPÉCIALES
ET ESPIONNAGE

Editorial des rédacteurs en chef

Auteur : Ciara McLaverty et Paulin Devanlay, Mastérants en Relations Internationales, Sécurité et Défense.

Le lundi 3 mars dernier, la Maison Blanche annonçait sa décision de geler l'aide apportée à l'Ukraine dans le cadre de sa guerre avec la Russie, à savoir l'aide militaire ainsi que le partage de renseignement. A ce propos, Andreï Kartapolov, un législateur russe et ancien officier avait déclaré : « It would be much more important if the Americans stopped giving them with intelligence information, then this would allow us to achieve results more quickly¹».

En réalité, depuis le début de la guerre en Ukraine, le partage de renseignements de la part des services américains s'est révélé crucial dans le déroulement du conflit, les Etats-Unis partageant des informations sur les mouvements et positions des forces armées russes, leur logistique ou encore l'interception de communications concernant les plans militaires et mouvement de leurs espions². L'arrêt temporaire de l'aide américaine dans le domaine du renseignement a généré de nombreuses inquiétudes à Kiev, celui-ci pouvant entraver la capacité de l'armée

ukrainienne à mener des frappes de drone dans la profondeur efficaces, n'ayant plus d'informations sur les cibles à l'intérieur de la Russie³, notamment lorsque l'entreprise de satellites américains Maxar a bloqué l'accès à ses services alors que les images satellites fournies par celui-ci permettaient à l'Ukraine d'étudier le terrain adverse.

Cette pause dans le partage de renseignement des Etats-Unis à l'Ukraine a également suscité de vifs débats à l'échelle européenne et des questions sur le long-terme concernant la dépendance de la sécurité du continent aux services de renseignements américains, un membre du Bundestag allemand, Konstantin von Notz allant jusqu'à proposer la création d'une alliance de renseignement européenne, « Euro Eyes⁴ », rappelant étrangement l'alliance de renseignement anglo saxonne existante Five Eyes⁵.

Le monde du renseignement fascine et ne cesse de susciter des fantasmes. Les nombreuses œuvres de fiction sur le sujet en témoignent et la figure de « l'espion » - qu'il soit séduisant comme le célèbre espion britannique James Bond ou plutôt à la OSS 117... dans un autre style - structure nos imaginaires collectifs. L'amalgame se fait,

¹ Bo Lillis, K., Sciutto, J., Cohen, Z., & Bertrand, N. (2025, 5 mars). Trump officials say US paused intelligence sharing with Ukraine but signal it may not last long after fiery meeting. *CNN Politics*. <https://edition.cnn.com/2025/03/05/politics/us-pause-intelligence-support-ukraine/index.html>

² « Intelligence that officials say has been as important as any American weapon system to both Ukraine's ability to protect its cities and push back on Moscow on the battlefield. », *Ibid*.

³ Harding, L., & Saddagh, D. (2025, 5 mars). US stops sharing intelligence on Russia with Ukraine. *The*

Guardian. <https://www.theguardian.com/world/2025/mar/05/us-stops-sharing-intelligence-on-russia-with-ukraine>

⁴ Mackinnon, A., Dettmer, J., & Mcleary, P. (2025, 8 mars). Europe scrambles to aid Ukraine after US intelligence cutoff. *Politico Defense*. <https://www.politico.com/news/2025/03/08/europe-scrambles-to-aid-ukraine-after-us-intelligence-cutoff-00219678>

⁵ Five Eyes est l'alliance de Renseignement entre les Etats-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande. Voir l'article page 37 de cette revue.

l'espion est un agent d'action, il recueille du renseignement, le renseignement tout entier se confond avec cet agent de terrain aux qualités exceptionnelles. La réalité est peut-être moins séduisante. Le renseignement n'est pas l'apanage d'un individu isolé en milieu hostile mais le produit d'une ou plusieurs structures organisées. Ces agences nationales de renseignement (CIA, DGSE, Mossad ou encore FSB) - pour ne citer que les plus connus - sont la face cachée des relations internationales, de la sécurité et de la Défense, en temps de paix comme en temps de guerre.

L'évolution des moyens technologiques au service du Renseignement ainsi que l'émergence de nouvelles menaces (terrorisme, acteurs non-étatiques, *rogue states*...) pousse ces agences à un renouvellement constant dans le but de conserver leur « temps d'avance » sur les pays. Le Renseignement est également un monde d'alliances, où espionner son allié est considéré comme une trahison, alors que le partage d'informations à un allié sur son adversaire permet de renforcer les liens diplomatiques (« Les ennemis de mes amis sont mes ennemis »). Or, même dans le monde du Renseignement, comme le disait le général de Gaulle : « les Etats n'ont pas d'amis, ils n'ont que des intérêts ».

Dans cette vingtième revue *Stratégie et Sécurité*, nous vous proposons de vous plonger dans le monde du Renseignement, sa théorie, ses applications, ses moyens et ses enjeux les plus saillants, afin de mieux comprendre le face cachée des relations internationales. HUMINT, OSINT, GEOINT ou encore

IMINT⁶, notre nouveau numéro s'ouvre avec des articles de théorie qui permettront aux novices comme aux experts de découvrir ou redécouvrir les différentes déclinaisons et pratiques de ce domaine.

Des services secrets français, chinois, américains, soviétiques, ou encore britanniques, à l'étude du renseignement économique, industriel et cyber ou encore à l'histoire des femmes espionnes pendant la première guerre mondiale, les analyses précises et thématiques que nos rédacteurs passionnés dresseront nous aiderons à mieux comprendre ce monde du secret.

Bonne lecture !

⁶ HUMINT: Human Intelligence ; OSINT: Open Source Intelligence ; GEOINT : Geospatial Intelligence ; IMINT : Imagery Intelligence.

Sommaire

GRAND ENTRETIEN.....	6
DOSSIER SPECIAL	14
THEORIE.....	14
Définition du renseignement et comparaison avec l'information.....	15
Du renseignement et des hommes : La dialectique entre technique et humain au service de l'information	18
DOSSIER SPECIAL	22
ETUDES DE CAS DES SERVICES DE RENSEIGNEMENTS NATIONAUX.....	22
Les services de renseignement français : compétition ou synergie ?	23
Les services de renseignement chinois, un réseau tentaculaire dangereux	28
Les Etats-Unis et l'éthique du renseignement.....	32
L'alliance Five Eyes et la coopération internationale en matière de renseignement	37
DOSSIER SPECIAL	43
LES NOUVEAUX ESPACES DU RENSEIGNEMENT	43
Le renseignement industriel au coeur de la guerre économique : synergies et rivalités entre États et entreprises	44
La numérisation des activités humaines et le tournant du renseignement vers la quantité.....	49
DOSSIER SPECIAL	53
HISTOIRE DU RENSEIGNEMENT	53
Les espionnes de la Seconde Guerre mondiale	54
Du KGB au SVB/FSR: l'histoire du renseignement de l'URSS à la Fédération de Russie	58
Les cinq de Cambridge.....	63
Le rôle du renseignement dans la non-prolifération nucléaire à travers l'exemple irakien.....	67
SCENARIO.....	72
Scénario : 2040 ou la fin des secrets d'Etat.....	73

HORS-SERIE	77
Hors-série : Du déclin de la pensée stratégique occidentale	78
POSTFACE	83

The background of the page is a complex, abstract geometric pattern. It consists of numerous overlapping, irregular polygons and lines in a light gray color. The shapes vary in size and orientation, creating a sense of depth and movement. The overall effect is that of a wireframe or a network of interconnected points and lines. The pattern is centered on the page and extends to the edges.

Grand Entretien

Grand Entretien

Avec M. Thierry Maurin, ancien Officier

Renseignement dans l'Armée de l'Air et de
l'Espace

Auteurs : Ciara Mclaverty et Hugo Swatridge, Mastérants en Relations Internationales, Sécurité et Défense.

Les opinions exprimées dans le cadre de cette interview n'engagent que leur auteur et en aucun cas l'Armée de l'Air et de l'Espace.

Dans un long entretien de près de deux heures, réalisé par Ciara Mclaverty et Hugo Swatridge, M. Maurin a accepté de revenir sur sa carrière dans l'Armée de l'Air et de l'Espace en tant qu'officier de renseignement.

Qui est notre invité ?
M. Maurin rejoint les rangs de l'Armée de l'Air française en 1991 où il sert en qualité d'officier de renseignement pendant près de 33 ans jusqu'en 2023. Il connaît plusieurs bases aériennes durant sa carrière : la BA 105 Evreux, la BA120 Cazaux, la BA101 Toulouse, le CPCO (en qualité d'officier traitant ciblage). Il termine sa carrière sur la BA942 de Lyon Mont Verdun affecté au CRA puis à la Brigade aérienne connaissance et anticipation.

Il a connu des théâtres d'opérations variés, des Balkans à l'Asie centrale, en passant par l'Afrique des grands lacs. Ciblage, planification, conduite des opérations aériennes, et plus encore, son expérience, riche par sa densité, fait de son témoignage aujourd'hui, une opportunité rare.

Après avoir pris sa retraite du monde militaire en 2023, il entame des aventures pas moins, sinon plus palpitantes. Après l'obtention d'un master Relations internationales et études de la sécurité internationale au sein de l'Université Jean

Moulin Lyon III, il s'engage cette fois-ci en qualité d'enseignant, notamment à l'ILERI. Thierry Maurin écrit dans la revue Vortex (Vortex n°4 Décembre 2022 Renseignement aérien et spatial « Bilan et perspectives de deux décennies d'adaptation du renseignement air à l'évolution de la conflictualité dans la 3e dimension », avec Sylvain Polizzi) et plus récemment dans l'ouvrage collectif « Les maîtres de la stratégie » (2025, sous la direction de Benoît Durieux et d'Olivier Wiewiorka) avec son chapitre sur William 'Billy' Mitchell de l'US Air Force, en apportant une réflexion sur le bombardement stratégique et le Global Air Power.

Sa carrière militaire, et l'expérience qu'elle recèle lui permettent ainsi de transmettre un savoir unique à la jeunesse d'aujourd'hui. Veille stratégique, relations internationales, grands enjeux stratégique et militaire en passant par l'emploi de l'arme aérienne, ses domaines de prédilection sont multiples.

Pourriez-vous succinctement présenter le métier d'officier de renseignement au sein de l'armée de l'air et de l'espace (AAE) ?

L'AAE fonctionne par spécialités regroupées au sein de trois corps. Le corps du personnel navigant, le corps des mécaniciens et le corps des bases. Le renseignement est une spécialité du corps des bases. La spécialité recouvre une variété de missions qui ont pour objectif commun la fonction d'aide à la décision. Certains orientent le renseignement en comprenant les besoins pour déterminer quels capteurs mettre en œuvre, pour combien de temps et sur quoi se focaliser. D'autres mettent en œuvre ces capteurs à travers l'utilisation d'avions et de drones. Une fois la donnée captée, cette dernière se transforme en information par un processus d'analyse, de mise en contexte avec d'autres informations et de synthèse. Une fois cela effectué, l'information devient alors du renseignement. Cette « fabrication » du renseignement recouvre à elle-seule une variété de métiers s'offrant à l'officier de renseignement, de la planification de la manœuvre à la captation d'informations en passant par l'analyse. Cette dernière étape permet de valoriser le renseignement récolté au bénéfice de la préparation des missions pour déterminer la meilleure façon d'atteindre l'objectif, de le traiter et de revenir.

La collecte de renseignement se fait aussi, occasionnellement, par l'opportunité avec le volet Non Traditional Intelligence Surveillance and Reconnaissance (NTISR). Cette dernière se fait par des moyens non dédiés à la collecte. Par exemple, un avion qui prendrait une photo d'un lieu suspect pendant sa simple mission de transport.

Quelles sont les différences entre le renseignement d'intérêt militaire et les

autres organes de renseignement en France (DGSE, DGSII2, TRACFIN...)?

Le niveau stratégique est réservé en grande partie aux directions. Un officier de renseignement au sein de l'AAE sera plus concerné par la tactique et l'opératif. En revanche, si ce dernier est rattaché à une direction (DRM, DGSE), sa priorité sera le stratégique et l'analyse.

Le renseignement d'intérêt militaire, c'est celui qui concourt à la préparation et à la mise en œuvre de la force militaire. L'organe qui y participe est la Direction du Renseignement militaire (DRM). Le militaire n'a pas vocation à intervenir sur le territoire français, c'est pourquoi la DRM est toujours tournée vers l'extérieur. Chaque armée va ensuite se spécialiser dans son domaine. Le renseignement d'intérêt air, par exemple, c'est le renseignement utile et nécessaire à la préparation et à la mise en œuvre de l'arme aérienne. Il faut éviter le piège de la binarité, un champ de mines par exemple n'est pas que du renseignement d'intérêt terrestre, il intéresse aussi l'AAE puisqu'il va dimensionner le plan d'évasion des équipages en cas d'éjection ainsi que les procédures de récupération de ces derniers. Ces notions de renseignement d'intérêt sont donc transverses.

Il existe aussi du renseignement d'intérêt économique ou politique. La DRSD4 a en charge le renseignement de contre-espionnage et de la protection du secret. La priorité des agences de renseignement françaises évolue, la DGSE s'est beaucoup orientée sur le contre-terrorisme, les questions économiques/industrielles et le renseignement d'intérêt politique. Si vous prenez l'exemple de la guerre en Ukraine, la DGSE se focalise plus sur les instances

politiques et les mouvements du Kremlin pendant que la DRM suit le théâtre d'opérations militaires. Il y a un risque, en multipliant les agences, qu'elles « se marchent sur les pieds ». En France ce n'est pas vraiment le cas, les six agences du premier cercle ont des périmètres et des compétences complémentaires. Le niveau politique veille à ce qu'il n'y ait pas de concurrence entre les agences et pour ne parler que du renseignement d'intérêt militaire, le discours des DRM successifs que j'ai connu était celui de la chasse aux doublons. Nous n'en avons, de toute manière, pas les moyens. Dépendant du ministère des armées, il y a la DRM, la DGSE et la DRSD. Il y a ensuite la DGSI qui dépend du ministère de l'intérieur, et le ministère de l'économie et des finances qui gère la DNRED et TRACFIN. Entre toutes ces instances, l'esprit de compétition n'est pas vraiment présent, au profit d'une collaboration évidente. Si vous prenez l'exemple du contre-terrorisme, DGSE et DGSI pour être efficaces sont contraintes de collaborer (cas d'individus radicalisés, détectés en France puis partis au Levant ou le cas inverse). L'opération Barkhane a été un cas d'usage de collaboration entre la DGSE et la DRM.

Quel est l'impact de la dimension psychologique sur la pratique du travail dans le domaine du Renseignement militaire ?

Le niveau de stress va d'abord dépendre du domaine dans lequel vous travaillez et à quel tempo ce dernier est associé. Quand il s'agit d'une cellule de crise à l'occasion de l'opération Barkhane, le rythme est très élevé. La pression temporelle vient notamment de l'exigence

de résultats de l'échelon supérieur. Cela crée un dilemme puisque les décideurs souhaitent une réponse rapide, alors que les processus de renseignement prennent du temps. Pour donner une réponse fiable il faut être sûr de l'information et donc avoir les capteurs adéquats, les orienter dans la bonne direction, patienter et espérer qu'ils captent quelque chose. Il faudra ensuite traiter, corréler et vérifier ce qui a été récolté pour enfin le transmettre. Comprendre la question initialement posée par le décideur pressé est aussi primordial.

La notion de point culminant (moment à partir duquel la poursuite de l'action est plus négative que positive) introduite par Clausewitz existe dans le renseignement. Il faut savoir à partir de quand il faut arrêter de chercher et délivrer une information partielle, plutôt que de perdurer à chercher et fournir une information complète mais trop tard.

Le capteur le plus adapté et correctement orienté dépend quoiqu'il arrive « des erreurs » et du comportement de sa cible. Le résultat n'est donc pas intégralement dans les mains de celui qui cherche. Notion que certains décideurs négligent ou ne veulent pas entendre.

Il y a aussi la question de la confiance, c'est pour cela qu'il faut être juste dans son jugement, puisque la parole portée par l'officier de renseignement constitue une aide à la décision. La justesse dans l'appréciation d'une menace est primordiale. Sous-estimez-la et vous perdez immédiatement tout crédit, surestimez la trop souvent et vous finirez par ne plus être écouté. Votre appréciation de la situation est toujours challengée par celle de votre décideur qui a sa propre vision des choses, (c'est humain et immuable) influencée par

une somme de choses allant de son expérience, les médias, un échange avec quelqu'un à qui il accorde une confiance supérieure, etc...

Il est aussi difficile de se séparer de son travail, cela est lié à la peur de manquer une information. Quand on rentre à la maison, la situation traitée est toujours dans la tête, puisque, par exemple, un théâtre d'opération ne s'arrête jamais. Il est fréquent de suivre pendant nos vacances les différentes situations avec des sources ouvertes et de continuer à réfléchir à celles-ci.

Un dernier phénomène pesant c'est le fait d'être constamment en concurrence avec les médias et réseaux sociaux actuels. L'information circule de manière quasi-instantanée. Une autorité peut venir vous poser une question en rapport avec un événement s'étant déroulé dans les dix minutes précédentes, alors que vous étiez en train d'analyser les informations de la veille. Cela crée donc parfois un décalage entre les traitants et les décideurs, poussant à une forme de pression.

Pourriez-vous nous décrire certaines évolutions marquantes que vous avez vécues au cours de votre longue carrière, concernant les moyens de renseignement de l'AAE ?

Il y a d'abord la numérisation. Cela a permis plusieurs évolutions, notamment dans le domaine de la photographie. Il existait, au début de ma carrière, des interprètes photos qui analysaient les pellicules développées. Ce processus était extrêmement chronophage avec une quantité limitée de photos analysées. Avec la numérisation, l'interprétation ne se fait plus sur une photo mais sur une image. Le temps d'accès à l'image a été

considérablement réduit, la qualité est bien meilleure et le nombre de clichés pertinents à analyser a fortement augmenté. L'imagerie s'est étendue du domaine du visible à ceux de l'infra-rouge et du radar. Tandis que l'observation n'était envisageable que de jour et par beau temps, à présent l'observation est également possible (dans certaines mesures) de nuit et par mauvais temps. Quand je suis arrivé dans l'AAE, la première génération de satellites entrainait en service. Trois générations de satellites plus tard, la France voit mieux, plus et plus vite. Cette efficacité entraîne néanmoins un problème puisqu'il faut un nombre plus important d'interprètes image pour traiter ces nouvelles données. L'IA, en cours de déploiement, se révèle indispensable pour tenter d'absorber le flux conséquent d'images.

Pour rester dans le domaine de l'imagerie, une évolution marquante a été le passage de la reconnaissance à la surveillance. La reconnaissance c'est un instant précis représenté sur une image. La surveillance c'est l'observation en continue d'une zone. Cette technique permet de dresser un Pattern of Life, des habitudes de vie pour mieux connaître la cible. Le renseignement obtenu n'est donc pas le même.

La numérisation a aussi investi le spectre électromagnétique. Les signaux analogiques sont remplacés par des signaux numériques bien plus difficiles à analyser. Les trames radars sont de plus en plus complexes et les communications sont maintenant cryptées. De véritables défis dans le domaine du ROEM avec l'apparition notamment de nouveaux savoir-faire comme le COMINT technique qui consiste à caractériser un signal et

l'attribuer à un porteur à défaut de pouvoir accéder au discursif.

Enfin, la numérisation a permis la création de bases de données, permettant une meilleure capitalisation du renseignement pour le réutiliser plus rapidement et en archiver le maximum. La base de données permet de rendre exploitable ce qui a été lu, c'est le passage capital d'une base documentaire (ensemble des documents détenus) à une base de connaissances (capitalisation de l'exploitation des documents détenus).

L'émergence d'Internet a généré dans les services de renseignement une nouvelle discipline : la veille des sources ouvertes numériques. Il en est de même pour l'apparition des réseaux sociaux, qui a été accompagnée par une surveillance accrue de ces mines d'informations. La veille sur internet était au début une discipline du renseignement qui n'était pas prise au sérieux. Elle a depuis fait ses preuves et acquis ses lettres de noblesse. Elle répond aux mêmes processus et exigences que les autres disciplines. C'est un métier à part entière. On lui doit beaucoup...

La combinaison de certaines de ces évolutions permet l'existence de ce qui est appelé la transparence du champ de bataille. La guerre en Ukraine par exemple est très documentée, il y a aussi toutes les interactions des combattants, entre eux ou sur les réseaux sociaux. Il y a donc beaucoup d'informations qui circulent ce qui en fait un terrain de jeu idéal pour les différentes agences de renseignement étatiques.

Pouvez-vous nous raconter une mission ou une opération qui vous a particulièrement

marqué en tant qu'officier renseignement ?

Les missions les plus significatives sont couvertes par le sceau du secret... J'ai une certaine idée du métier que j'ai exercé pendant 33 ans. L'officier de renseignement n'est pas le notaire du jour d'avant, c'est-à-dire celui qui capitalise consciencieusement ce qu'il s'est passé et qui raconte l'histoire récente. C'est beaucoup plus le prévisionniste du jour d'après, c'est-à-dire d'être en mesure de verbaliser plusieurs hypothèses de ce qui pourrait arriver en leur attribuant un niveau de probabilité. Le terme prévisionniste ne s'emploie que dans le domaine de la météorologie et celui de la bourse. Il colle pourtant parfaitement à la fonction renseignement.

J'ai travaillé à l'élaboration d'un indice d'alerte sur la probabilité de survenance des vols des bombardiers stratégiques russes aux abords de l'espace aérien français. Ces vols qui avaient disparu avec l'effondrement de l'URSS, ont été réactivé en 2007 et pris une certaine importance entre 2014 et 2022... J'ai obtenu de bons résultats permettant une évolution des procédures de la Posture Permanente de Sureté-Air (PPS-Air), mission prioritaire de l'AAE avec la Posture Permanente de Dissuasion (PPD). Voilà à quoi sert la fonction renseignement, on a le sentiment du devoir accompli. Bien entendu, ce qui est vrai en temps de paix l'est moins voire plus du tout en temps de guerre. Je ne doute pas que mes successeurs aient travaillé à l'évolution des critères de cet indice d'alerte en raison de la guerre en Ukraine.

Comment s'opère le renseignement interarmées en France ? Quelles sont les

particularités de l'apport de l'AAE au renseignement militaire ? En quoi le renseignement est-il différent des activités de la Marine Nationale ou de l'Armée de Terre ?

La fusion interarmées se fait à la DRM. Chaque composante dispose de capteurs et d'un centre de renseignement (CRT, CRA, CRGE). Les trois armées ne se contentent pas de travailler pour leurs besoins exclusifs. Cela n'a d'ailleurs pas de sens puisqu'on a vu précédemment que les notions de renseignement d'intérêt sont transverses. Le tempo est battu par la DRM. C'est-à-dire qu'elle oriente et coordonne les actions de renseignement des trois armées pour bâtir le renseignement d'intérêt militaire dont elle est la garante. Elle gère les différentes demandes et en fonction des questions posées elle oriente ses propres capteurs ou se tourne vers telle ou telle armée pour collaborer. L'analyse de toutes ces données se fait par niveaux. Le premier niveau d'exploitation est celui du capteur, par exemple l'analyse de l'image prise par un Rafale. Le second niveau est celui du centre d'armée, dans ce cas le CRA mettra en perspective le renseignement tiré de ladite image avec les autres renseignements détenus à son niveau. Enfin le troisième niveau d'exploitation est celui de la DRM qui mettra en perspective les renseignements issus du CRA avec ceux des autres centres d'armées. Le tout fera l'objet d'une note de renseignement pour la collectivité.

Ce processus peut paraître long et fastidieux, il relève du renseignement stratégique. Pour les théâtres d'opération où les forces françaises sont engagées, il ne s'agit plus de renseignement pour savoir mais du renseignement pour agir, aussi des

structures et des procédures adaptées sont mises en place pour aller plus vite.

Comment s'articulent les jeux d'alliances et/ou de dépendance dans le renseignement interalliés ?

Le livre blanc de 2008 introduit cinq fonctions stratégiques, la première étant Connaissance et Anticipation. La fonction est rebaptisée Connaissance, Compréhension et Anticipation avec la Revue Nationale Stratégique de 2022. Cela prouve l'importance du renseignement puisqu'avant de dissuader un Etat, il faut savoir qui nous menace, comment et pourquoi. Dans l'ADN français il y a la nécessité d'avoir une autonomie stratégique, qui passe par l'autonomie de l'appréciation de la situation. C'est pour cela que la France a des services de renseignement complets, cohérents et qui performant.

Être capable de fabriquer son propre renseignement n'exclut pas la coopération. La France collabore donc avec ses partenaires mais sans aucune forme de dépendance. La France entretient des échanges de renseignements en bilatéral ou multilatéral comme dans le cadre de l'OTAN ou la participation à des opérations en coalition. A chaque fois les échanges sont réalisés sous le principe de Chatham House⁶. Sont aussi bien échangées des données brutes (épurées de certains paramètres pour ne pas compromettre nos capteurs) que des données élaborées (notes d'appréciation par exemple).

Selon vous, quels sont les enjeux futurs du renseignement pour l'AAE ?

Un des défis principaux pour les agences de renseignement est l'infobésité.

L'IA s'impose comme solution à ce qu'on appelle le Big Data. Des solutions sont déjà en place pour soulager les tâches répétitives et ne nécessitant pas une charge cognitive importante. Le défi est surtout de définir les outils à mettre en place pour les tâches cognitives les plus élevées : comprendre un texte, relier un texte à un ou plusieurs autres, procéder à la mise en base de données automatique (génération automatique de la base de connaissances). Les possibilités offertes par l'IA et ses progrès rapides peuvent nous amener à penser que le concept même de base de données est peut-être devenu obsolète. L'avenir nous le dira. Les analystes militaires sont sujets à la mutation. Chaque mutation est un défi, le partant maîtrisant son sujet lorsque l'arrivant se l'approprié. De la qualité des bases de connaissances, dépend donc la performance des services. C'est là que l'IA doit apporter toute sa puissance.

Un autre enjeu pour la fonction renseignement est sa mise en concurrence constante avec les réseaux sociaux et les médias sur lesquels apparaissent des "experts" en tout genre. La tentation est grande pour un décideur d'écouter à temps perdu, sur les ondes ou à la télévision, ces « experts ». Le risque, déjà vécu à de multiples reprises, c'est que les services soient contraints de passer du temps à convaincre que leur analyse est la bonne contrairement à celle de « l'expert »...

Plus spécifiquement, le renseignement de l'AAE est confronté au défi de la très haute altitude, cette partie haute de l'espace aérien, entre 20 et 100 Km d'altitude, mise en lumière par l'affaire des

ballons chinois. Il s'agit de savoir précisément ce qu'il s'y passe et de l'exploiter avec de nouveaux capteurs. Elle offre des opportunités intéressantes et beaucoup moins onéreuses que l'espace exo atmosphérique. Le train est en marche, il s'agit de ne pas rester sur le quai.

L'ouverture de nouveaux espaces de conflictualité favorise l'apparition de nouveaux champs d'action pour les agences de renseignement, notamment dans le cyber, le domaine de l'influence ou l'espace. Tout cela entraîne la création de nouveaux sujets pour les agences, et donc in fine de nouveaux métiers et de nouvelles disciplines. Il est nécessaire que les trois armées veillent constamment sur ces espaces pour permettre une réponse efficace.

Enfin, l'évolution des équilibres stratégiques et la prise de conscience d'un nécessaire réarmement focalisent les esprits vers la question de la masse des armées et de leurs stocks de munitions. C'est effectivement la priorité mais il ne faut pas qu'à l'occasion de cet effort d'équipement, que la fonction renseignement soit oubliée. Si le recours à l'IA et à la réserve peut satisfaire le volet des ressources humaines, il n'en reste pas moins que la durée de vie des capteurs est comptée et qu'il faut régulièrement les renouveler. Par ailleurs la fonction renseignement est à l'image du reste des armées, adaptée et dimensionnée principalement pour la basse intensité dans des zones permissives ou semi-permissives. A ma connaissance, les ukrainiens ne mettent pas en œuvre, et pour cause, des REAPER ou des ALSR par exemple.



Dossier Spécial

Théorie

Définition du renseignement et comparaison avec l'information.

Auteur : Victor Suteau, Mastérent en Francophonie, Stratégie et Relations Internationales.

Information, renseignement ou Renseignement ?

Dans le rapport « Étudier le renseignement : État de l'art et perspectives de recherche » dirigé par Olivier Chopin, l'IRSEM tente de définir le renseignement et admet qu'aucune définition n'est universelle. Le rapport souligne cependant la définition établie par Jacques Baud dans son article « Renseignement » de l'*Encyclopédie du renseignement et des services secrets*, qui définit le renseignement comme une « information évaluée et exploitée ayant passé le cycle du renseignement et prête à être livrée à un client¹ ». Elle correspond à la première définition du renseignement écrite avec un « r » minuscule, désignant l'information transformée, élaborée et interprétée. Le renseignement ne se limite cependant pas à sa substance ; il est aussi une activité à part entière institutionnalisée, adoptant cette fois un caractère en majuscule pour le différencier.

Le Renseignement se définit quant à lui comme « l'ensemble des activités visant à rechercher et exploiter des informations au profit d'un État et de ses forces armées. Il est exécuté aux niveaux stratégique, opérationnel et tactique, dans les domaines les plus variés² ». Cette définition met en évidence la transformation de l'information brute en une ressource exploitée pour la prise de décision. En outre, elle distingue le renseignement de l'information simple en insistant sur l'étape d'analyse et

Le cycle du renseignement :

Déclenché par l'expression d'un besoin en renseignement ;

Continu car il organise de manière cohérente et progressive la réalisation des besoins ;

Réactif car il s'achève par la confrontation entre les besoins exprimés et ceux satisfaits, générant ainsi des besoins nouveaux ou une relance de la recherche ;

Dynamique car chaque phase du cycle est activée en permanence.



[Ministère des Armées](#)

d'exploitation. Le renseignement est une information qui doit être prélevée de la bonne source, détectée et rapportée au bon destinataire dans le bon tempo comme le définissait Pierre Joxe, ministre de la Défense : « Le renseignement de défense est traditionnellement un instrument privilégié pour la compréhension des rapports de forces internationaux, la prévision des conflits, la conduite des guerres. Par excellence, il symbolise, dans le domaine de la défense, cet outil de la connaissance permettant, selon l'aphorisme Auguste Comte, de « savoir pour prévoir afin d'agir » ; j'ajouterai : afin d'agir le cas échéant³. »

Le cycle du renseignement

L'aspect fondamental du renseignement repose sur le cycle du renseignement. Ce dernier diverge selon les États et les institutions ; nous prendrons celui établi par la Direction du renseignement militaire, qui comprend plusieurs phases clés : la collecte,

¹ Jacques Baud, *Encyclopédie du renseignement et des services secrets*, Paris, Lavauzelle, 1998, seconde édition, article « Renseignement », pp. 462-463.

² *Ibid.*

³ Joxe, Pierre. « Défense et renseignement. » *Revue* n° 522 Juillet 1991.

correspondant à l'obtention de données brutes par divers moyens ; le traitement, qui constitue l'analyse et le croisement des informations pour les rendre exploitables ; enfin, la diffusion, qui est la transmission des renseignements aux décideurs et aux opérateurs⁴.

De la théorie à la pratique

09/11 - L'échec du traitement de l'information

Le 11 septembre 2001 est un exemple cuisant de l'importance cruciale que représente le renseignement dans les domaines régaliens de la Défense et de la Sécurité intérieure. Cet événement marque un tournant dans l'histoire du renseignement. En amont des attentats, plusieurs informations avaient été recueillies par différentes agences de renseignement américaines, mais elles n'ont pas été correctement analysées ni mises en relation ; ainsi, ces données sont restées des informations brutes. Parmi les nombreuses informations remontant des différents services de renseignement américains, à savoir : la CIA, le FBI, et la NSA essentiellement, on retrouve la note du 10 août 2001 adressée à la CIA pour le président G.W. Bush. Cette note stipule dans son premier paragraphe: « Clandestine, foreign government, and media reports indicate Bin Laden since 1997 has wanted to conduct terrorist attacks in the US. Bin Laden implied in US television interviews in 1997 and 1998 that his followers would follow the example of

World Trade Center bomber Ramzi Yousef and "bring the fighting to America»⁵.» Le rapport pointe également du doigt le manque de coopération entre les différentes agences de renseignement américaines : « Information was not shared, sometimes inadvertently or because of legal misunderstandings. Analysis was not pooled. Effective operations were not launched. Often the handoffs of information were lost across the divide separating the foreign and domestic agencies of the government⁶. » Des erreurs lancinantes, similaires à celles commises lors des attaques de Pearl Harbor. Ainsi, en revenant à notre cycle de renseignement, nous pouvons constater que l'étape consistant à recouper les informations, à les rassembler et à les synthétiser a été manquée. Il en résulte l'échec de la centralisation du renseignement confiée à la CIA en 1947, puis au DNI à partir de 2005. L'agence n'a ainsi pas donné toute la valeur stratégique à l'information recueillie.

La Bataille de Denain (1712) – Le Renseignement décisif

En 1712, durant la Guerre de Succession d'Espagne, la France, affaiblie par plusieurs défaites, semble sur le point de céder Landrecies, dernière place forte française avant Paris, et d'être envahie par les forces alliées commandées par le prince Eugène de Savoie et le duc de Marlborough. Le maréchal français Villars, commandant les troupes de Louis XIV, doit empêcher l'effondrement du royaume, fort de ses 70 000 hommes face aux 130 000 coalisés⁷.

⁴ Ministère des Armées. « Nos Missions. » *Défense.gouv.fr*, Direction du Renseignement Militaire.

⁵ Bush, George W. *Presidential Daily Brief: Bin Ladin Determined to Strike in US*. CIA, 6 août 2001. National Archives

⁶ National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. U.S. Government Printing Office, 2004.

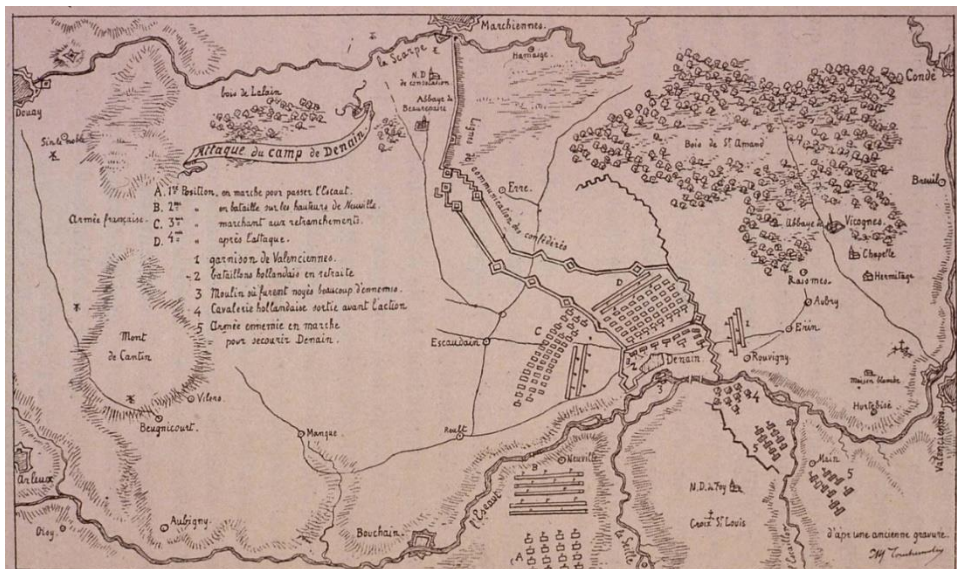
⁷ Herodote. « 24 juillet 1712 : La bataille de Denain. » *Herodote.net*

Parmi les trois grands acteurs de la bataille de Denain, on retrouve le conseiller au Parlement de Flandre, Jean-Robert Lefebvre d'Orval, le maréchal de Villars et le marquis de Montesquiou. C'est Lefebvre d'Orval qui semble avoir joué le rôle essentiel en organisant à la frontière un dense service de renseignements et d'espionnage au ministre de la Guerre Voysin ainsi qu'au maréchal de Villars. L'étude de Maurice Sautai révèle que cet homme de robe, a insisté dans toutes ses lettres sur les immenses avantages d'une attaque contre le camp retranché de Denain. Il a même tracé les grandes lignes de l'opération. Précisément, il a indiqué jusqu'aux points de passage sur l'Escaut les détails de l'opération que l'armée entreprendra le 24 juillet 1712⁸. Ce succès militaire repose sur la transformation d'une information en un renseignement exploitable.

Conclusion

Ce premier article introductif aura donc eu pour but de dresser un rapide aperçu des enjeux qui recouvrent le domaine du renseignement, lesquels seront approfondis dans les articles suivants. Si la confusion persiste parfois entre « renseignement » et « information », cet article, au travers de son explication puis de ces deux exemples historiques, aura su démontrer leurs différences fondamentales : si toute donnée est une information, tout renseignement est une information traitée et analysée pour produire une valeur stratégique. En d'autres termes : l'information est brute, accessible à tous, multiple et dispersée. Le renseignement, quant à lui, est structuré, confidentiel (secret) et orienté vers un objectif stratégique.

V.S.



Touchemolin, Alfred (1829-1907), Croquis simplifié de l'Attaque du camp de Denain (1897) à partir de la même source, BNU de Strasbourg – Source : BnF / Gallica

⁸ Sautai, M. « Les dernières années de Lefebvre d'Orval. » *Revue du Nord*, vol. 3, no. 3, août 1912, pp. 197-244,

Du renseignement et des hommes : La dialectique entre technique et humain au service de l'information

Auteur : Clémence Ripoché, Mastérante en Relations Internationales et Diplomatie.

Le renseignement est un domaine stratégique inscrit dans le temps long, pilier essentiel de la politique étrangère des États. Cette quête de connaissance et de maîtrise de l'environnement est ancestrale, comme l'illustre l'épisode biblique de Josué envoyant des espions à Jéricho : « Josué, fils de Nun, fit partir secrètement de Sittim deux espions, en leur disant : Allez, examinez le pays, et en particulier Jéricho. Ils partirent, et ils arrivèrent dans la maison d'une prostituée, qui se nommait Rahab, et ils y couchèrent » (Josué, 2,1¹).

À côté de l'action visible conventionnelle et diplomatique, l'action clandestine et secrète garde sa place. Cette action invisible para-diplomatique² se mène en fonction d'une politique et d'une stratégie secrète, en englobant, outre l'action, le renseignement et le contre-espionnage. Le renseignement suit un processus rigoureux : il commence par la collecte de données, suivie de leur tri et de leur enrichissement, puis de l'identification des liens pertinents qui les transforment en informations exploitables. Une fois analysées et replacées dans leur contexte, ces informations deviennent du renseignement prêt à être utilisé. Les différentes techniques de renseignement

sont désignées par l'acronyme anglophone « INT » soit « intelligence ». On entend par « INT », ce que Cattell et Horn³ distinguent entre intelligence cristallisée et intelligence fluide. Aujourd'hui, cette distinction fait office de modèle central dans l'étude de la cognition et de la résolution de problèmes. Les humains possèdent une aptitude innée à relier divers éléments d'information pour former des structures cohérentes, réutilisables et transmissibles d'une génération à l'autre.

Au fil du temps, le renseignement a su évoluer, s'adaptant aux mutations technologiques et à l'ère numérique. Malgré la montée en puissance des outils de surveillance et d'analyse, le renseignement humain (HUMINT) demeure un levier central. Depuis la fin des années 1980, la révolution numérique a transformé la société, et le renseignement n'y échappe pas. Internet, avec ses protocoles de transfert de données, permet la diffusion rapide et massive d'informations et cette mutation a bouleversé les pratiques et donné naissance à une génération totalement connectée. Internet, et son outil le plus puissant à ce jour, le *World Wide Web*, ont la capacité de transformer l'évolution de l'intelligence humaine et d'étendre les activités cognitives dirigées et structurées

¹Vial, Fabrice. *et al.* « L'importance du renseignement humain à l'ère numérique dans une démarche de conformité ». Revue Cyber & Conformité, 2021/3 N° 3, 2021. p.12-14.

² Ministère des Armées. « Le Renseignement à l'Ère du Numérique. » Chemins de Mémoire, Direction du Renseignement Militaire, 2023.

³ Cattell, Raymond B. « Some Theoretical Issues in Adult Intelligence Testing. » *Psychological Bulletin*, vol. 38, no. 7, 1941, pp. 592-593. et Horn, John L. « Fluid and Crystallized Intelligence: A Factor Analytic and Developmental Study of the Structure among Primary Mental Abilities. » Thèse de doctorat, Université de l'Illinois, 1965.

de l'esprit humain au cœur de l'univers de l'information. Dans ce contexte, le renseignement technique a pris une ampleur inédite et grâce aux outils de surveillance avancés, aux satellites et aux algorithmes d'analyse, il capte et traite un volume colossal de données. Dans le renseignement technique, on inclut, le SIGINT (écoutes électroniques : surveillance et interception des communications), l'IMINT (imagerie satellite : vision stratégique des conflits), l'OSINT (sources ouvertes : démocratisation de l'accès à l'information), et le GEOINT (renseignement géospatial : analyse des déplacements et terrains d'opération). Alors, le renseignement technique a-t-il relégué le facteur humain au second plan ou assistons-nous à une hybridation de ces deux « intelligences » ?

Renseignement technique ou renseignement humain : des logiques distinctes mais complémentaires

On oppose bien souvent le renseignement technique au renseignement humain, mais ces deux façons de faire, bien que distinctes, restent complémentaires. Si les technologies offrent des capacités de surveillance et d'analyse sans précédent, elles ne peuvent remplacer la finesse et le discernement de l'intelligence humaine. Loin d'être opposées, ces deux dimensions se nourrissent mutuellement. La technologie permet d'agréger, d'analyser et de croiser d'immenses quantités de données, mais c'est l'humain qui leur donne du sens, les valide et les exploite intelligemment. On

observe une synergie entre renseignement humain et technique.

L'*Open source intelligence*⁴ est le meilleur exemple du résultat de l'évolution des relations entre l'humain et l'information, due à l'émergence et à la domination croissante d'Internet et du Web dans la vie quotidienne. Internet et le Web continuent de susciter confusion et crainte à mesure que nous avançons dans cette nouvelle ère du renseignement, mais l'OSINT a su en tirer le meilleur (ou le pire) des possibilités extraordinaires de cette augmentation de l'intellect humain, à condition de comprendre et d'en exploiter le potentiel⁵. Les développements plus récents d'Internet ont créé de nouveaux rôles pour la symbiose entre l'homme et la machine dans les relations à l'information, augmentant ainsi réellement l'intelligence humaine dans la résolution dynamique de problèmes. Cette technique a contribué à populariser un capteur spécifique des services de renseignement puisque l'ère de l'information engendre une démocratisation des capacités de recherche, de recueil et d'exploitation des données, qui ne sont plus uniquement réservées aux services de renseignement. Les caractéristiques de cette manière de se renseigner reposent sur : une source accessible librement, de manière légale et gratuitement. Le renseignement d'origine source ouverte constitue en effet un moyen de collecte essentiel au processus d'exploitation et d'analyse du renseignement, aux côtés du renseignement électromagnétique (SIGINT) ou encore du renseignement

⁴ Renault, Clément., et al. « Renseigner autrement ? Trajectoires de l'Osint dans les services de renseignement ». Hérodote, 2022/3 N° 186, 2022. p.19-30.

⁵ Glassman, Michael, and Min Ju Kang. « Intelligence in the Internet Age: The Emergence and Evolution of Open Source Intelligence (OSINT). » Computers in Human Behavior, vol. 28, no. 2, Mar. 2012, pp. 673-682.

d'origine image (IMINT). Ainsi, les avantages du renseignement technique sont nombreux ; collecte massive, couverture large, rapidité de traitement grâce aux algorithmes et à l'IA.

Toutefois, le renseignement humain reste une approche irremplaçable pour l'interprétation, la contextualisation et tout le volet qui échappe à la technologie. Le couple d'agents dormants russes Artiom Doultsev et Anna Doultseva sont la preuve de cette efficacité de l'HUMINT, qui passe au-delà de ce dont les moyens techniques sont capables. Ils ont été arrêtés en décembre 2022 en Slovénie, où ils étaient arrivés en 2017. Ils y vivaient avec des passeports argentins, sous les noms de Ludwig Gisch et de Maria Rosa Mayer Munos, avec leurs deux enfants. Le renseignement humain, soit HUMINT⁶, repose sur l'intelligence et le savoir-faire des agents, qui recueillent des informations auprès de sources humaines en mobilisant des compétences analytiques, relationnelles et stratégiques. Ce travail s'organise autour de plusieurs étapes essentielles, soit l'étude, qui définit les actions à mener, la préparation qui structure les opérations et la gestion des sources, qui implique l'entretien et l'activation des réseaux d'informateurs. L'HUMINT s'appuie sur des agents infiltrés, informateurs et sur des réseaux « d'honorables correspondants ». C'est un renseignement de terrain : validation des données, compréhension des motivations adverses, adaptation aux spécificités locales. L'HUMINT aura toujours la capacité de combler les failles des outils

techniques tels que les risques de manipulation de données (deepfake, brouillage). Le chercheur s'efforce de répondre aux exigences de la collecte de renseignements et de combler les lacunes d'analyse. C'est aussi un renseignement qui s'apparente à un « art de la manipulation⁷ », manipulation des sources, jouant parfois avec les failles des relations humaines. L'échec des renseignements purement techniques face aux attaques surprises souligne l'importance de l'interprétation et de l'adaptabilité humaine restant cruciales face aux limites du « tout technologique ».

Néanmoins, l'HUMINT relève d'enjeux éthiques et politiques : la nécessité d'un équilibre entre sécurité, respect des libertés et efficacité opérationnelle. Le renseignement humain reste une entreprise délicate ; les exigences, en démocratie, de transparence et de contrôle politique, devraient aller de pair avec celles requises, par le secret des opérations.

Une nécessaire hybridation face aux nouvelles menaces

Nous vivons dans un monde où la circulation des informations est devenue instantanée, où l'incertitude des risques et menaces actuelles confèrent une place prépondérante à la connaissance et à l'anticipation⁸. A travers ce prisme, il est nécessaire de savoir quel est l'avenir pour le renseignement, et comment celui-ci s'adapte-t-il ?

Face à l'évolution des conflits et du

⁶GALLAGHER, Michael. « Human Intelligence in Counterinsurgency: Persistent Pathologies in the Collector- Consumer Relationship », Small Wars Journal, June 5, 2011, pp.2-3.

⁷Rondot, Philippe. « Face aux menaces diffuses, le

renseignement humain devrait pouvoir garder sa place ». *Après-demain*, 2016/1 N ° 37, NF, 2016. p.34-36.

⁸ Masson, Michel. « L'avenir du renseignement ». *Géoeconomie*, 2009/4 n° 51, 2009.

renseignement, la connaissance est devenue un outil maître dans les stratégies des États, menant à de nouvelles formes de conflictualité telle que la guerre de l'information⁹. Les nouvelles menaces asymétriques comme le terrorisme, les cyberattaques et les guerres hybrides, impliquent la maîtrise de cette connaissance de l'ombre et du renseignement. L'information est manipulée, et usée comme une nouvelle arme, pour troubler les stratégies de sécurité des États. Dans cette ère de la désinformation et des *fake news*, on note l'importance du renseignement humain pour vérifier et contrer les manipulations informationnelles. Le renseignement humain fait donc petit à petit sa place dans l'ère du numérique et se joint aux processus de renseignement technique. Le facteur humain devient plus stratégique pour s'adapter aux nouveaux terrains du renseignement. Loin d'être antagonistes, ces formes de renseignement s'articulent en une dialectique essentielle. On témoigne d'opérations de renseignement modernes mêlant HUMINT et techniques avancées, soulignant l'importance des analystes et de la prise de décision basée sur une intelligence hybride. C'est le cas de la traque d'Oussama Ben Laden, illustrant parfaitement l'alliance entre renseignement humain et technologique. En effet, sur une longue période, des agents infiltrés et des informateurs locaux ont suivi la piste d'Abou Ahmed al-Koweïti, identifié comme son principal relais. Ensuite, ce sont les moyens techniques qui ont pris le relais, notamment grâce à une analyse des communications (SIGINT) et grâce aux

imageries satellite (IMINT) : les drones ont fourni des vues détaillées du complexe, mettant en évidence des habitudes de vie du principal suspect. Enfin, le renseignement géospatial (GEOINT) a permis de cartographier les déplacements des messagers et de cerner la structure du site, permettant à l'opération des Navy SEALs, d'être menée sur la base de cette intelligence hybride.

Loin d'être une dualité, la relation entre renseignement humain et technique est une dialectique productive.

C.L.

⁹ GRAY, Colin S. « Irregular Warfare: One Nature, Many Characters », *Strategic Studies Quarterly*, Winter 2007, p.49.

The background features a complex, abstract geometric pattern of thin, light gray lines forming various polygons and shapes. A thin red border frames the entire page.

Dossier Spécial

Etudes de cas des services de renseignements nationaux

Les services de renseignement français : compétition ou synergie ?

Auteur : Romane Chatel, Mastérante en Relations Internationales, Sécurité et Défense.

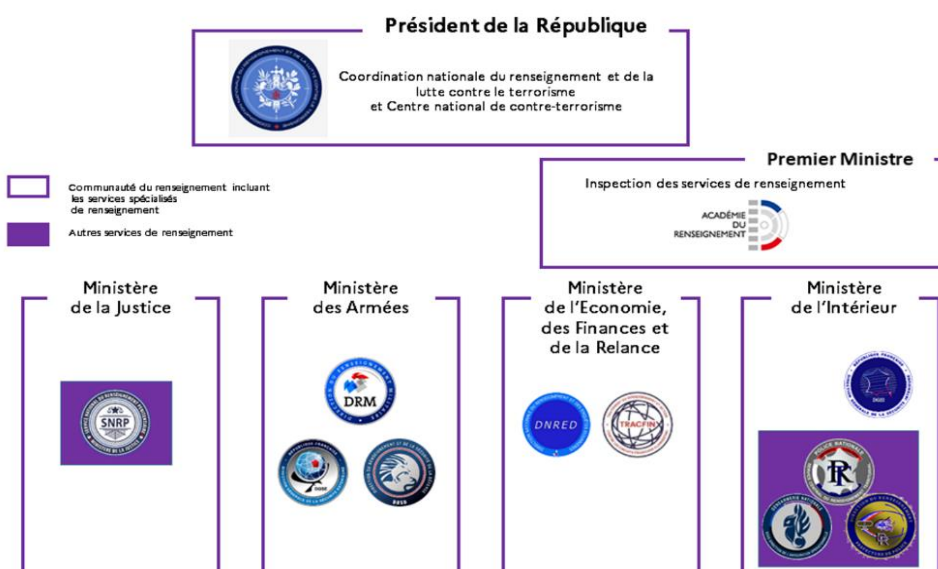
En 2008, le Livre Blanc sur la défense et la sécurité nationale a introduit la notion de communauté française du renseignement. Officialisée dans un décret du 12 mai 2014, modifié en 2017, ce terme rassemble six services spécialisés : la DGSE, DGSI, DRM, DRSD, DNRED, et TRACFIN¹, qui sont complétées par la Coordination Nationale du Renseignement et de la Lutte contre le Terrorisme, l'Académie du renseignement, et l'Inspection des services de renseignement. Il incombe à ses services une mission commune : rechercher, collecter et exploiter « des renseignements relatifs aux enjeux géopolitiques et stratégiques ainsi qu'aux menaces et risques susceptibles d'affecter la

vie de la Nation »². Il existe aussi des services dits du second cercle, dont le

renseignement n'est qu'une partie des activités (police, gendarmerie, préfecture, administration pénitentiaire). Chacun des services spécialisés détient une mission et une direction propres, mais, sous un cadre juridique commun, ils témoignent de la volonté d'une culture nationale de renseignement.

L'organisation des services de renseignement découle d'un enjeu majeur et de plus en plus imminent pour les États. En effet, le contexte international, le bouleversement des équilibres mondiaux, ainsi que la diversification des menaces, placent le renseignement face à des défis croissants. La révolution numérique et les

La communauté française des services du renseignement



Source : [MINISTÈRE DES ARMÉES. Direction du Renseignement Militaire. Nos partenaires.](#)

¹ Direction générale de la sécurité extérieure, Direction générale de la sécurité intérieure, Direction du renseignement militaire, Direction du renseignement et de la sécurité de la défense, Direction nationale du renseignement et des enquêtes douanières, et le service de

« Traitement du renseignement et action contre les circuits financiers clandestins »

² CNCTR. Les principaux services de renseignement. <https://www.cnctr.fr/services-de-renseignement>

problématiques propres à la cybersécurité prennent un rôle grandissant dans la conduite et les normes de relations internationales, ainsi, le renseignement est un milieu qui se doit d'être performant. La maîtrise de l'information est aujourd'hui plus que jamais un pouvoir, que ce soit dans une démarche défensive ou active, et pour ce faire, les États doivent s'adapter rapidement aux menaces modernes.

Dans ce contexte, la France a opté pour la recherche d'un équilibre entre spécialisation et coordination entre ces services. Selon la Direction du Renseignement Militaire (DRM), la communauté française de renseignement « permet un meilleur partage des savoir-faire et des informations, dans le respect du périmètre de responsabilités dévolu à chaque service »³. Mais justement, comment comprendre ce périmètre et comment s'y limiter dans un contexte où la sécurité est une notion de plus en plus globale, et où les enjeux se mêlent, voire se contredisent ? Peut-on parler d'une compétition entre ces services de renseignement, ce qui impliquerait de penser un jeu à somme nulle, ou est-il possible au contraire de tendre vers une synergie assez efficace pour un renseignement national cohérent ?

La spécialisation des services de la communauté du renseignement français

Juridiquement, les différents services spécialisés disposent d'autorisations communes quant aux techniques de renseignement, et surtout ils

sont soumis à une liste commune d'intérêts fondamentaux de la Nation pour lesquels ils ont le droit d'exercer leurs missions respectives (intégrité territoriale, intérêts économiques, intérêts majeurs de la politique étrangère...⁴). En partant de ces objectifs larges, la distinction entre chaque service tient alors surtout à une répartition par domaines d'enjeux sécuritaires. Pour résumer la spécialisation de chaque service, la DGSE s'intéresse au renseignement et aux opérations qui sont extérieures au territoire français, alors qu'à l'inverse la DGSIS lutte contre les menaces depuis l'intérieur. La DRM et la DRSD sont davantage tournées vers le domaine militaire, la première en s'occupant du renseignement d'intérêt militaire pouvant soutenir les opérations des forces armées, la deuxième en assurant la sécurité du personnel et des infrastructures de défense. Enfin, les deux derniers services se focalisent sur le plan économique, soit le financement du terrorisme par des circuits financiers illicites (TRACFIN) ainsi que la lutte contre les trafics douaniers (DNRED).

Si la répartition des spécialités semble donc assez claire, on observe en réalité que les missions sont proches et se croisent. Par exemple, la DGSIS présente sur son site internet trois missions principales que sont la lutte anti-terroriste, le contre-espionnage, et la cyberdéfense. Or, le site de la DGSE présente les trois mêmes catégories, d'autant plus que la lutte contre le terrorisme est aussi une des missions principales de TRACFIN.

Alors, ce qui permet de les distinguer, c'est la direction hiérarchique de chacun des services. Tandis que la DGSIS

³ MINISTÈRE DES ARMÉES. Direction du Renseignement Militaire. Nos partenaires. <https://www.defense.gouv.fr/drm/direction-du-renseignement-militaire/nos-partenaires>

⁴ D'après l'article L811-3 du Code de la Sécurité Intérieure, Livre VIII « Du renseignement ». Légifrance.

relève du ministère de l'Intérieur, la DGSE relève, elle, du ministère des Armées, et TRACFIN est un service rattaché au Ministère de l'Économie et des Finances. De même, alors que la Direction du Renseignement Militaire est aussi placée sous le Ministère des Armées, elle relève plus précisément de l'État-Major des Armées, et c'est ce qui vient la différencier de la DGSE. En effet, ce qu'on appelle le renseignement d'intérêt militaire concerne les informations nécessaires à la planification et la conduite des opérations au sens stratégique et tactique. À ce propos, en 2021 Jean Pierre Bat, historien et chercheur au CNRS, écrivait dans la Revue Défense Nationale que « les réformes du renseignement militaire de 1992 complètent les virages engagés par la DGSE en singularisant mieux ce qui relève du militaire et l'opérationnel tactique, de ce qui relève de la géopolitique et du politique »⁵. Ainsi, la répartition en services semble traduire une volonté de distinguer le domaine civil et le domaine militaire, et le domaine tactique du domaine politique. C'est pour cela que sur le site de la DGSE figure deux autres catégories de missions qu'on ne retrouve pas chez la DGSI : la géopolitique et la contre-prolifération.

Une communauté à six services, atout ou frein à l'efficacité ?

Même en partant du postulat que la répartition des missions entre les services soit théoriquement claire, une communauté

divisée en six services fait évidemment face à plusieurs complexités pratiques.

D'abord, bien que la poursuite d'objectifs communs permette de maintenir une cohérence dans la stratégie du renseignement français, on peut imaginer qu'elle amène les services à se chevaucher dans de nombreux domaines communs, comme la lutte contre le terrorisme. Le risque de cette similarité entre certains objectifs et domaines sécuritaires peut être la redondance des informations, menant à une perte d'efficacité, ou à l'inverse à la perte d'une information qui se noierait entre les fines frontières des services. Cette question n'est pas récente, en 1997, l'Institut national des hautes études de la sécurité et de la justice publiait un de ses Cahiers de la sécurité pour discuter de la coordination du renseignement français et des cultures d'institutions⁶. Dans ce dossier, Michel Dobry propose d'adapter la théorie d'Harold Wilenski⁷ au sens où le renseignement serait un milieu confronté aux défaillances et aux hiérarchies bureaucratiques⁸. Ces éléments entraîneraient alors des rivalités organisationnelles ainsi que des doctrines de renseignement et des cultures locales différentes entre les services. La compétition bureaucratique est un élément important en sociologie des organisations à cause des potentiels effets néfastes du jeu des négociations intra-gouvernementales où les différentes unités peuvent se placer dans une dynamique de concurrence, notamment pour des questions d'arbitrage budgétaire vis-à-vis des décideurs politiques.

⁵ Bat, J. (2021). Réformer le renseignement militaire français après la guerre du Golfe : un enjeu politique. Revue Défense Nationale, N° 843(8), 78-84. <https://doi.org/10.3917/rdna.843.0078>

⁶ Institut des hautes études de la sécurité intérieure. (1997). Les Cahiers de la sécurité intérieure, n°30 : Le renseignement. https://www.vie-publique.fr/files/collection_number/portrait/photo/3000000000043.pdf

⁷ Wilenski, H (1967). Organizational Intelligence. Knowledge and Policy in Government and Industry, New York, Basic Books.

⁸ Dobry, M. (1997). Le renseignement dans les démocraties occidentales. Les Cahiers de la sécurité intérieure, n°30 : Le renseignement. pages 53 à 85. https://www.vie-publique.fr/files/collection_number/portrait/photo/3000000000043.pdf

Pour faire face à ces défis, des solutions sont recherchées et des réformes sont mises en place pour assurer une organisation efficace. Dans ce même dossier (Cahiers de la sécurité, INHESJ), Isabelle Renouard, Secrétaire générale de la défense nationale à l'époque, présentait le Comité interministériel du renseignement comme responsable d'une « synergie entre les acteurs du monde du renseignement »⁹. Depuis, plusieurs autres mécanismes ont été créés pour consolider la communauté du renseignement français comme le plan national d'orientation du renseignement de 2015 qui vient fixer les sujets prioritaires d'intervention des services, ou encore la création du poste de coordonnateur national du renseignement en 2008. Ces initiatives ont pour objectif de faciliter les rapports entre ces agences nationales. Ces interactions sont fondamentales, comme le souligne Bruno Elie, directeur du renseignement militaire dans les années 1990 lorsqu'il explique que la DRM coopère avec la DGSE afin de « compléter leurs informations », et qu'inversement la DRM a besoin des services du Ministère de l'Intérieur pour assurer sa sécurité en matière de contre-espionnage¹⁰.

Ainsi, la communauté de renseignement française est organisée de sorte à se compléter, dans un partage mutuel de compétences, et ce pour répondre efficacement aux orientations générales qui doivent guider les acteurs. C'est pour cela

qu'on peut parler d'une volonté de consolider une culture nationale du renseignement français avec des normes, des règles et des pratiques communes qui serait cruciale pour que l'organisation en communauté reste un atout pour la sécurité française¹¹.

Le Coordonnateur national du renseignement et de la lutte contre le terrorisme (CNRLT), ou la nécessité d'un « chef d'orchestre »¹²

Créée en 2008, la coordination nationale du renseignement a pris depuis 2017 la forme du CNRLT, une structure ayant pour but d'assurer la coordination des services de renseignement dans leur activité générale et de piloter l'ensemble des services contribuant à la lutte anti-terroriste. En effet, depuis les années 2010, la lutte contre le terrorisme est l'une des missions centrales des services de renseignement français. La communauté du renseignement français se rapproche ainsi davantage, sous le prisme de cet objectif commun, afin d'assurer leur bonne coopération.



[ACADÉMIE DU RENSEIGNEMENT](#). La communauté du renseignement. La CNRLT. 2024

⁹ Renouard, I (1997). La coordination du renseignement en France. Les Cahiers de la sécurité intérieure, n°30 : Le renseignement. pages 53 à 85. https://www.vie-publique.fr/files/collection_number/portrait/photo/300000000043.pdf

¹⁰ Institut des hautes études de la sécurité intérieure. (1997). Les Cahiers de la sécurité intérieure, n°30 : Le renseignement. https://www.vie-publique.fr/files/collection_number/portrait/photo/300000000043.pdf

¹¹ Munier, M. (2022). Au cœur de la raison d'État : la culture nationale du renseignement français au prisme de la DGSE et de la DGSI. Annuaire français de relations internationales 2022. (p. 491 -506). Éditions Panthéon-Assas. <https://doi.org/10.3917/epas.ferna.2022.01.0491>

¹² Sciences Po/PSIA, . (2022). Rendre compte du renseignement : les services français peuvent-ils faire mieux ? Revue Défense Nationale, N° 849(4), 103-108. <https://doi.org/10.3917/rdna.849.0103>

Le CNRLT s'assure que les divers services travaillent de manière cohérente en préparant notamment le plan national d'orientation du renseignement qui s'adresse à tous les services de la communauté du renseignement. Il fait aussi le lien avec le Président de la République et d'autres instances comme le Conseil National du Renseignement ou la Commission nationale de contrôle des techniques de renseignement. Ainsi, en 2022 on peut lire dans la Revue Défense Nationale que le CNRLT joue un véritable rôle de « chef d'orchestre des services de renseignement nationaux »¹³. C'est aussi ce coordinateur qui représente la communauté du renseignement français à l'international et développe les initiatives prises par la France en matière de coopération. Cela soulève un autre enjeu important dans l'organisation entre les services français : les interactions avec les autres acteurs de la scène internationale et européenne doivent impérativement être cohérentes.

Avec le CNRLT, la France cherche donc à créer cette synergie nécessaire au bon fonctionnement du renseignement et de toutes les répercussions majeures que ce domaine peut avoir sur la sécurité nationale ainsi que dans les relations internationales. Pour autant, au-delà des complexités pratiques que l'on peut imaginer, la diversité des moyens de renseignement en France démontre avant tout une conception large de la notion de sécurité nationale, ainsi qu'une capacité à déléguer des responsabilités à des acteurs spécialisés. À titre comparatif, d'autres pays comme la Russie et la Chine semblent favoriser des structures plus centralisées avec moins de répartition des rôles, ce qui démontre une culture stratégique différente de celle de la France.

R.C.

¹³ Sciences Po/PSIA, . (2022) . Rendre compte du renseignement : les services français peuvent-ils faire

mieux ? Revue Défense Nationale, N° 849(4), 103-108.
<https://doi.org/10.3917/rdna.849.0103>

Les services de renseignement chinois, un réseau tentaculaire dangereux

Auteur : Hugo Exposito, Mastérand en Francophonie, Stratégie et Relations Internationales.

« Ayez des espions partout, soyez instruit de tout, ne négligez rien de ce que vous pourrez apprendre »¹

- Sun Tzu, *L'art de la guerre*, Chapitre XIII

Tout État, qu'il soit autoritaire ou non, dispose d'un service de renseignement plus ou moins développé. À vrai dire, dans un monde anarchique où les intérêts nationaux prévalent, il convient pour chaque État de se doter d'un appareil de renseignement efficace.

Si les services de renseignement russes et états-uniens ont particulièrement été mis sur le devant de la scène lors de la Guerre froide, les services de renseignement chinois, bien que moins connus, n'en restent pas moins puissants. Christopher Wray, directeur du *Federal Bureau of Investigation* (FBI) de 2017 à 2025 soulignait d'ailleurs que « le programme de piratages informatiques de la Chine est plus important que celui de tous les autres grands pays réunis »¹.

Mais quels sont les éléments qui différencient l'espionnage chinois des autres méthodes employées par les États ? Comme le soulignait le *Wall Street Journal*, « nous sommes face à un espionnage d'État »²; l'État chinois étant la représentation morale du Parti communiste chinois (PCC), l'espionnage est ici plus amplement au service d'un parti politique,

et d'idéaux particuliers. Il permet à l'État de conserver sa position sur la scène internationale, notamment par la répression de dissidents ou la collecte d'informations étrangères. Plus largement, les systèmes de renseignement chinois « ne sont pas simplement un organe de connaissance voire d'influence et d'action limitée, comme dans les pays démocratiques. Ils constituent un pilier essentiel du pouvoir aux côtés de l'armée et du parti unique »³.

Il est important de rappeler que, quelques décennies auparavant, la Chine était fortement en retard sur le plan technologique et économique. Ce n'est qu'en 1978, avec l'arrivée au pouvoir de Deng Xiaoping que le pays va s'ouvrir à l'international jusqu'à se convertir en la « première économie socialiste de marché ». L'année de son investiture, le président émérite de la République populaire de Chine (RPC) lance le projet des « Quatre modernisations », visant à rattraper le retard sur la scène internationale. Les services de renseignement jouent alors un rôle fondamental dans cette course à la technologie.

Alors que la Chine est aujourd'hui la

¹ Sun Tzu, *L'art de la guerre*, Chapitre 13, De la manière d'employer les dissensions et de mettre la discorde

¹ Untersinger Martin, Les hackers chinois ont des méthodes plus sophistiquées, discrètes et agressives que jamais, *Le Monde*, Cyberespionnage, 2025

² LCI, L'occident face au tentaculaire espionnage chinois, 2024

³ Roger Faligot, Les services secrets chinois De Mao à Xi Jinping, Nouveau Monde éditions, 2015, Paris, p. 637

deuxième puissance économique mondiale, Pékin poursuit sa politique de renseignement au niveau international. L'espionnage chinois prolifère dans l'espace international, si bien que « les gouvernements occidentaux en sont souvent réduits à composer avec les événements et souvent, après qu'ils se soient produits⁴ ». En somme, le système d'information est devenu bien plus qu'un moyen de répondre aux intérêts vitaux de l'État-Nation. Il est en réalité un nouveau canal de contrôle et de déstabilisation internationaux.

L'organisation du service de renseignement chinois, un réseau tentaculaire

L'organisation du système d'information chinois est à l'image d'une toile d'araignée aux fils d'acier. La Chine déploie des moyens que peu d'États sont capables de mobiliser. Civils, gouvernement, entreprises privées et armées s'entremêlent dans cette chasse à l'information. La bureaucratie chinoise du renseignement se divise en différents ministères et organismes. On compte parmi eux le Ministère de la sécurité d'État (MSE), le Ministère de la sécurité publique (MSP) et certaines divisions de l'Armée populaire de libération (APL).

Le MSE, ou *guoanbu*, traite des

affaires externes du pays. Il fonctionne par le biais de différents départements touchant tant aux opérations qu'à la gestion. On retrouve, parmi dix-huit bureaux, des missions telles que le contre-espionnage offensif, la surveillance du territoire ou encore le renseignement international⁵.

Le MSP, ou *gunganbu*, a pour but, à en lire sa deuxième mission officielle, de lutter contre « toutes les situations qui peuvent déstabiliser la sécurité nationale et l'ordre public⁶ ». On y retrouve le bureau de supervision du réseau internet, chargé de contrôler les activités des citoyens; ou encore du bureau 610⁷, chargé de réprimer le mouvement Falun Gong⁸. Par ailleurs, le MSP dispose d'un ancrage territorial dans chacune des provinces de l'État.

Enfin, l'APL, après une réforme en 2016⁹, se divise en deux entités centrales : la Force de soutien stratégique, et le bureau de renseignement. Respectivement, ces bureaux sont spécialisés dans la cyberdéfense et le renseignement humain¹⁰.

Depuis 2012, et les nombreuses réformes instaurées par Xi Jinping, les services de renseignement chinois sont enclins à des mouvements de centralisation, confiant la majorité de la prise de décision au chef du parti. Pour autant, bien que la Chine se considère, de par sa Constitution,

⁴ Calder Walton, auteur, expert en sécurité internationale, au sujet de l'espionnage chinois dans les États occidentaux

⁵ Damon, F.Y, Les services de renseignement de la République populaire de Chine. Deuxième partie : Le ministère de la sécurité d'État (Guojia Anquanbu), CF2R, Bulletin de documentation n°11, 2014

⁶ Puig Emmanuel, L'influence politique du Ministère de la sécurité publique en Chine : acteurs et dynamiques contemporaines, Asia Centre, Délégation aux affaires stratégiques, Observatoire Chine 2011/2012, 2012

⁷ Jamet, Gabriel, Les services de renseignement et de sécurité en République populaire de Chine : un instrument

essentiel de survie et d'hégémonie, programme Asie, IRIS, Janvier 2019

⁸ Mouvement spirituel né en 1992, ayant pour objectif le travail sur soi au travers de trois piliers fondamentaux (authenticité, bonté, tolérance).

⁹ Genevaz, Juliette La réforme de l'Armée populaire de libération, au cœur de la rénovation de l'État chinois, Note de recherche stratégique n°29, Août 2016

¹⁰Damon, F.Y, Les services de renseignement de la République populaire de Chine. Troisième partie : Le renseignement militaire, CF2R, Bulletin de documentation n°15, 2015

comme un Etat unitaire; la pratique démontre un éclatement de la prise de décision, marqué par un pouvoir accru des différentes provinces.

La diaspora chinoise comme vecteur de renseignement et de diffusion de discours

La Chine utilise ses nationaux à l'étranger comme méthode de renseignement privilégié. La loi sur le renseignement de 2017 encourage « tous les citoyens et toutes les organisations » à « soutenir et assister » les autorités centrales et à « signaler rapidement » tout comportement suspect. En outre, cette loi fait du renseignement l'affaire de tous, et oblige chaque citoyen à coopérer avec les autorités communistes dans cette chasse à l'information. Néanmoins, comme le soulignait le cabinet d'avocats néerlandais De Brauw Blackstone Westbroek, cette loi « peut potentiellement entrer en conflit avec les deux textes législatifs de l'UE, laissant les opérateurs économiques entre le marteau et l'enclume »¹¹.

Cette loi est d'autant plus préoccupante en raison de la forte diaspora chinoise autour du monde, et notamment en France. Antoine Izambard, grand reporter au service international du magazine *Challenge*, soulignait par ailleurs le taux important de mariages entre les officiers de la marine de Brest et les femmes chinoises. Pouvons-nous considérer ces amours comme vraies, ou sont-elles de simples simulacres dissimulant un espionnage gouvernemental ? Certes, on ne pourrait assener à chacun des

mariages franco-chinois le spectre du doute, pour autant, un sentiment d'incertitude et de méfiance peut s'installer, si bien que chacun de nous pourrait être un espion inaperçu¹².

Cette chasse à l'information passe notamment par une autre institution notable : le département du front uni, lequel fut « salué par Mao comme la clé du triomphe du Parti communiste dans la guerre civile chinoise qui a duré plusieurs décennies. »¹³ Le front uni est une stratégie mise en place par le PCC qui, entre autres, vise à étendre son réseau d'influence par le biais de l'élite nationale et la diaspora; si bien que, pour reprendre les mots de Ho-fung Hung « les gouvernements occidentaux doivent désormais se montrer moins naïfs à l'égard des activités du Front uni chinois et les considérer comme une menace sérieuse. »¹⁴

Simon Menet, chargé de recherche à la Fondation pour la Recherche Stratégique, soulignait par ailleurs la présence de bureaux de polices chinois autour du monde comme moyens de contrôle de la diaspora chinoise¹⁵. En somme, ces derniers tendent à servir les intérêts du PCC à l'étranger, contrôler l'opinion publique mais également surveiller les nationaux dans leur mission de renseignement.

Par ailleurs, le PCC renforce son influence en s'appuyant sur les élites nationales étrangères. Il utilise fréquemment le triptyque « argent, amour et idéologie » pour servir ses intérêts; stratégie ayant récemment touché l'Europe, et plus particulièrement la Belgique.

¹¹ Liboreiro, Jorge, Pourquoi la loi chinoise contre l'espionnage inquiète l'UE ?, Euronews, Europe, L'Europe décodée, 2013

¹² En référence à Jean Baudrillard, « chacun de nous est un criminel inaperçu », quant au sentiment de méfiance dans la société face aux risques de terrorisme.

¹³ Koh Ewe et Laura Bicker, Front uni : L'« arme magique » de la Chine au cœur d'une controverse sur l'espionnage, BBC News, Reporting from Singapore et Beijing, 2024

¹⁴ Koh Ewe et Laura Bicker, op.cit

¹⁵ France culture, Épisode 2/4 : Chine : les réseaux tentaculaires de l'espionnage, Les maîtres du renseignement, Culture Monde, 2024

Dans une enquête conjointe du *Financial Times*, de *Der Spiegel* et du *Monde*, publiée le 15 décembre 2023, un cas historique de corruption au sein du Parlement bruxellois a été dévoilé. L'affaire concerne Frank Creyelman, ex-député du parti d'extrême droite *Vlaams Belang*, qui travaillait secrètement pour les renseignements chinois. Rémunéré en crypto monnaies, il servait les intérêts de Pékin, non seulement par appât du gain, mais aussi par idéologie, son parti étant favorable à la position chinoise. Il exécutait des missions confiées par Daniel Wo, agent du MSE, lequel cherchait à obtenir des informations sensibles sur les institutions européennes et à diffuser des éléments de langage favorables à la Chine. Face à ces révélations, l'ambassade de Chine en Belgique a qualifié l'enquête de « fabrication », affirmant que Pékin suit un principe de non-ingérence dans les affaires étrangères.

L'organisation tentaculaire du renseignement chinois illustre la place centrale qu'occupe l'information dans la stratégie de puissance de Pékin. Plus qu'un simple outil de défense des intérêts nationaux, il est un instrument fondamental de contrôle politique, d'influence internationale et de projection de pouvoir. En combinant espionnage d'État, cyber-opérations, mobilisation de la diaspora et infiltration des élites étrangères, le Parti communiste chinois dépasse le cadre traditionnel des services de renseignement pour imposer une véritable guerre de

l'information. Plus encore, la Chine ne se limite pas aux méthodes précitées, mais déploie un arsenal sans précédent dans sa mission d'espionnage. Des entreprises comme I-Soon viennent en aide au gouvernement dans la recherche de renseignement. Cette entreprise, spécialisée dans la cybersécurité et le renseignement, se revendique elle-même comme « une force robuste pour la défense nationale », servant les intérêts du gouvernement¹⁶. Paul Charon, directeur du domaine Influence et Renseignement de l'IRSEM, soulignait d'ailleurs que cette entreprise « travaille surtout pour le ministère de la Sécurité d'État et le ministère de la Sécurité publique, donc pour les services de renseignement chinois ». Par ailleurs, il aurait été révélé, suite à une fuite de données en février 2024, qu'I-Soon avait infiltré les systèmes de plus d'une douzaine de gouvernements, d'organisations pro-démocratie à Hong Kong, ainsi que de l'OTAN¹⁷

Face à cette approche globalisée, les démocraties occidentales semblent souvent réagir après coup, contraintes de composer avec une menace diffuse et difficile à contenir. Cette asymétrie interroge : comment préserver les principes démocratiques sans devenir vulnérable face aux rapports de force redéfinis par des méthodes comme l'ingérence et la manipulation ? Plus que jamais, la maîtrise de l'information apparaît comme un levier essentiel dans la recomposition de l'ordre mondial.

H.E.

¹⁶ NewsRoom, Le catalogue et les activités d'un prestataire cyber privé du renseignement chinois révélés par la fuite de données I-Soon, HarfangLab, 2024

¹⁷ Un prestataire chinois a piraté des gouvernements, selon une fuite de données, selon des analystes, Nice-Matin, 2024

Les Etats-Unis et l'éthique du renseignement

Auteur : Hugo Swatridge, Mastéran en Relations Internationales, Sécurité et Défense.

La *Central Intelligence Agency* (CIA) est fondée en 1947 suite au *National Security Act*. Cette agence de renseignement américaine fournit et analyse les données sur les Etats, les entreprises et les individus du monde entier. Elle conduit aussi des opérations clandestines à l'étranger pour le compte de Washington⁵⁵. Entre déstabilisations de gouvernements, méthodes de tortures contestables, trafic de drogues et propagande intense, la CIA n'a pas toujours priorisé l'éthique concernant la nature de ces missions ou sa façon de les exécuter. Cette absence de moralité sera approfondie dans cet article.

La torture et les « sites noirs » de la CIA

En 2005, *The Washington Post* révèle la présence de prisons clandestines contrôlées par la CIA avec pour principal objectif, depuis le 11 septembre 2001, la détention et la torture des personnes suspectées de terrorisme⁵⁶. Ces dernières portent aussi le nom de sites noirs. Pour faire confesser les détenus, une multitude de pratiques sont utilisées dans un « *Enhanced interrogation program*⁵⁷ ». Ce projet présente une double violation du droit international, dans l'absence de jugement entraînant la détention et dans les pratiques de torture. Le site noir le plus

symbolique est la prison militaire de Guantanamo. Joseph R. Biden Jr., sénateur démocrate, assure que ce site « *est devenu le meilleur outil de propagande qui existe pour recruter des terroristes dans le monde*⁵⁸ », et ce au vu de l'atrocité des techniques utilisées. Le *Detention and Interrogation Program* permet l'existence d'un vaste réseau de prisons clandestines, toutes sous le contrôle de la CIA. Les méthodes de torture appliquées aux détenus varient, mais un point commun subsiste : la cruauté. Les supplices sont à la fois physiques et psychologiques⁵⁹. De la privation de sommeil à l'aspersion d'essence (ou eau dans le meilleur des cas), tout est fait pour que le prisonnier subisse des conditions de (sur)vie inhumaines⁶⁰. Pour ne pas que lui incombe l'entièreté de la responsabilité, la CIA a pu collaborer avec différentes puissances⁶¹. Les Etats concernés comprenaient par exemple le Maroc, la Lituanie, la Roumanie ou encore la Thaïlande⁶². La liste est complexe à dresser puisque la majorité des collaborations étatiques se sont effectuées dans le secret. Concernant ces pratiques, l'absence d'éthique est frappante, tout comme la relative impunité présente. Cette impunité s'explique entre autres par la phrase suivante de John Stockwell, ancien officier de la CIA, : «

⁵⁵ KIRIAKOU John, *The CIA Is an Ethics-Free Zone*, Institute for Policy Studies, consulté le 8 mars 2025, <https://ips-dc.org/the-cia-is-an-ethics-free-zone/>

⁵⁶ CHIESA Giulietto, *L'archipel des prisons secrètes de la CIA*, *Le Monde Diplomatique*, consulté le 8 mars 2025, <https://www.monde-diplomatique.fr/2006/08/CHIESA/13832>

⁵⁷ Seton Hall Law, *How America Tortures*, SSRN, consulté le 8 mars 2025,

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3494533

⁵⁸ Chiesa, op.cit.

⁵⁹ Seton Hall Law, op.cit.

⁶⁰ Ibid.

⁶¹ Ibid.

⁶² Ibid.

*Enemies are necessary for the wheels of the U.S. military machine to turn*⁶³ ». Pourquoi punir alors que les Etats-Unis ont en partie besoin de ces « ennemis » pour faire fonctionner un pan conséquent de leur économie nationale ? Depuis la reconnaissance officielle du *Detention and Interrogation Program* en 2006, de nombreuses associations militent, en vain, pour la fermeture des « sites noirs » et l'arrêt de la torture par les agences de renseignement étatiques.

La « guerilla warfare »

La « guerilla warfare » est une forme de guerre politique. C'est pourquoi ces zones d'opérations dépassent les limites territoriales de la guerre conventionnelle pour s'étendre et pénétrer la créature politique par excellence : « l'animal politique », défini par Aristote⁶⁴. Dans cette forme de conflit, l'être humain devient la priorité et la propagande ainsi que la manipulation sont les moyens principaux. L'essence de l'Homme est son esprit. Une fois que l'esprit a été atteint, « l'animal politique » a été vaincu, sans nécessairement avoir reçu des coups de feu⁶⁵. Pour manipuler ou effectuer une propagande efficace, la CIA a recours à des opérations psychologiques dit *PsyOps*, devenu en 2010 des *Military Information*

*Support Operations*⁶⁶. Ces actions sont immorales puisqu'elles entraînent des manipulations de la vérité, des atteintes aux droits humains, de la désinformation volontaire, le tout dans le but d'influencer une certaine population. *Mockingbird* est l'une des opérations les plus emblématiques de la CIA. C'était un programme débutant dans les années 1950 et se poursuivant jusque dans les années 1970. L'agence américaine, durant cette période, a recruté des journalistes de plusieurs grandes structures d'informations pour promouvoir les objectifs américains. Le programme a eu un impact majeur sur l'opinion publique pendant la guerre froide, il a notamment contribué à façonner la manière dont les Américains percevaient le communisme et l'Union soviétique à l'époque⁶⁷.

Hormis la propagande, la CIA a tenté des programmes ayant eu pour objectif de contrôler l'esprit d'individus. Ces expérimentations se focalisaient sur le développement de drogues, tel que le LSD, pouvant être utilisées pour affaiblir les victimes et forcer l'aveu par le lavage de cerveau ou la torture psychologique⁶⁸. Le projet *MKUltra* était l'un des plus renommés mais la plupart de ses dossiers ont été détruits en 1973⁶⁹, rendant difficile la compréhension complète du programme. *MKUltra* était précédé par le

⁶³ National Security Council, *Secret Wars of the CIA*, consulté le 7 mars 2025, https://www.youtube.com/watch?v=bmYZ_kWHk3Q

⁶⁴ CIA, *PSYCHOLOGICAL OPERATIONS IN GUERRILLA WARFARE*, consulté le 7 mars 2025, <https://www.cia.gov/readingroom/docs/CIA-RDP86M00886R001300010029-9.pdf>

⁶⁵ *Ibid.*

⁶⁶ CIA, *INTELLIGENCE SUPPORT FOR PSYCHOLOGICAL OPERATIONS*, consulté le 7 mars 2025, <https://www.cia.gov/readingroom/document/cia-rdp80r01731r003500180010-8>

⁶⁷ NSA Archives, *CIA Behavior Control Experiments*, consulté le 7 mars 2025,

<https://nsarchive.gwu.edu/briefing-book/dnsa-intelligence/2024-12-23/cia-behavior-control-experiments-focus-new-scholarly>

⁶⁸ NSA Archives, *CIA Behavior Control Experiments*, consulté le 7 mars 2025, <https://nsarchive.gwu.edu/briefing-book/dnsa-intelligence/2024-12-23/cia-behavior-control-experiments-focus-new-scholarly>

⁶⁹ Harvard Kennedy School, Carr Center, *Mind Control : Past and Future*, consulté le 7 mars 2025, <https://www.hks.harvard.edu/centers/carr/publications/min-d-control-past-and-future>

Project Artichoke. D'autres programmes ont pu s'attarder sur diverses méthodes de manipulation comme les électrochocs, l'hypnose, la privation sensorielle, l'isolement et dans certains cas extrêmes l'abus sexuel⁷⁰. Des projets comme *MKNaomi* se sont focalisés sur la recherche en matière de guerre biologique⁷¹. Ces programmes ont été largement condamné comme une violation des droits humains et un exemple d'abus de pouvoir de la CIA.

Les déstabilisations et renversements de gouvernements

Le 15 septembre 1970, Richard Nixon et son conseiller à la sécurité Henry Kissinger autorisèrent les services de renseignement américains à renverser le gouvernement socialiste de Salvador Allende au Chili. L'objectif était de faire « hurler l'économie » (« make the economy scream⁷²») sans prendre en compte les risques encourus. Suite à cela, la CIA lança le projet FUBELT. Ce projet faisait partie d'une vision plus large des Etats-Unis : la suppression des dictatures militaires en Amérique Latine avec l'Opération Condor. Les campagnes d'assassinats et de déstabilisations furent conduites conjointement par les services secrets de différents Etats, entre autres, l'Argentine, la Bolivie, le Brésil et le

Paraguay avec un accord tacite des U.S. La terreur d'Etat visait les « guérilléros » au nom de la doctrine de sécurité nationale. Divers procédés étaient employés notamment les « vols de la mort » au-dessus de différentes chaînes de montagnes ou la noyade. D'après une étude de l'université d'Oxford au moins 805 cas de violations transnationales des droits de l'homme résultant de l'opération *Condor* sont identifiés, dont 382 cas de détentions illégales et de tortures et 367 meurtres et disparitions⁷³.

L'Amérique Latine n'est pas la seule zone impliquée par ces déstabilisations, il y a aussi le Moyen-Orient. L'Opération AJAX par exemple, est une preuve de la volonté de l'agence américaine pour un coup d'état en Iran en 1953 pour renverser Mossadegh⁷⁴. Cette opération a impliqué de la propagande, l'achat de loyauté parmi les dirigeants militaires et politiques iraniens, ainsi que le soutien de manifestations de rue, à travers une aide monétaire destinée à certains groupes⁷⁵. De nombreuses missions ont aussi eu lieu en Asie durant la guerre de Corée et du Vietnam. En 1958, la CIA lançait l'Opération HAIK, ayant eu pour objectif le soutien tacite à un coup d'état par les militaires indonésiens en fournissant aux rebelles des informations sur les leaders communistes⁷⁶.

⁷⁰ *Ibid.*

⁷¹ Commission Church - Sénat des États-Unis, *94e Congrès, 2de Session, Book I : Foreign and Military Intelligence*, Washington, U.S. Government.

⁷² ABRAMOVICI Pierre, « *Opération Condor* », *cauchemar de l'Amérique latine*, Le Monde diplomatique, consulté le 8 mars 2025, <https://www.monde-diplomatique.fr/2001/05/ABRAMOVICI/1729>

⁷³ LESSA Francesca, *Database on South America's Transnational Human Rights Violations*, Oxford University, consulté le 7 mars 2025,

<https://sites.google.com/view/operationcondorjustice/data-base>

⁷⁴ Beaulieu-Brossard Philippe, *Opération Ajax, 1953, Le mythe fondateur des tensions entre l'Iran et l'Amérique*, Chaire Raoul-Dandurand en études stratégiques et diplomatiques, consulté le 6 mars 2025, https://dandurand.uqam.ca/wp-content/uploads/2016/03/ERD19_Beaulieu-Brossard_091010.pdf

⁷⁵ *Ibid.*

⁷⁶ KENNEDY BLAKE Douglas, *OPERATION HAIK: THE EISENHOWER ADMINISTRATION AND THE CENTRAL INTELLIGENCE AGENCY IN INDONESIA*,

L'assistance est très souvent tacite de la part des Etats-Unis, leur permettant ainsi d'échapper aux risques d'escalade, de maintenir leurs alliances stratégiques et préserver leur influence sans entacher leur image. De nos jours les opérations de déstabilisations continuent, au Venezuela ou en Syrie par exemple, ou des ressortissants américains sont parfois détenus pour suspicion de complot visant à fragiliser le pouvoir⁷⁷. Ces renversements de gouvernements entraînent parfois des guerres civiles ou des dépressions économiques, qui *in fine* profitent aux Etats-Unis en renforçant leur influence et maintenant leur hégémonie sur la scène internationale.

Pour financer de telles opérations de renversements, la CIA a lourdement été accusé d'avoir facilité le trafic illicite d'armes et de drogues. Un exemple marquant de telles pratiques est l'affaire Iran-Contra (Irangate) dans laquelle des responsables américains ont soutenu un trafic d'armes vers l'Iran, pourtant sous embargo⁷⁸. La CIA a aussi, très probablement, facilité l'entrée aux Etats-Unis de cocaïne venant d'Amérique Latine en échange de fonds permettant le soutien de groupuscules rebelles locaux⁷⁹. Le trafic de drogues a, très probablement,

aussi eu lieu en Asie avec l'héroïne au Vietnam et durant la guerre civile du Laos à partir de 1962. Une partie des populations locales travaillaient et dépendaient des champs de coca ou de pavots à opium ce qui facilitait la circulation de ces substances.

L'absence d'éthique dans le numérique

En 1975, le *US Intelligence Church Committee* a publié une enquête dans laquelle est révélé que la CIA détenait des journaux, magazines et maisons d'édition influents à l'internationale⁸⁰. Avec ce réseau, l'agence de renseignement américaine a pu effectuer de la propagande en douce. Cette influence s'est accrue suite à l'arrivée d'internet, des médias et des données personnelles, avec comme pilier fondamental les GAFAM. La CIA s'appuie sur eux pour obtenir des *backdoors*, permettant un accès, voulu et caché, aux données de millions d'utilisateurs^{81,82}. Le programme *PRISM*, relevant de la NSA, est une illustration parfaite des liens existants entre ces géants du numérique et les agences américaines. Cette collaboration non-éthique continue d'être dénoncée de nos jours et a eu comme point de départ les révélations

B.S., United States Air Force Academy, 1989, consulté le 7 mars 2025, <https://apps.dtic.mil/sti/pdfs/ADA321861.pdf>

⁷⁷ AP News, *Three Americans among latest to be detained in Venezuela over alleged anti-government plot*, consulté le 7 mars 2025, <https://apnews.com/article/venezuela-arrests-americans-presidential-election-maduro-opposition-94bba826350cd20816e6902f5ae73e41>

⁷⁸ Brown University, *Understanding the Iran-Contra Affairs*, consulté le 7 mars 2025, https://www.brown.edu/Research/Understanding_the_Iran_Contra_Affair/iran-contra-affairs.php

⁷⁹ Department of Justice, *THE CIA-CONTRA-CRACK COCAINE CONTROVERSY: A REVIEW OF THE JUSTICE DEPARTMENT'S INVESTIGATIONS AND PROSECUTIONS*, consulté le 7 mars 2025,

<https://oig.justice.gov/sites/default/files/archive/special/9712/ch01p1.htm>

⁸⁰ United States Senate, *The Church Committee*, consulté le 7 mars 2025, <https://www.senate.gov/about/powers-procedures/investigations/church-committee.htm>

⁸¹ FONTANEL Jacques, *GAFAM, a progress and a danger for civilization*, St. Petersburg State University of Economics (UNECON), consulté le 6 mars 2025, <https://hal.univ-grenoble-alpes.fr/hal-02102188/document?utm>

⁸² WINDER Davey, *CIA Secretly Owned Global Encryption Provider; Built Backdoors, Spied On 100+ Foreign Governments: Report*, Forbes, consulté le 6 mars 2025, <https://www.forbes.com/sites/daveywinder/2020/02/12/cia-secretly-bought-global-encryption-provider-built-backdoors-spied-on-100-foreign-governments/>

d'Edward Snowden en juin 2013. En réponse, des actes juridiques sont pris, notamment le *USA FREEDOM Act* en 2015, qui permet de restreindre certaines pratiques de surveillance de masse, en particulier concernant la collecte des métadonnées des appels téléphoniques⁸³. Cependant le problème reste lui aussi juridique. En effet, les GAFAM peuvent être obligés de fournir aux agences américaines des données personnelles, y compris de citoyens non-américains, notamment en vertu de la loi *FISA (Foreign Intelligence Surveillance Act)* et sa section 702 qui permet aux agences de renseignement d'accéder à des données provenant de communications électroniques étrangères, souvent collectées via les entreprises de technologie américaines⁸⁴. Au vu de l'importance, croissante, des données personnelles, le contrôle, ou du moins une position favorable à l'exploitation de ces dernières, sont essentiels pour la survie de la CIA et des autres agences de renseignement américaines. Grâce, ou à cause, de toutes ces pratiques non-éthiques, la CIA a ses tentacules dans tous les aspects de la vie moderne.

Pourquoi le maintien d'une telle agence ?

D'un point de vue éthique la CIA est une très mauvaise élève et est même qualifié, par certains défenseurs des droits humains, d'organisation terroriste. Le souci est que du point de vue américain, la CIA est extrêmement efficace et permet aux U.S. de maintenir leur position ultra hégémonique sur la scène internationale en tentant de contrôler le plus possible. Les Etats-Unis

doivent faire en sorte que le plus de pays possible reposent sur eux et que toute alternative ou tentative d'alternative soit punie. La réalité est aussi la suivante : qui va les arrêter ? Que voulez-vous faire contre ces agences de renseignement ayant des fonds gigantesques, l'absence d'un code éthique et des moyens efficaces. Comme l'a dit John Stockwell, « The CIA, and other American agencies, have a licence to kill, but also to do a lot more.³¹ ».

L'essence du problème que pose ces agences se trouve dans cet extrait de la note de recherche d'un ancien agent de la CIA, John Kiriakou :

« Members of America's spy agency don't even learn the rules. They're in a foreign country, after all, and they likely have diplomatic immunity. They don't care about local laws. [...] They're pressured to « go do it » or suffer the consequences. But no one's able or willing to tell them the rules. That's what's wrong with the CIA today. And that's where the moral and ethical rebuilding of the organization should begin.³²».

H.S.

⁸³ House Judiciary Committee, *USA Freedom Act*, consulté le 6 mars 2025, <https://judiciary.house.gov/usa-freedom-act>

⁸⁴ INTEL.gov, *FISA Section 702*, consulté le 6 mars 2025, <https://www.intel.gov/foreign-intelligence-surveillance-act/1237-fisa-section-702>

L'alliance Five Eyes et la coopération internationale en matière de renseignement

Auteur : Ciara Mclaverty, Mastérante en Relations Internationales, Sécurité et Défense.

La nomination par Donald Trump le 12 février 2025 de Tulsi Gabbard au poste de directrice du renseignement national a suscité de vives inquiétudes au sein des agences de renseignement américaines ainsi que celles de leurs alliés des Five Eyes du fait des controverses dont elle fait l'objet, notamment par ses prises de position prorusses⁸⁵. Les « Five Eyes » désignent l'alliance de renseignement entre les services secrets des Etats-Unis, du Royaume-Uni, du Canada, de l'Australie et de la Nouvelle-Zélande. Ceux-ci collaborent et partagent du renseignement, notamment à travers une division du monde en zones géographiques. Plus précisément, le Royaume-Uni est responsable de surveiller l'Europe, le Moyen-Orient, l'Ouest de la Russie et Hong Kong. Les Etats-Unis de leur côté se rendent responsables du Moyen-Orient, de la Chine, de la Russie, de l'Afrique et des Caraïbes. Le Canada quant à lui prend en charge l'intérieur de la Russie, la Chine et certaines parties de l'Amérique Latine. Enfin, La Nouvelle-Zélande est chargée de surveiller le Sud du Pacifique et le Sud-Est Asiatique et l'Australie le Sud et l'Est de l'Asie⁸⁶. Ainsi, les Five Eyes ont

progressivement évolué face au développement de nouvelles formes de conflictualités, pendant la Seconde Guerre mondiale, la Guerre froide et jusqu'à aujourd'hui.

1. La fondation des Fives Eyes : 1941-1956

La « *Special Relationship* » durant la Seconde Guerre mondiale

Pendant la Seconde Guerre mondiale, le partage d'informations vitales entre les gouvernements britannique et américain avait permis de faciliter l'effort de guerre et *in fine* a constitué un réel atout pour la victoire des Alliés⁸⁷. La rencontre entre Winston Churchill et Franklin Roosevelt à bord du HMS Prince of Wales les 9 et 12 août 1941 qui a débouché sur la Charte de l'Atlantique⁸⁸ a été un des moments décisifs dans la constitution de la *Special Relationship*. Si les deux chefs d'État ont principalement échangé autour d'une grande stratégie maritime pour vaincre Hitler, un des autres sujets était la formation d'un réseau de partage de renseignements sensibles sur l'Allemagne et le Japon basé sur des interceptions de communication⁸⁹. En effet, de la charte

⁸⁵ The Economist. (2025, 16 mai). Trump v the spies of Five Eyes Will the president damage the world's most powerful intelligence pact? *The Economist International*. <https://www.economist.com/international/2025/03/16/trump-v-the-spies-of-five-eyes>

⁸⁶ Sylvain Gaillaud. *Friends, Fools and Foes: les "relations spéciales" entre le Royaume-Uni et les États-Unis à l'épreuve de la révolution islamique en Iran (années 1970-1980)*. Histoire. Université Rennes 2, 2022. Français. NNT: 2022REN20041. tel-04016495 <https://theses.hal.science/tel-04016495v1/file/2022theseGaillaudS.pdf>, p. 32.

⁸⁷ Tossini, J. V. (14 Avril 2020). The Five Eyes – The Intelligence Alliance of the Anglosphere. *UK Defence Journal*. Disponible sur: <https://ukdefencejournal.org.uk/the-five-eyes-the-intelligence-alliance-of-the-anglosphere/>

⁸⁸ Une déclaration basée sur le discours des quatre libertés de Roosevelt, présentant une nouvelle vision des relations internationales.

⁸⁹ Wells, A. R. (2020). *Between Five Eyes: 50 Years of Intelligence Sharing*. Casemate Publishers.

susnommée a émané l'accord bilatéral secret BRUSA⁹⁰, signé le 17 mai 1943 entre le London Signals Intelligence Board (SIB⁹¹), qui représentait le Foreign Office, l'Admiralty, le War Office, Air Ministry et d'autres agences de l'Empire britannique, et le US State–Army–Navy Communication Intelligence Board (CIB⁹²), qui représentait l'Etat Américain, la Navy, le War Department et d'autres agences de Renseignement.

Pendant la guerre, la coopération transatlantique a permis d'intercepter des communications radio provenant des armées allemande, italienne et japonaise grâce au réseau étendu de stations d'écoute qui avait été constitué⁹³. L'excellence britannique dans le monde du décryptage a de manière évidente profité à leurs homologues américains, qui en étaient devenus dépendants⁹⁴, mais a surtout permis de fonder une alliance de renseignement solide en temps de guerre. Parmi ces réussites nous pouvons citer les opérations ENIGMA à Bletchley Park⁹⁵ et ULTRA.⁹⁶

Officialisation de l'alliance après la guerre

La signature le 5 mars 1946 d'un accord, cette fois multilatéral, le « British-U.S. Communication Intelligence Agreement⁹⁷ » a marqué le renouvellement de l'alliance⁹⁸ en réaffirmant la coopération sur les opérations SIGINT⁹⁹. La création d'un standard pour le partage d'informations permet aussi de réglementer le partage de produits d'intelligence tels que les types de communications échangées ou les méthodes et techniques partagées en plus du renseignement « brut »¹⁰⁰. Une nouveauté dans le document est le statut spécial de l'Australie, la Nouvelle-Zélande et le Canada qui sont considérés comme des pays collaborateurs du fait de leur statut de territoire du Commonwealth (des « dominions¹⁰¹ »).

Actualisation des accords et entrée de l'Australie, de la Nouvelle-Zélande et du Canada

La grande réforme dans le monde du renseignement américain, notamment par la centralisation des services en 1952 sous l'égide de la NSA¹⁰², a permis la mise à jour

⁹⁰ Plus tard renommé UKUSA Agreement.

⁹¹ Pfluke, C. (2019). A history of the Five Eyes Alliance: Possibility for reform and additions. *Comparative Strategy*, 38(4), 302–315. <https://doi.org/10.1080/01495933.2019.1633186>

⁹² *Ibid.*

⁹³ Farrell, P. (2 décembre 2013). History of 5-Eyes – explainer. *The Guardian*. Disponible sur : <https://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer>

⁹⁴ Gaillaud (2022), *op.cit.*

⁹⁵ Wells, A. R. (2020). *Between Five Eyes: 50 Years of Intelligence Sharing*. Casemate Publishers.

⁹⁶ Farrell, P. (2 décembre 2013). History of 5-Eyes – explainer. *The Guardian*. Disponible sur : <https://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer>

⁹⁷ Ou UKUSA.

⁹⁸ Kim, S., et al. (2018). Newly Disclosed Documents on the Five Eyes Alliance and What They Tell Us about Intelligence-Sharing Agreements. *Lawfare media*

[Preprint]. Disponible sur : <https://www.lawfaremedia.org/article/newly-disclosed-documents-five-eyes-alliance-and-what-they-tell-us-about-intelligence-sharing>.

⁹⁹ Les deux missions principales assignées à la science de SIGINT (*signals intelligence*) sont la COMINT (*communications intelligence*), soit l'interception et l'analyse de communications électromagnétiques et de liaisons de données, et l'ELINT (*electronic intelligence*), soit la collecte et l'analyse d'émissions comme entre autres la détection de radars, ou bien d'essais nucléaires. Même si SIGINT ne permet pas de révéler les intentions et stratégies d'un Etat adverse, son utilisation est utile pour découvrir ses actions. Cox, *op.cit.*

¹⁰⁰ Pfluke, C. (2019). A history of the Five Eyes Alliance: Possibility for reform and additions. *Comparative Strategy*, 38(4), 302–315. <https://doi.org/10.1080/01495933.2019.1633186>.

¹⁰¹ Pfluke, *op.cit.*

¹⁰² NSA : National Security Agency.

du traité BRUSA. En 1955, les trois pays du Commonwealth sont enfin considérés comme membres à part entière de l'alliance¹⁰³, formalisant le partenariat entre la NSA, le GCHQ (Government Communications Headquarters), le CSEC (Canada's Communications Security Establishment), le DSD (Australian Defense Signals Directorate) et le GCSB (New Zealand's Government Communications Security Bureau¹⁰⁴).

Le nom de l'alliance tire d'ailleurs son origine du timbre qui était apposé sur les dossiers classifiés communiqués aux services de renseignements des cinq États, c'est-à-dire : « TOP SECRET—AUS/CAN/NZ/UK/US EYES ONLY. ». Les services ont ensuite choisi de simplifier la mention par « TOP SECRET- FIVE EYES ONLY », car plus simple à lire, d'où le nom¹⁰⁵.

2. Le rôle de Five Eyes durant la Guerre Froide

Maturation de l'alliance

Les tensions permanentes de la Guerre Froide alimentées par la montée en puissance de la menace (nucléaire) soviétique ont permis à l'alliance Five Eyes de mûrir et d'établir une confiance mutuelle entre les pays du groupe,

notamment en approfondissant la coopération dans le domaine des SIGINT et de la cryptologie¹⁰⁶. Par exemple, les programmes ECHELON¹⁰⁷ et VENONA¹⁰⁸ étaient des outils utilisés de manière importante par les pays des Five Eyes pendant la Guerre Froide.

L'enjeu central était le besoin d'une évaluation constante des capacités et des modèles opérationnels des forces soviétiques afin de comprendre leurs tactiques et techniques et donc à terme, d'améliorer le niveau de préparation à la guerre¹⁰⁹. La complémentarité de ces services de renseignement a contribué à ce que les Five Eyes gagnent la « intelligence war », leurs capacités SIGINT dépassant celles des Soviétiques pendant toute la durée du conflit.¹¹⁰

Il était intéressant pour les États-Unis de coopérer avec ces pays notamment compte tenu de la présence de l'Empire Britannique au Moyen-Orient¹¹¹, à l'image de l'Iran, qui a servi de « zone d'observation des installations d'essai des missiles soviétiques en Asie centrale¹¹² » et de « poste de collecte de renseignements électroniques à partir de 1957¹¹³ », permettant par exemple aux alliés anglosaxons d'intercepter les communications militaires¹¹⁴. De plus, le

¹⁰³ Le Canada est entré officiellement dans l'accord en 1948 et l'Australie et la Nouvelle-Zélande en 1956. Farrell, *op.cit.*

¹⁰⁴ Pfluke, *op.cit.*

¹⁰⁵ *Ibid.*

¹⁰⁶ Cox, J. (2012). Canada and the Five Eyes Intelligence Community. Dans *Canadian Defence & Foreign Affairs Institute and Canadian International Council*.

¹⁰⁷ ECHELON : programme d'écoute géré par la NSA depuis Fort Meade, bénéficiant de stations partout dans le monde. Dans les années soixante, les pays des Five Eyes basaient leurs interceptions sur une liste de mots clés sensibles.

¹⁰⁸ VENONA : programme d'espionnage débuté en 1943 (sous la direction de l'AFSA puis de la NSA).

« VENONA » est en réalité le nom de code qui a été donné à quasiment 3 000 communications ou télégrammes soviétiques secrets interceptés par les pays des Five Eyes.

¹⁰⁹ Wells, *op.cit.*

¹¹⁰ *Ibid.*

¹¹¹ Tossini, *op.cit.*

¹¹² Gaillaud (2022), *op.cit.*, p. 32.

¹¹³ *Ibid.*

¹¹⁴ Gaillaud, Sylvain. « Family Matters : les relations de renseignement entre le Royaume-Uni et les États-Unis à l'épreuve de la révolution islamique en Iran ». *Études françaises de renseignement et de cyber*, 2023/1 N° 1, 2023. p.185-203. CAIRN.INFO, <https://doi.org/10.3917/efrc.231.0185>, p. 6.

territoire arctique du Canada a profité au gouvernement américain car situé assez proche géographiquement pour pouvoir écouter et intercepter les communications des bases militaires arctiques russes situées au Nord de l'URSS à l'aide de la base canadienne « Alert », au Nunavut¹¹⁵.

Coopération entre services de renseignement et les Marines de guerre

En dernier lieu, la menace sous-marine soviétique dans les années 1960 a fait émerger une nécessité pour les Five Eyes de coopérer d'autant plus dans le domaine naval. La forte coopération entre les Marines des pays membres des Five Eyes signifie en pratique des opérations navales spéciales liées à la NSA, au GCHQ et aux autres services. L'objectif des Marines des Five Eyes était à ce moment d'être techniquement et opérationnellement supérieures à la marine soviétique et à celles de ses alliés du Pacte de Varsovie.

Pendant la Guerre Froide, l'URSS entreprenait la construction de nouvelles classes de sous-marins, et les Five Eyes avaient donc un besoin constant et urgent de connaître exactement leurs capacités techniques. Ainsi, les services ont développé des profils pour chaque sous-marin soviétique, à partir de leur signature acoustique. La coopération entre quatre des cinq pays de l'alliance qui disposaient des capacités sous-marines (à l'exception de la Nouvelle-Zélande) leur a permis de perfectionner la science de l'intelligence acoustique (ACINT) afin de localiser et de

suivre les sous-marins soviétiques en développement constant. La mer est donc devenue l'un des théâtres de la collecte de renseignements pour Five Eyes pendant la Guerre Froide.

3. Enjeux actuels

Le fonctionnement des Five Eyes

En 2017, le Canada faisait référence à l'alliance dans son livre blanc consacré à la défense en parlant de la « Five-Eyes community¹¹⁶ ». Cette alliance bénéficie d'un réseau d'agences de renseignement distinctes mais reliées entre elles¹¹⁷. Ce qui fait réellement son homogénéité et son unité est avant tout les liens que partagent les pays membres et qui constituent ce qu'on appelle souvent l'« Anglosphère »¹¹⁸.

Lors de sa création, le point focal de l'alliance se limitait au domaine SIGINT¹¹⁹. Five Eyes dispose aujourd'hui d'un large champ de compétences, opérant selon une division du monde en zones géographiques¹²⁰. Les responsables des agences de renseignement de défense des cinq pays se rencontrent deux fois par an pour échanger des stratégies communes et la ligne de communication très sécurisée *Stoneghost* leur est dédiée. Une division en cinq domaines de guerre (maritime, terrestre, aérien, spatial et cyberspace) a également été instituée dans le fonctionnement.¹²¹

L'avantage de cette alliance étendue est d'avoir des renseignements actualisés en temps réel sur les menaces dans le monde sans pour autant que les pays doivent

¹¹⁵ Pfluke, *op.cit.*

¹¹⁶ Vucetic, S. (2 Janvier 2020). CANZUK anyone? Diplomat Magazine. Disponible sur : <https://diplomatonline.com/mag/2020/01/canzuk-anyone/>

¹¹⁷ Cox, *op.cit.*

¹¹⁸ Wells, *op.cit.*

¹¹⁹ Vucetic, 2020.

¹²⁰ Pfluke, *op.cit.*

¹²¹ Cox, *op.cit.*

étendre leurs ressources. Fives Eyes constitue une force stratégique sur la scène internationale¹²² et la coopération avec les services de renseignement américains, dotés d'importants moyens, bénéficie aux quatre autres pays¹²³ et renforce en conséquent la prédominance de l'Anglosphère.¹²⁴

La confidentialité

Lorsque que nous mentionnons Five Eyes, il est important de rappeler qu'il s'agit ici d'une alliance d'une confidentialité extrême de 1946 au début des années 2000. L'alliance a été reconnue en 1999¹²⁵ mais n'a été connue des populations seulement en 2005 et la déclassification du UKUSA Agreement sur le site de la NSA¹²⁶ n'a pas eu lieu avant 2010¹²⁷. Ce sont en grande partie les révélations d'Edward Snowden en 2013 qui ont mené à l'entrée de Five Eyes dans le débat public¹²⁸, en exposant notamment les postes d'écoutes australiens en Asie-Pacifique partageant des renseignements avec les Etats-Unis¹²⁹. Les informations sur cette station d'écoute située à Alice Springs¹³⁰ ont aujourd'hui été déclassifiées et on peut désormais lire le « Pine Gap Agreement » de 1998¹³¹, sur l'utilisation d'une base opérée à la fois par les services de renseignements australiens et américains.

Développements au XXIème siècle

Si les avancées technologiques récentes offrent de nombreuses possibilités aux Five Eyes pour intercepter des communications diplomatiques et militaires ou pour rassembler des informations sur des caractéristiques de radars, d'engins spatiaux et de systèmes d'armes développés par d'autres pays¹³², la confidentialité de l'alliance ne permet pas de connaître ses derniers développements. L'histoire récente de l'alliance a été marquée par la réintégration de la Nouvelle-Zélande. En effet, des tensions avaient éclaté entre les Etats-Unis et la Nouvelle-Zélande lorsque cette dernière avait déclaré en 1986 sa volonté de devenir une zone démilitarisée, refusant l'accès aux navires américains soit dotés d'armes nucléaires, soit à propulsion nucléaire. Ce désaccord avait fragilisé les traités de l'alliance et la Nouvelle-Zélande avait cessé son partage de renseignements avec le reste des Five Eyes, tout en continuant à en recevoir. Sa réintégration s'est prouvée cruciale étant donné la possession de postes d'écoute radio à Waihopai¹³³ et Tangimoana¹³⁴.

Au XXI^{ème} siècle, les Five Eyes se renouvellent par une ouverture (limitée) à des pays tiers. Effectivement, les Nine Eyes incluent en plus des cinq pays fondateurs le Danemark, la France, la Norvège, et les

¹²² Wells, *op.cit.*

¹²³ O'Neil, A. (2017) 'Australia and the "Five Eyes" intelligence network: the perils of an asymmetric alliance', *Australian Journal of International Affairs*, 71(5), pp. 529–543. Disponible sur : <https://doi.org/10.1080/10357718.2017.1342763>.

¹²⁴ *Ibid.*

¹²⁵ *Ibid.*

¹²⁶ Archives en ligne de la NSA, « UKUSA Agreement Release », <https://www.nsa.gov/Helpful-Links/NSA-FOIA/Declassification-Transparency-Initiatives/Historical-Releases/UKUSA/>

¹²⁷ Tossini, *op.cit.*

¹²⁸ Voir article précédent.

¹²⁹ Farrell, *op.cit.*

¹³⁰ Joint Defense Facility at Pine Gap Agreement Between the UNITED STATES OF AMERICA and AUSTRALIA Extending the Agreement of December 9, 1966, As Amended and Extended Effected by Exchange of Notes Signed at Canberra June 4, 1998 <https://www.state.gov/wp-content/uploads/2019/02/12959-Australia-Defense-SDI-6.4.1998.pdf>

¹³¹ Qui prolongeait l'accord similaire conduit en 1966.

¹³² Cox, *op.cit.*

¹³³ A cessé de fonctionner en 2021.

¹³⁴ Pfluke, *op.cit.*

Pays-Bas, auxquels s'ajoutent la Belgique, l'Italie, l'Allemagne, l'Espagne et la Suède dans le cadre des Fourteen Eyes¹³⁵. Ces pays coopèrent déjà au sein de l'OTAN, dans le NATO Special Committee où les chefs des services de renseignement nationaux sont rassemblés. Le choix de ces alliés n'est donc pas anodin.

Conclusion

L'adhésion limitée de l'alliance engendre des problèmes de surcharge pour les pays, qui doivent pallier un besoin de renseignement constant et actualisé sur les nombreuses menaces mondiales en développement¹³⁶. De plus, si l'alliance est chère aux gouvernements en faisant partie, certains pointent du doigt une asymétrie et une domination américaine dans l'alliance et selon Sylvain Gaillaud : « Aux termes de cette complémentarité stratégique, chacun des partenaires entend tirer son épingle dans le grand jeu de la puissance¹³⁷ ». Cette coopération avec les Etats-Unis pourrait bel et bien avoir un impact sur la sécurité de ses alliés, à l'image de l'Australie qui serait exposée à un risque plus grand de devenir la cible d'attaques nucléaires due à la présence d'installations et d'infrastructures de renseignements américains sur son sol¹³⁸. D'un autre côté, certains considèrent que le Canada, l'Australie et la Nouvelle-Zélande ont eu tendance à suivre le modèle de renseignement britannique du fait de leur histoire¹³⁹.

Si la frontière entre renseignement intérieur et extérieur était auparavant très claire, elle est aujourd'hui de plus en plus

brouillée et provoque des questionnements de la part du public sur l'atteinte au droit à la vie privée¹⁴⁰. Cette pression de l'opinion publique pourrait dans une certaine mesure limiter les marges de manœuvre des Five Eyes, notamment dans la lutte contre le terrorisme¹⁴¹. En effet, l'émergence d'acteurs non-gouvernementaux, la menace du terrorisme et l'importance croissante du cyberspace et de la guerre informationnelle constituent de nouveaux enjeux pour les Five Eyes.

C.M.

¹³⁵ Ou SSEUR SIGINT Seniors Europe. Tossini, *op.cit.*

¹³⁶ Pfluke, *op.cit.*

¹³⁷ Gaillaud, *op.cit.*, p. 32.

¹³⁸ O'Neil, *op.cit.*

¹³⁹ Wells, *op.cit.*

¹⁴⁰ O'Neil, *op.cit.*

¹⁴¹ Pfluke, *op.cit.*

The background features a complex, abstract geometric pattern of thin, light gray lines forming various irregular polygons and shapes. A thin, solid red border frames the entire page.

Dossier Spécial

Les nouveaux espaces du renseignement

Le renseignement industriel au coeur de la guerre économique : synergies et rivalités entre États et entreprises

Auteur : Alexis Toesca, Mastérand en Francophonie, Stratégie et Relations Internationales.



La guerre économique est au cœur des préoccupations depuis l'instauration de la présidence de Donald Trump en janvier 2025. Multipliant les annonces de l'augmentation des droits de douane de 15 % à 25 % contre la Chine, le Canada ou bien l'Union européenne, les États-Unis misent sur une stratégie de pression périlleuse pour l'économie mondiale en vue de maximiser des gains économiques immédiats. Le président américain privilégie une approche transactionnelle mise en œuvre par des accords bilatéraux et des négociations (*deals*)¹. Il utilise le commerce comme levier fondamental pour mener sa politique étrangère.

La guerre économique semble renvoyer à une confrontation entre les parties (États, entreprises et ONG) qui vise

Source : [La Tribune](#)

à capter, maîtriser et accaparer des richesses dont l'objectif est l'accroissement de la puissance par l'économie. Elle remplit cinq critères : la limitation des dépendances, la localisation des activités économiques et industrielles, la compétition informationnelle, la projection sur les marchés extérieurs et la prédation économique². Le renseignement économique va intervenir sur ces cinq thématiques avec des acteurs différents. Tandis que l'espionnage industriel est décrit comme un dérivé malsain de la veille technologique, il s'agit en réalité de l'ensemble des pratiques à travers lesquelles des informations de sources fermées sont obtenues par des moyens répréhensibles (corruption, piratage, vols)³. L'espionnage industriel ne peut être confondu avec l'intelligence économique

¹ La politique étrangère de l'administration Trump par Maya Kandel | vie-publique.fr. (2020, mars 4). <https://www.vie-publique.fr/parole-dexpert/273699-la-politique-etrangere-de-ladministration-trump-par-maya-kandel>

² FRANCE 24. (2024, 12 novembre). *Guerre économique : l'arme du renseignement* • FRANCE 24 [Vidéo].

YouTube.

<https://www.youtube.com/watch?v=VFAGLNZgZUE>

³ Fane, O., Feige, J., & Bidi, G. (2024). Espionnage industriel et intelligence économique : Cadre d'analyse d'une délimitation. *Management & Sciences Sociales*, 36(1), 134-151. <https://doi.org/10.3917/mss.036.0134>

qui utilise des moyens légaux ou pouvant se trouver dans un flou juridique pour récolter l'information. L'intelligence économique, selon Henri Martre est :

«L'ensemble des actions coordonnées de recherche, de traitement et de distribution, en vue de son exploitation, de l'information utile aux acteurs économiques [...] L'information utile est celle dont ont besoin les différents niveaux de décision de l'entreprise ou de la collectivité, pour élaborer et mettre en œuvre de façon cohérente la stratégie et les tactiques dans le but d'améliorer sa position dans son environnement concurrentiel⁴.»

De surcroît, le numérique a aussi transformé les méthodes d'espionnage industriel avec l'apparition du cyberespionnage. Des malwares, des logiciels espions et des attaques de phishing sont utilisés pour exploiter les vulnérabilités des systèmes et des réseaux informatiques⁵. Selon, le Rapport Hiscox 2023, 53% des entreprises françaises ont subi une attaque cette même année. Les entreprises comme les États redoublent d'efforts pour se protéger face aux cyberattaques.

L'article cherchera à expliquer comment les États et les entreprises utilisent l'espionnage industriel et le renseignement économique dans un contexte de guerre économique.

En premier lieu, nous étudierons les actions des États en matière de guerre économique à travers des études de cas

historiques sur la France Gaullio-pompidolienne et sur les États-Unis. En second lieu, nous approfondirons le concept de guerre économique à partir des stratégies d'espionnage industriel mises en place dans les pays asiatiques à partir des années 1960.

Le Rôle des États dans la protection et l'influence des entreprises nationales : La France Gaullio-pompidolienne et les États-Unis de l'après-guerre froide

Dans un souci de souveraineté, la France Gaullio-pompidolienne a construit un ensemble administré, favorisant les grands projets industriels, spatiaux et a cherché à accéder à une indépendance énergétique. Les grandes entreprises pétrolières françaises servaient de bras armé, sécurisant les approvisionnements en matières premières essentielles (Elf-Aquitaine, Cogema, etc.) en lien avec les services de renseignement⁶. Après l'indépendance algérienne en 1962, la France se tourne alors vers les ressources de son ancien empire colonial en Afrique de l'Ouest. Par l'intermédiaire de Jacques Foccart⁷, du SDECE⁸ et de la compagnie pétrolière Elf. Paris, va créer un réseau d'influence pour maintenir ou mettre en place des dirigeants « amis de la France » à la tête des États pétroliers du golfe de Guinée.⁹ Le but est d'assurer la stabilité du pays producteur, car la rentabilité d'un gisement pétrolier se fait sur le temps long.

⁴ Martre, H. (1994). Rapport du Groupe « Intelligence économique et stratégie des entreprises ». 11.

⁵ *Qu'est-ce que le cyber espionnage ?* | Proofpoint FR. (2024, mai 13). Proofpoint. <https://www.proofpoint.com/fr/threat-reference/cyber-espionage>

⁶ Moinet, N. (2021). Le renseignement d'intérêt économique au défi de la souveraineté nationale. *Revue Défense Nationale*, 842(7), 23-27. <https://doi.org/10.3917/rdna.842.0023>

⁷ Homme politique français, secrétaire général aux affaires malgaches et africaines de 1960 à 1974.

⁸ Le Service de documentation extérieure et de contre-espionnage est le service renseignements extérieur français créé le 28 décembre 1945 et devient la direction générale de la Sécurité extérieure le 2 avril 1982.

⁹ Pernod, M., Rey, M., Phung, J., Meresse, P.-A., & Martin, R. (2021). Le rôle des services de renseignement dans une politique pétrolière (p.30). *Dossier Ecole de guerre économique*. <https://www.ege.fr/infoguerre/le-role-des-services-de-renseignement-dans-une-politique-petroliere>

La guerre du Biafra au Nigéria (1967-1970) est un cas d'étude de guerre économique entre les entreprises françaises et britanniques. L'objectif français était d'acquérir des gisements de pétrole nigériens et le terminal pétrolier de Port Harcourt alors sous contrôle anglo-saxon. En utilisant le SDECE, la France va soutenir le mouvement sécessionniste en envoyant des armes et des mercenaires sous couvert humanitaire. La guerre du Biafra peut être analysée aussi comme une guerre entre les compagnies pétrolières britanniques, Shell et BP et le français SAFRAP. Paris parvient ainsi à concurrencer au Nigeria les compagnies pétrolières britanniques. Bien que la révolte fut écrasée par l'armée nigérienne, causant plus d'un million de morts, la compagnie pétrolière va maintenir l'essentiel de sa production de pétrole. En somme, le « système Foccart » constitue un modèle d'efficacité concernant l'indépendance énergétique. Cependant, il n'a pas permis à la France de développer une vision globale du renseignement économique.¹⁰

Le cas des États-Unis depuis la fin de la guerre froide démontre la création d'un écosystème novateur dans le renseignement économique. Dans un premier temps, la législation joue un rôle central dans cet écosystème. Au cours des mandats du président Reagan, la signature des *Executive orders* a conduit à l'inclusion du secteur privé dans des opérations clandestines visant à lutter contre l'espionnage économique, scientifique et

technologique de l'URSS. Après la guerre froide, les différentes administrations américaines et les services de renseignements ont placé comme priorité le renseignement économique. Les agences ont renforcé leur surveillance des entreprises étrangères concurrentes, souvent dans le cadre de la lutte contre la corruption et l'espionnage économique. Par exemple, les lois votées - comme l'*Economic Espionage Act* et l'*Economic Security Act* - protègent les entreprises contre le vol de secrets d'affaires, de brevets technologiques et d'informations économiques confidentielles. Les contrevenants risquent jusqu'à 500 000 dollars d'amende et 15 ans de prison.¹¹ Dans un deuxième temps, la collaboration entre les entreprises numériques américaines (GAFAM) avec l'État fédéral facilite le renseignement économique. Les révélations d'Edward Snowden ont mis en exergue leurs participations dans la mise en œuvre des programmes de surveillance de masse de la National Security Agency (NSA).¹²

Tandis qu'au niveau européen, la législation et la stratégie de protection contre l'espionnage industriel ont des difficultés à se structurer. Le rapport Frantz publié en 2014 pointe l'insuffisance et la fragmentation de la protection juridique des secrets d'affaires dans l'Union européenne. Les entreprises déclarent à 63 % que le niveau de protection juridique des secrets d'affaires est faible¹³. En définitive, la guerre économique entre les États dépasse

¹⁰ *Ibid.*, p. 32

¹¹ Masson (Hélène), *Les fondements politiques de « l'intelligence économique »*, thèse de doctorat en sciences politiques, Université Paris XI, 2001. <http://masson-intelligenceeconomique.blogspot.fr/>. Voir également Hélène Masson, *L'intelligence économique, une histoire française*, Vuibert, 2012.

¹² Thibout, C. (2022, mai 13). *Les GAFAM et l'État : Quelles évolutions du champ du pouvoir?* IRIS. <https://www.iris-france.org/167483-les-gafam-et-letat-queelles-evolutions-du-champ-du-pouvoir/>

¹³ Fane, O., & Feige, J. (2019). *Espionnage industriel : Protections, outils de gestion et perspectives ?* *Question(s) de management*, 23(1), 89-102. <https://doi.org/10.3917/qdm.191.0089>

les alliances et s'inscrit dans une dynamique d'adaptation constante. Ainsi que les stratégies de protection développées par les États sont en évolution perpétuelle et durablement confronté à l'espionnage industriel. Ce dernier constitue un levier stratégique majeur dans l'intensification de la compétition économique entre pays développés et émergents. Notamment, certains pays asiatiques recourent à ces pratiques pour accélérer leur rattrapage technologique pour accroître leur puissance économique.

L'espionnage industriel dans les pays asiatiques, un moteur de développement ?

Dans cet affrontement impitoyable entre les économies mondiales. Chaque nation souhaite engranger des profits et des revenus croissants aux dépens des autres pays. Les États doivent disposer de moyens de renseignements performants afin de se protéger des actions des groupes rivaux et de connaître les projets des concurrents pour éventuellement les copier. Cet espace conflictuel est particulièrement actif en Asie dont au premier rang figurent le Japon, la Chine et la Corée du Sud¹⁴.

Le Japon après la Seconde Guerre mondiale, a réussi l'exploit de redresser son économie dévastée et d'en faire l'une des plus puissantes au monde. Ce rebond est en partie dû à l'appropriation des secrets de fabrication des produits étrangers pour les imiter et les confectionner dans leurs usines. Le JETRO (*Japanese External Trade Organization*) a joué un rôle essentiel dans ce rattrapage économique¹⁵. Il sert à promouvoir le commerce extérieur et les investissements étrangers dans le pays ainsi

que les échanges technologiques. Pour ce faire, le JETRO entretient une centaine de bureaux à l'étranger qui « travaillent » en relation étroite avec les compagnies de commerce. Par ce moyen, le JETRO se comporte comme un véritable service d'espionnage à l'échelle planétaire. Des stagiaires, étudiants et touristes japonais ont ainsi parcouru les États-Unis notamment dans la zone de la Silicon Valley en recueillant des informations¹⁶. Si les États-Unis et le Japon restent de solides alliés dans le champ militaire, ils sont au contraire de farouches adversaires économiques.

La Chine adopte une stratégie globale et intégrée en matière de renseignement économique. Elle allie à la fois l'espionnage industriel et dispositifs légaux d'intelligence économique¹⁷. Depuis les années 1980, les services de renseignements chinois sont stratégiquement intégrés pour recueillir les informations économiques. Puis, la Chine a acquis des solides compétences en cyberespionnage. De plus, la Chine a bénéficié des transferts technologiques des entreprises occidentales pour sa modernisation. Cette stratégie vise à rendre l'économie chinoise moins dépendante et plus compétitive dans des domaines tels que l'aérospatial ou les nanotechnologies. Toutefois, la Chine utilise massivement l'espionnage aussi bien dans l'industrie que dans le milieu universitaire. L'ancien chef du FBI Christopher Wray déclarait dans un cercle de réflexion le 7 juillet 2020 « Sur dix ans, on a assisté à une hausse de 1 300% des dossiers d'espionnage économique impliquant la Chine », c'est-à-dire « l'un des

¹⁴ Klen, M. (2022). Les Asiatiques dans l'espionnage économique. *Revue Défense Nationale*, N° 847(2), 105. <https://doi.org/10.3917/rdna.847.0105>

¹⁵ *Ibid.*, p.105.

¹⁶ *Ibid.*, p.106.

¹⁷ Moinet, N. (2023). De l'espionnage industriel à l'intelligence économique : la stratégie agile et intégrée de la puissance chinoise. *Diplomatie : affaires stratégiques et relations internationales*, 88. <https://hal.science/hal-04703195>

plus importants transferts de richesses de l'histoire humaine¹⁸ ».

L'affaire Ommic¹⁹ illustre un cas d'espionnage industriel sur une entreprise française afin de contourner des restrictions technologiques imposées par les États-Unis à la Chine. En 2018, l'investisseur chinois Ruodan Zhang a acquis 94 % des parts de



Source : Illustration IP3/Vincent Isore pour [le Parisien](#)

l'entreprise française Ommic, spécialisée dans les semi-conducteurs. Le dirigeant est soupçonné d'avoir utilisé sa position de président pour permettre l'exportation de semi-conducteurs vers la Chine à un prix bradé. En 2021, un contrôle douanier a mis en évidence des tentatives d'exportation illicite de composants électroniques dissimulés sous des fiches techniques falsifiées. Les dirigeants impliqués ont été mis en examen en mars 2023 pour « livraison à une puissance étrangère de procédés, documents ou fichiers de nature à porter atteinte aux intérêts fondamentaux de la nation²⁰. » Ce crime est passible d'une peine de quinze ans de réclusion criminelle et d'une amende pouvant atteindre 225 000 euros.

Bien que la Chine continue de recourir à l'espionnage, elle s'affirme comme une puissance d'innovation dans les nouvelles technologies et la production scientifique. Pékin est leader dans certains domaines d'avenir comme la 5G, l'éolien et les batteries électriques. Globalement, la Chine apparaît aujourd'hui comme un pays disposant de ses propres capacités de recherche et d'innovation, rivalisant directement avec les États-Unis, elle est devenue une machine de guerre économique.

Conclusion

Dans un contexte de guerre économique, les États en collaboration avec les entreprises ont adopté des stratégies d'espionnage et d'intelligence économique spécifiques. L'analyse des cas étudiés met en évidence le rôle structurant du renseignement économique dans la consolidation des puissances économiques. Si les pays asiatiques, en particulier la Chine, ont tiré profit de l'espionnage industriel pour leur transition vers une innovation autonome, cette dernière reconfigure les rapports de forces économiques mondiaux. Dans ce contexte instable, la sécurisation des industries stratégiques devient une priorité, nécessitant des investissements et un cadre législatif renforcé pour préserver les intérêts nationaux. **A.T.**

¹⁸ *Élections américaines et espionnage industriel : Le patron du FBI évoque la menace chinoise.* (2020, juillet 8). RFI. <https://www.rfi.fr/fr/am%C3%A9riques/20200708-elections-am%C3%A9ricaines-et-espionnage-industriel-le-patron-fbi-%C3%A9voque-la-menace-chi>

¹⁹ Deville, R. (2023, novembre 9). *L'affaire Ommic, l'illustration du contournement de l'embargo américain*

de la Chine par l'espionnage industriel. Ecole de Guerre Economique. <https://www.ege.fr/info Guerre/laffaire-ommic-lillustration-du-contournement-de-lembargo-americain-de-la-chine-par-lespionnage-industriel>

²⁰ *Ibid.*

La numérisation des activités humaines et le tournant du renseignement vers la quantité

Auteur : Loïc Parmentier, Mastérent en Prévention et Gestion des Risques.

Depuis un siècle, le renseignement a connu plusieurs mutations liées aux avancées technologiques. Avec l'avènement des moyens de communication modernes, le renseignement d'origine électromagnétique, ROEM ou SIGINT, a progressivement pris une place prépondérante. Dès la Première Guerre mondiale, l'interception des communications téléphoniques ou des transmissions radios croît en importance, notamment lors de la Bataille de Verdun¹. Durant la Seconde Guerre mondiale, le cryptage des communications allemandes par *Enigma*, ainsi que son déchiffrement par les services britanniques jouèrent un grand rôle dans la conduite des opérations. Pendant la Guerre froide, américains et soviétiques ne cessèrent d'innover technologiquement dans le renseignement. La diffusion du numérique a forcé les services de renseignement à muter. Auparavant centré sur le renseignement d'origine humaine (HUMINT), le renseignement d'origine électromagnétique a progressivement pris une place prépondérante. Dans les années 1970 s'établit le réseau ECHELON entre les pays des *Fives Eyes*, à savoir les Etats-Unis, le Royaume-Uni, l'Australie, le Canada et la Nouvelle-Zélande, destiné à recueillir du ROEM. L'augmentation exponentielle des communications mondiales a amené une restructuration généralisée des services de renseignement vers le SIGINT, puis vers l'OSINT. Cet article va donc chercher à montrer comment la prise en importance du SIGINT dans le renseignement a entraîné une

mutation de ce dernier vers la problématique de la quantité de données.

Le SIGINT comme outil de surveillance massive

L'avènement du SIGINT, basé sur l'augmentation exponentielle des communications mondiales, a amené une restructuration généralisée des services de renseignement, et a permis à la lutte contre le terrorisme d'obtenir des moyens de surveillance inégalés jusqu'alors. Avec le 11 septembre 2001, les priorités américaines en matière de renseignement vont radicalement évoluer. Engagés dans une guerre globale contre le terrorisme, les services américains vont utiliser les nouvelles technologies de communication pour établir des programmes de surveillance massive afin de prévenir les actes de terrorisme. La priorité est donnée à la prévention par la captation massive des données personnelles. Cette masse devient donc la cible du renseignement américain. L'*USA Patriot Act*, adopté le 25 octobre 2001 va considérablement élargir les prérogatives des services de renseignement américains tout en réduisant le contrôle judiciaire de leurs activités. Il permet notamment au FBI d'utiliser massivement les « *National Security Letters* », lui permettant de forcer, des groupes privés, dont les FAI², à partager les données personnelles dont ils disposent sur un individu sans que celui-ci ne soit clairement en lien avec une menace³. De plus, le Président Bush autorise secrètement la NSA à réaliser une surveillance massive de l'ensemble des moyens de communication, à

¹ Jean-Marc Degoulange, « Les services de renseignement français dans la bataille de Verdun », dans *Renseignement et espionnage pendant la Première Guerre Mondiale*, sous la direction d'Eric Denécé, <https://unr-ra-scholarvox-com.ezscd.univ-lyon3.fr/book/88945781>

² Fournisseur d'Accès Internet

³ Ursula Gorham-Oscilowski et Paul T. Jaeger, « National Security Letters, the USA PATRIOT Act, and the Constitution: The tensions between national security and civil rights », *Government Information Quarterly* 25, n° 4 (1 octobre 2008): 625-44, <https://doi.org/10.1016/j.giq.2008.02.001> . p 629

l'étranger comme sur le territoire national, en l'absence de tout contrôle judiciaire pourtant exigé par le *Foreign Intelligence Service Act* de 1978⁴. Ce programme, officiellement appelé « *Terrorist Surveillance Program* » fut suspendu en 2004 pour ces mêmes raisons avant d'être remplacé par le programme « *PRISM* ». Dans ce dernier la collecte est réalisée directement au travers de fournisseurs électroniques privés américains⁵, autorisé par l'amendement de 2008 au FISA, qui introduit la Section 702 autorisant la collecte d'information électronique sur des étrangers ne se trouvant pas sur le territoire américain, même en l'absence de lien évident avec une menace. Les agences de renseignement américaines, la NSA en particulier, ont développé de multiples programmes de surveillance massive. On peut notamment citer le programme *RAMPART-A*, collectant des données sur les câbles sous-marins au points d'interconnexion, ou *XKeyscore* collectant et centralisant massivement des métadonnées ainsi que l'historique de navigation ou d'e-mails⁶. Aujourd'hui, la numérisation massive des activités humaines entraîne la possibilité d'une surveillance encore accrue. L'ensemble des communautés du renseignement ont aujourd'hui partiellement basculé vers le SIGINT et le quantitatif, bien que l'HUMINT garde une place importante.

En France, la restructuration vers le SIGINT a débuté au début des années 2000, avant d'accélérer avec la « Loi relative au renseignement », promulguée en mars 2015. Elle autorise ainsi la collecte de données à titre préventif en ligne, ainsi que la création des « boîtes noires ». Ces dernières permettent, en

passant par les Fournisseurs d'Accès à Internet, d'analyser massivement et automatiquement les métadonnées des communications de certains individus⁷. Au Royaume-Uni, on peut citer l'« *Investigatory Powers Act* » de 2016 qui permet notamment aux agences de renseignement britanniques d'avoir accès aux enregistrements de connexions internet sans mandat. La prévention par la quantité de données personnelles est donc devenue prioritaire pour les services de renseignement.

L'OSINT et le nouveau bouleversement du renseignement militaire

La massification du numérique et le développement des Nouvelles Technologies de l'Information et de la Communication (NTIC), notamment avec le smartphone, ont permis à l'OSINT d'occuper une place majeure aujourd'hui. Alors qu'auparavant la tâche principale du renseignement était de pouvoir accéder à des informations protégées, désormais il s'agit également de pouvoir traiter la masse de données disponibles, et de faire les recoupements nécessaires.

La numérisation des flux humains et des données a rendu la quantité stratégique dans le renseignement militaire. La guerre en Ukraine montre l'importance dorénavant acquise par ce type de renseignement, issu de six catégories de sources, que sont la presse et les médias, Internet, les publications gouvernementales, les publications académiques et professionnelles spécialisées, les données commerciales, et enfin la littérature grise⁸. Dans ce conflit, les ukrainiens ont encouragé, et parfois organisé, les civils à filmer et diffuser sur les réseaux sociaux toute information concernant l'ennemi. De plus, des

⁴ Marc Hecker, Tenenbaum Élie. (2022). *La guerre de Vingt Ans*. (Robert Laffont). p 67.

⁵ Stephen Gamar, « A Crucial Aspect of National Security in Need of Reform: Section 702 of the FISA Amendments Act Student Articles », *South Dakota Law Review* 65, n° 3 (2020): 489-510.

⁶ Glenn Greenwald, « XKeyscore: NSA Tool Collects "Nearly Everything a User Does on the Internet" », *The Guardian*, 31 juillet 2013, sect. US news, <https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data> .

⁷ Martin Untersinger, « Une première « boîte noire » de la loi sur le renseignement désormais active », 14 novembre 2017,

https://www.lemonde.fr/pixels/article/2017/11/14/les-boites-noires-de-la-loi-sur-le-renseignement-sont-desormais-actives_5214596_4408996.html .

⁸ Clément Renault, Paul Charon, et Fabien Laurençon, « Renseigner autrement ? Trajectoires de l'Osint dans les services de renseignement », *Hérodote* 186, n° 3 (11 octobre 2022): 19-30, <https://doi.org/10.3917/her.186.0019> .

organisations et groupes civils virtuels, à l'instar de *Bellingcat*, se sont spécialisés dans l'OSINT et apportent directement ou non, un soutien aux ukrainiens. Le cycle du renseignement s'est donc démocratisé, en particulier grâce au smartphone⁹. En effet, l'Ukraine a utilisé le haut degré de numérisation de sa population pour alimenter la base de données de l'armée ukrainienne avec de l'OSINT. Chacun est désormais équipé, avec son appareil, d'un capteur de renseignement. Des experts en OSINT de l'armée ukrainienne collectent et vérifient les informations publiées sur les réseaux sociaux, ou qui leurs sont directement envoyées par des civils ukrainiens (ou par l'OTAN), pour ensuite les insérer dans l'application de téléphone « Delta¹⁰ » qui permet de visualiser le champ de bataille et de mieux communiquer. C'est cette horizontalité qui donne une plus grande efficacité de l'armée ukrainienne.

Cette collecte massive d'information donne ainsi l'occasion à l'Ukraine de faire des bombardements ciblés, visant notamment des cibles d'une haute importance, et de compenser ainsi leur faiblesse en termes de quantité d'équipement par rapport aux russes. Néanmoins, l'importance de l'OSINT dans un conflit entraîne par ricochet une augmentation des possibilités de désinformation¹¹. Non seulement l'immense quantité d'information produite demande un traitement massif et encore plus rapide, mais aussi elle augmente considérablement les chances de manipulation.

En dehors du renseignement militaire, l'OSINT est devenu le principal facteur d'acquisition du renseignement, et son cycle d'acquisition et de traitement implique

individus comme entreprises privées¹². Plus généralement, l'OSINT vient aujourd'hui compléter le cycle du renseignement. Elle permet ainsi de faire un tri préalable et d'orienter l'action de recherche du renseignement en utilisant les capacités spécifiques, techniques ou humaines, des services de renseignement¹³. Ces derniers doivent donc réussir à gérer la quantité massive d'information, et pour cela, l'IA peut être d'un certain secours en venant soutenir l'analyste dans sa mission.

Face à la quantité, l'intelligence artificielle ?

L'intelligence artificielle va entraîner de multiples bouleversements dans le renseignement, en particulier parce qu'elle semble être le seul moyen capable de traiter l'immense quantité d'informations numériques, notamment l'OSINT. De ce fait, l'IA soutient le cycle du renseignement dans ses quatre étapes, que sont l'orientation, la collecte, l'exploitation et la diffusion. La numérisation continue des capteurs, ainsi que le développement massif de la quantité de données en ligne ont fait que l'IA peut jouer un rôle crucial dans l'étape de la collecte. Au niveau de l'exploitation, non seulement l'intelligence artificielle soutient fortement le pré-traitement des données ou leur analyse technique, mais elle joue également un rôle crucial en aidant l'analyste à repérer les données les plus susceptibles de lui être utiles¹⁴. De cette manière, l'IA vient partiellement combler le décalage grandissant entre la masse des données existantes et le traitement réalisable par l'homme¹⁵. Enfin, grâce au *deep-learning*, elle peut apporter un soutien qui n'est plus seulement technique ou au niveau des capteurs. Elle peut notamment dégager des

⁹ Sanjay P Vishwasrao, « Rising Role of OSINT in Conflict/War », *CLAWS Journal* 16, n° 2 (2023), <https://nbn-resolving.org/urn:nbn:de:0168-ssoar-97176-2> . p 90.

¹⁰ Julian Borger, « 'Our Weapons Are Computers': Ukrainian Coders Aim to Gain Battlefield Edge », *The Guardian*, 18 décembre 2022, sect. World news, <https://www.theguardian.com/world/2022/dec/18/our-weapons-are-computers-ukrainian-coders-aim-to-gain-battlefield-edge> .

¹¹ Vishwasrao, « Rising Role of OSINT in Conflict/War ». p 90.

¹² Vishwasrao. p 86.

¹³ Renault, Charon, et Laurençon, « Renseigner autrement ? »

¹⁴ DRM, « Intelligence artificielle et renseignement militaire », *Revue Défense Nationale* 820, n° 5 (2019): 107-16, <https://doi.org/10.3917/rdna.820.0107>. p 109.

¹⁵ Pascal Martin. La place de l'analyste au sein des services de renseignement avec l'essor de l'intelligence artificielle. Les Notes du CREOGN, 2024, 97. hal-04457330 . p 2.

tendances ou des singularités difficilement perceptibles pour l'homme dans une masse importante d'informations¹⁶.

L'IA permettrait ainsi de prendre en charge les tâches à faible valeur ajoutée, tout en soutenant les analystes humains dans leur travail. On se dirigerait donc vers une « hybridation de l'analyse », c'est-à-dire que l'IA viendrait en support de l'analyste humain, lui permettant de gagner en efficacité et en temps et donc en ressources¹⁷. Elle permettrait également de répondre à un suivi nécessairement plus rapide, et plus individualisé des menaces¹⁸. Néanmoins, intégrer davantage cet outil requiert une profonde mutation des services de renseignement, tant au niveau organisationnel que technique. De plus, pour des raisons évidentes de sécurité, l'IA utilisée ne peut qu'être souveraine. Enfin, pour Julien Barnu, le réel atout des nouveaux logiciels impliquant l'IA soutenant l'analyste n'est pas tant l'IA en elle-même, qui n'est que marginale, mais leur capacité à rapidement collecter, rassembler et organiser des données pour les présenter de la meilleure manière possible à l'analyste humain¹⁹.

La numérisation des communications et activités humaines est donc en train d'entraîner une mutation globale des services de renseignement vers la quantité. Plus généralement, le domaine cyber croît en

importance dans les relations entre États, et dans le domaine du renseignement. Le cyber espionnage est devenu monnaie courante, tant entre États, qu'entre acteurs économiques tandis que les cyberattaques ont pleinement intégré le registre des moyens d'actions des services. À ce sujet, Jean-Marc Wasielewski, général (2S) spécialiste des systèmes d'informations, fait justement remarquer que, bien que l'on connaisse pas toutes les actions cybernétiques se déroulant dans le cadre du conflit en Ukraine, il semble que les cyberattaques les plus développées se déroulent en temps de paix²⁰.

La numérisation des activités humaines a donc amené à une restructuration généralisée des services de renseignements à l'échelle mondiale. Si le renseignement d'origine humaine demeure crucial, de nouveaux enjeux sont apparus. Les services de renseignement ont désormais de nouveaux moyens d'action, tant par des cyber intrusions, que par la captation massive des données ou par l'exploitation du renseignement en sources ouvertes. Sur ces deux derniers points, ils sont confrontés à la problématique du tri et de l'exploitation de la masse d'information disponible, et une solution possible est, nous l'avons dit, le soutien de l'intelligence artificielle.

L.P.

¹⁶ Julien Barnu, « Intelligence artificielle et sécurité nationale », *Annales des Mines - Enjeux numériques* 12, n° 4 (2020): 54-57, <https://doi.org/10.3917/ennu.012.0054>. p 55.

¹⁷ *Ibid.* p 4.

¹⁸ DRM, « Intelligence artificielle et renseignement militaire ».

¹⁹ Barnu, « Intelligence artificielle et sécurité nationale ».

²⁰ Jean-Marc Wasielewski, « L'emploi de la cyber-électronique en Ukraine », *Revue Défense Nationale* 859, n° 4 (12 avril 2023): 90-96, <https://doi.org/10.3917/rdna.859.0090>.

Dossier Spécial

Histoire du renseignement

Les espionnes de la Seconde Guerre mondiale

Auteur : Charlotte Alesandrini, Mastérante en Francophonie, Stratégie et Relations Internationales.

« Une femme normalement douée peut, à l'égal de l'homme, devenir un parfait détective : la finesse de son esprit, sa souplesse naturelle jointe à l'influence non négligeable de son charme doivent même lui assurer une incontestable supériorité sur ses émules masculins¹ ». Robert Boucard.

De Mata Hari à Joséphine Baker en passant par Noor Inayat Khan, les récits des femmes espionnes fascinent. Cependant leurs exploits en tant qu'agents des renseignements sont souvent associés à leurs attributs physiques, minimisant leur courage et leur intelligence. Cela est notamment dû aux fantasmes provoqués par l'image d'une femme fatale et « sexy », souvent relayés par les films d'espionnage. De nombreux ouvrages participent également à cette image réductrice du rôle des femmes dans les renseignements. En déclarant « the girls who served as secret agents in Churchill's Special Operations Executive were young, beautiful and brave¹ », l'auteur Marcus de Binney dessine d'emblé une représentation physique de ces femmes. Cette discrimination tend à reléguer les femmes de l'ombre encore plus à l'ombre que les hommes de l'ombre.

Nous allons analyser l'importance du rôle des espionnes françaises résistantes

à l'occupation allemande nazie, au cours de la Seconde Guerre mondiale.

Des Françaises au sein du Spécial Operations Executive

À la suite de la défaite de la France en juin 1940, le premier ministre britannique Winston Churchill va charger le ministre de l'Économie, Hugh Dalton de créer les *Special Operations Executive* avec l'objectif de *set Europe ablaze*², en soutenant la résistance locale. Les agents du SOE³ vont opérer de 1940 à 1946 dans les territoires européens occupés par l'Allemagne nazie. A Londres une branche française, la *F section* va rapidement être créée et va déployer un total 480 agents dont 39 femmes⁴. Ces dernières vont y suivre une formation identique à celle de leurs homologues masculins. En effet, conscients des dangers inhérents aux missions, en particulier le risque de torture, les recruteurs ne faisaient aucune distinction des sexes, obligeant à des formations intenses et exigeantes. Les femmes apprenaient donc à manier des armes à feu, à utiliser des

¹ Boucard, R. (1932). *Les femmes et l'espionnage les dessous de l'expédition en Russie*. AbeBooks. <https://www.abebooks.fr/rechercher-livre/kw/les-femmes-et-l%27espionnage-les-dessous-de-l%27expedition-en-russie/>

¹ Vigurs, K. (2021). *Mission France : The True History of the Women of SOE* (Yale university press). Yale University Press. https://books.google.fr/books?hl=fr&lr=&id=JtAtEAAAQBAJ&oi=fnd&pg=PP1&dq=women+of+SOE&ots=7W2bWWa3I2&sig=4GUW2JGL8Ia5Ds6rI10jtbO7_dU#v=onepage&q&f=false

² *Ibid.*

³ SOE: Special Operations Executive

⁴ Patrick, P. (2024). *Le réseau « Prosper » ou l'énigme du fameux SOE* [Émission]. Consulté 10 mars 2025, à l'adresse <https://www.radiofrance.fr/franceinter/podcasts/rendez-vous-avec-x/rendez-vous-avec-x-du-samedi-22-janvier-2022-4450518>

explosifs et à récolter des informations sur l'ennemi⁵. En tant qu'agents de bureau, opératrices sans fil ou encore agents clandestins⁶, elles vont jouer un rôle majeur pour la résistance française. Ainsi, Andrée Borrel et Lise de Baissac deviennent les premières femmes agents parachutées clandestinement sur le territoire occupé du Nord de la France. Toutes deux vont mener des opérations de sabotage sur les infrastructures allemandes et vont fournir des informations aux réseaux de résistance français, dont le réseau Prosper créé en 1943 par la section française du SOE⁷. Capturée et torturée par la Gestapo, Andrée Borrel, fidèle à la Résistance, refusera de parler et sera exécutée en juillet 1944. Si le courage de certaines a été reconnu et décoré après la guerre, nombreuses demeurent celles étant restées dans l'ombre, occultant l'importance du rôle des femmes des renseignements pour lutter contre l'occupation nazie.

Des espionnes de la SOE parachutées en 1940 et les atouts des femmes dans les renseignements

L'efficacité des femmes dans les renseignements, fut particulièrement reconnue pendant la Seconde Guerre mondiale. En effet, les Allemands se méfiaient moins de la présence des femmes aux alentours des ports, des gares ou près des postes de contrôle ce qui facilita la récolte d'informations avant le débarquement⁸. Le général Jean-Pierre

Meyer, ancien directeur des opérations à la Direction du Renseignement Militaire observe :

« J'ai notamment remarqué que les femmes étaient plus nombreuses que les hommes à ne pas s'arrêter au premier aveu. Plus fines observatrices, elles se laissaient moins prendre aux apparences et tâchaient de découvrir la vérité plus profonde que leur cible pouvait vouloir dissimuler »⁹.

Bien que non exclusives aux femmes, les qualités d'écoute et d'observation sont des atouts majeurs que l'on retrouve plus fréquemment chez elles. Enfin, ce serait une erreur de nier l'efficacité du pouvoir de séduction des femmes lorsqu'il s'agit de récolter des informations chez les hommes. S'il est vrai - comme mentionné précédemment - que la séduction ou la sexualité ne caractérise pas leurs compétences, l'analyse



Source : Vigurs, K. (2021). *Mission France : The True History of the Women of SOE* (Yale university press). [Yale University Press](https://www.yale.edu/library/mission-france).

⁵Keith, K. (2013). *More than just a pretty face*. College of Bowling Green State University.

⁶ *Ibid.*

⁷ Patrick, P. (2024). *Le réseau « Prosper » ou l'énigme du fameux SOE* [Émission]. Consulté 10 mars 2025, à l'adresse

<https://www.radiofrance.fr/franceinter/podcasts/rendez-vous-avec-x/rendez-vous-avec-x-du-samedi-22-janvier-2022-4450518>

⁸ Manokha, I. (2018). Le scandale Cambridge Analytica contextualisé : Le capital de plateforme, la surveillance et les données comme nouvelle « marchandise fictive ». *Cultures et Conflits*, 109, 39-60. <https://www-jstor-org.ezscd.univ-lyon3.fr/stable/26651821?pq-origsite=summon&seq=4>

⁹ K2, C. (2025, mars 4). *Le renseignement et les femmes Cercle K2*. <https://cercle-k2.fr/etudes/le-renseignement-et-les-femmes-3>

comportementale du renseignement humain identifie le sexe comme un levier manipulateur efficace. Qualifiées comme « hirondelles¹⁰ », notamment par le KGB¹¹, ces femmes utilisent leur pouvoir de séduction afin d'entrer dans l'intimité de leurs cibles et recueillir des confidences sur l'oreiller. Les rencontres entre Hitler et Inga Arvad, premier amour de John F. Kennedy qui servait en cette période à l'*Office of Naval Intelligence*, le service de renseignement de l'*United States Navy*, laissaient penser que l'hirondelle Danoise aurait fourni des informations aux Allemands. Cette technique de manipulation par la séduction est appelée « piège à miel¹² ». Un exemple bien connu est celui de l'espionne néerlandaise Mata Hari, danseuse mondialement connue, qui aurait fourni des informations au profit des Allemands en séduisant des politiciens et des officiers français¹³.

Ce type de manipulation est également employé par les officiers traitants lors du recrutement de potentiels agents. Cette stratégie illustre l'utilisation de la manipulation des agents de renseignement selon la matrice théorique MICE¹⁴. Ce principe, développé par les services de renseignement britanniques, identifie quatre leviers sur lesquels un officier traitant peut exercer une influence sur un agent ou une

source. Dans le cas de la manipulation par la séduction, la lettre C soit la coercion ou la compromission est pertinente. Il s'agit de forcer quelqu'un à collaborer en faisant pression sur lui¹⁵. Ainsi, les hirondelles orientent la cible vers une chambre d'hôtel, où des photos sont prises dans le but de lui extorquer des informations en menaçant de les rendre publiques. Cependant, l'ancien directeur de la CIA, Allen Dulles souligne que ce chantage sexuel n'est pas infaillible car il dépend de la perception de l'infidélité selon les sociétés¹⁶. Il souligne notamment que « les citoyens d'un pays où la fidélité conjugale jouit d'une considération certaine et où l'infidélité est fortement désapprouvée par la société sont naturellement des cibles toutes désignées¹⁷ ». Il s'abstient cependant de nommer des pays où l'adultère est jugé avec indulgence afin d'éviter une « controverse internationale sur un sujet aussi délicat »¹⁸.

En plus du chantage sexuel, la flatterie constitue également une méthode courante de manipulation. C'est par son charme que Noreen Riols, auteure de la célèbre citation « les carottes sont cuites¹⁹ », parvient à évaluer la capacité des agents secrets britanniques à garder des informations sensibles sans les divulguer²⁰. Les agents trop bavards étaient envoyés en isolement au Nord de la Grande Bretagne en

¹⁰ Mafart, J. (2018). *Dictionnaire du renseignement*. Perrin. <https://doi.org/10.3917/perri.mouto.2018.01.0446>

¹¹ KGB : *Komitet gossoudarstvennoi bezopasnosti*

¹² Knightley, P. (2010, mars 12). *The History of the Honey Trap*. *Foreign Policy*. <https://foreignpolicy.com/2010/03/12/the-history-of-the-honey-trap/>

¹³ Shipman. (2020, mars 16). *Mata Hari, la femme fatale victime de la Grande Guerre*. National Geographic. <https://www.nationalgeographic.fr/histoire/premiere-guerre-mondiale-espionnage-mata-hari-la-femme-fatale-victime-de-la-grande-guerre>

¹⁴ MICE : Money, Ideology, Compromission, Ego. Acronyme anglo-saxon reprenant les 4 leviers de la manipulation.

¹⁵ Mafart, J. (2018). *Dictionnaire du renseignement*. Perrin. <https://doi.org/10.3917/perri.mouto.2018.01.0446>

¹⁶ *Ibid.*, p.574.

¹⁷ *Ibidem*.

¹⁸ *Ibidem*.

¹⁹ Riols, N. (2022). *Ma vie dans les services secrets : L'espionne de Churchill - Noreen Riols - Tallandier - Poche - Librairie des femmes Paris* (Tallandier). <https://www.librairie-des-femmes.fr/livre/9791021052321-ma-vie-dans-les-services-secrets-l-espionne-de-churchill-noreen-riols/>

²⁰ *Ibidem*.

guise de sanction. En effet, les cibles masculines sont souvent plus enclines à révéler des informations lorsqu'elles sont flattées, notamment par des femmes, se méfiant moins de ces dernières.

Joséphine Baker, une artiste au service de la France libre

Mondialement connue pour ses talents de chanteuse et de danseuse, Joséphine Baker va être recrutée comme agent du contre-espionnage sous les ordres de Jacques Abtey, chef du contre-espionnage militaire à Paris²¹. Sa renommée, va lui permettre de côtoyer de nombreux hommes politiques étrangers, notamment lors de réceptions au sein des ambassades. C'est de cette manière qu'elle va pouvoir récolter des informations sur les intentions de Mussolini. Dans ses mémoires elle témoigne :

« C'est très pratique d'être Joséphine Baker. Dès que je suis annoncée dans une ville, les invitations pleuvent à l'hôtel. A Séville, à Madrid, à Barcelone, le scénario est le même. J'affectionne les ambassades et les consulats qui fourmillent de gens intéressants. Je note soigneusement en rentrant... Ces papiers seraient sans doute compromettants si on les trouvait »²².

En cachant ces informations collectées dans des partitions musicales, elle transmet des informations cruciales sur des stratégies d'officiers allemands. Bien que sa renommée lui permettait de ne jamais éveiller les soupçons, elle va faire preuve d'un courage remarquable en traversant les

frontières à de nombreuses reprises, transportant des informations sensibles. Enrôlée comme infirmière au sein de l'Armée de l'air française, elle va récolter de nombreux renseignements auprès des blessés²³, notamment sur les positions des postes allemands. Après avoir exercé des fonctions d'officier chargée de la propagande, elle obtient le grade de sous-lieutenant. Le 30 novembre 2021, elle est la cinquième femme à rentrer au Panthéon²⁴.

Les femmes ont donc joué un rôle essentiel et souvent sous-estimé dans les services de renseignement français pendant la Seconde Guerre mondiale. Leur engagement, leur courage et leurs compétences ont été cruciaux dans la lutte contre l'occupation nazie, bien que leur travail ait été souvent réduit seulement à des stéréotypes liés à leur apparence physique. Des figures comme Joséphine Baker, Andrée Borrel et Lise de Baissac ont prouvé que, grâce à leur courage, leur intelligence et leur pouvoir de séduction, elles ont pu accomplir des missions d'espionnage cruciales. Leur contribution mériterait d'être davantage reconnue et valorisée dans l'histoire de la résistance.

C.A.



Source : Drogland, J. (2021, novembre 28). *L'engagement patriotique et résistant de Joséphine Baker 1939 – 1945*. [Les Clionautes](https://www.radiofrance.fr/franceinter/podcasts/affaires-sensibles/josephine-baker-1152379).

<https://www.radiofrance.fr/franceinter/podcasts/affaires-sensibles/josephine-baker-1152379>

²⁴ *Joséphine Baker entre au Panthéon*. | *Élysée*. (s. d.). Consulté 10 mars 2025, à l'adresse <https://www.elysee.fr/emmanuel-macron/2021/11/30/josephine-baker-entre-au-pantheon>

²¹ Ibid.

²² Chardonnet, P. (s. d.). *Joséphine Baker, la résistante*. Consulté 10 mars 2025. <https://histoire-vesinet.org/jbaker-resistante.htm>

²³ P. Nottret. (s. d.). *Joséphine Baker, une espionne au service de la France libre* [Émission]. Consulté 10 mars 2025, à l'adresse

Du KGB au SVB/FSR: l'histoire du renseignement de l'URSS à la Fédération de Russie

Auteur : Lou-Ann Lecointre, Mastérante en Relations Internationales, Sécurité et Défense.

A l'origine, tout poussa Eltsine, profondément marqué par les années noires du KGB¹, à empêcher le renouveau d'une institution similaire perçue comme totalitaire par la population, et comme un acteur politique indépendant et imprévisible. Lors de l'effondrement de l'URSS, une des premières mesures d'Eltsine fut donc de cloisonner et de disséminer les compétences de l'ancien KGB. Fut donc créé une myriade de services, qui, par cannibalisme administratif et l'aide présidentielle, ne laissèrent que le SVR² au-devant de la scène interne, le FSB³ pour les affaires internationales, ainsi que le GRU⁴ pour les affaires militaires.

Qualifiés de « nouvelle noblesse »⁵, les services secrets russes n'ont pas renié leur héritage soviétique, et ont même innové, dans une société en transition vers un capitalisme sauvage, où il n'y a plus de place pour les croyances idéologiques socialistes. Contrairement aux services secrets Occidentaux qui ont profondément muté après le 11 septembre 2001, les services russes se posent dans la continuité des tâches de leur ancêtre le KGB⁶. Cela a engendré un brouillage, un flou entre le nouveau et l'ancien service secret russe dans le discours public. Or, les apparences

mises à part, les logiques structurantes se révéleront progressivement divergentes, intrinsèquement liées au contexte du pays modifié par 30 ans d'ouverture au marché, et seront questionnées tout particulièrement les relations entre l'État et le FSB.

Les vestiges du KGB

Lors de la chute de l'URSS, le FSB récupéra du KGB ses missions de contre-espionnage et de lutte contre le terrorisme. Ses missions ressemblaient avant tout à celles du MI5⁷ britannique. De ses prédécesseurs, la première et la cinquième direction du KGB, le FSB avait hérité d'agents formés à l'ancienne, des méthodes soviétiques et surtout, de la croyance tchékiste en une menace⁸, manipulée par l'étranger pour renverser la fédération russe de l'intérieur. Néanmoins, certaines différences étaient déjà présentes : la place du nouveau service dans l'armée avait été amoindrie, de même que la protection des élites, ou encore le champ d'application qui s'est progressivement étendu à l'international, par connexion des menaces de séditions. Plus particulièrement, si le contrôle du KGB se voulait être une surveillance de masse, une ombre omniprésente garante de la société, le FSB va se concentrer sur certaines personnalités

¹ Comité pour la sécurité de l'État

² SVR : Service des renseignements extérieurs de la fédération de Russie

³ FSB : Service fédéral de sécurité de la fédération de Russie

⁴ GRU : Direction générale des renseignements de l'État-Major des Forces armées de la fédération de Russie (ou GU)

⁵ Taylor, Brian D. « The Russian Siloviki & Political Change ». *Daedalus*, vol. 146, n° 2, 2017, p. 53-63.

⁶ Wilde, Gavin. *Hypothesis #2: Bureaucratic Remit and Rivalry Favours Subversion Over War*. Carnegie Endowment for International Peace, 2022, p. 9-12. *JSTOR*, <https://www.jstor.org/stable/resrep45855.7>

⁷ Le Security Service (« Service de la sûreté »), communément dénommé MI5 (pour Military Intelligence, section 5)

⁸ Dziak, John J. *Chekisty: a history of the KGB*. Lexington Books, 1988.

actives en politique ou notoirement opposées au régime, matérialisation de cette peur de déstabilisation interne. Ses moyens seront considérés comme plus subtils, on passera par un proche de la personne visée, plutôt que d'envoyer directement un avertissement. Et cela dans des sphères variées, notamment culturelle ou scientifique, car le monde des danseurs, artistes, comédiens, ainsi que les élites de l'*Intelligencia* sont perçus comme ayant accès à des informations qui pourrait porter atteinte à la légitimité du régime et alimenter les avis licencieux⁹. Les mesures apparaissent davantage sécuritaires. Enfin, un point crucial de l'évolution du FSB sous Vladimir Poutine va être la question du contrôle civil sur le service. Si Eltsine a tout fait pour limiter le pouvoir du FSB personnellement, il l'a privé - si ce n'est « préservé » involontairement - d'un contrôle externe. Et ainsi, cette surveillance du service devient hiérarchique, unilinéaire et interne, contrairement à l'époque soviétique durant laquelle le KGB était encadré par différents organes du parti. Andropov, grande figure soviétique, et qui a aidé à améliorer l'image du KGB lors de son déclin, n'était pas un officier, mais un officiel du parti, contrairement à aujourd'hui où il s'agit exclusivement d'officiers subordonnés au président, à la tête de l'organigramme obscure du FSB¹⁰. L'institution devient opaque¹¹, au grand malheur des réformateurs démocrates du début des années 1990 qui avaient espéré y insuffler transparence et respect de l'État de droit. Cette problématique, similaire à celle de l'armée rouge du Parti communiste

chinois, va entraîner une corruption endémique des services secrets russes.

La déliquescence des services

Pour revenir à l'origine de cette corruption, il faut se placer dans le milieu des années 1990, où beaucoup d'agents ont vécu le changement de régime comme une perte personnelle. Auparavant, la loyauté, outil central du bon fonctionnement du KGB, était assurée par la menace des purges, mais aussi les conditions matérielles offertes dans l'économie atrophiee soviétique. Par exemple, les maisons le long de la Roubliovka étaient la propriété du KGB et étaient allouées à ses membres, mais l'organisation pouvait tout aussi vite les reprendre. Dans l'époque post-soviétique, ce confort a disparu et les officiers de l'ex-KGB se retrouvent à l'arrière de la scène, dans l'ombre des oligarques. Au départ, ces officiers, qui ont servi de figures structurantes lors du changement de régime, ont facilité les ventes aux enchères et acquisitions bancaires à leurs amis. Il y avait un véritable microcosme entre ces différents agents, dont certains s'étaient lancés dans les affaires, saisissant l'opportunité de l'ouverture du marché. Mais progressivement, ils ont été mis dans l'ombre des nouveaux riches. Forts de leurs compétences dans les services de protection et d'espionnage, ils ont trouvé par opportunisme de nombreux employeurs dans les secteurs industriels compétitifs, notamment chez ceux dont les affaires avaient tendance à cette période à dérapier violemment¹². Les fusillades remplaçaient

⁹ Fedor, Julie. *Russia and the Cult of State Security: The Chekist Tradition, from Lenin to Putin*. Routledge, 2011.

¹⁰ Alexandre Adler "Andropov, le KGB au pouvoir" et le "Chant du cygne du KGB" *Les nuits de France culture*, 4 mars 2019

<https://www.radiofrance.fr/franceculture/podcasts/les-nuits-de-france-culture/histoire-et-histoires-histoires-d-espionnage-sovietique-8-8-partie-9-andropov-le-kgb-au->

[pouvoir-partie-10-la-chute-du-mur-le-chant-du-cygne-du-kgb-1ere-diffusion-31-08-2000-et-01-09-2000-4285816](https://www.radiofrance.fr/franceculture/podcasts/les-nuits-de-france-culture/histoire-et-histoires-histoires-d-espionnage-sovietique-8-8-partie-9-andropov-le-kgb-au-pouvoir-partie-10-la-chute-du-mur-le-chant-du-cygne-du-kgb-1ere-diffusion-31-08-2000-et-01-09-2000-4285816)

¹¹ Bakatin, V. V. *Route vers le Passé. Vtoroe, Pererabotannoe i dopolnennoe izdanie, TSentrpoligraf*, 2015.

¹² Albin, Joseph L., et Julie Anderson. « Whatever Happened to the KGB? » *International Journal of Intelligence and Counter Intelligence*, mars 1998. world,

parfois la concurrence pure, les gardes du corps étaient donc très prisés.

Il y a donc eu une reconversion massive des agents, pour vendre leurs services de protection mais aussi pour leurs annuaires tentaculaires de contacts qu'ils avaient acquis par leur activités d'espionnage. À l'inverse, il y a eu une grande apathie de la part de ceux restés loyaux à l'État, qui ne travaillaient plus que dans des conditions miséreuses. Cette commercialisation des compétences se faisait évidemment en parallèle d'un emploi au FSB, ce qui posa, comme pour la « réserve active », des problèmes de loyauté.

En effet, la réserve active est un phénomène constant, mais qui prend de l'ampleur dans les années 2000. Sous la présidence de Vladimir Poutine, de nombreux officiers à la retraite - ou pas - ont infiltré les affaires, ou encore les médias. Par exemple, Zdanovitch, ex-chef du service de presse du FSB, se retrouve à la tête du plus grand service télévisé du pays. Ce proche du Chef du Kremlin a évidemment commencé à redorer l'image du KGB et du nouveau FSB, tout en imposant le narratif officiel¹³, notamment pour la tragédie de Beslan¹⁴. Par ailleurs, par son rôle de contre-espionnage, le FSB put s'immiscer dans de nombreux litiges économiques, notamment lorsqu'il obtint le droit de s'immiscer dans les affaires pénales. Mais tous n'ont pas été envoyés à de tels postes, ni ne gardèrent une telle allégeance. En raison du système de paie de ces agents, ceux-ci changèrent très vite de loyauté. En effet, l'agent recevait un double

salaires. Si le salaire versé dans le privé était inférieur à celui versé par le FSB, il pouvait garder la différence, mais si le salaire de l'État était inférieur, ce qui était souvent le cas, l'agent devait reverser la différence avec son salaire privé. Beaucoup ont donc officiellement démissionné tout en gardant leur fonction d'agent. Mais cela a fait évoluer leur fonction originelle, les agents se muant en représentants des affaires au sein du FSB, que de véritables outils de surveillance et de contrôle de ces mêmes entreprises. Ce fut une grande crainte pour certains agents, notamment V. Tcherkessov, qui disait : « La caste se détruit de l'intérieur quand les guerriers deviennent des commerçants »¹⁵.

Il y a donc eu un processus à double finalité dans les sphères privées avec des accusations à tout-va, notamment dans des centres de recherche, où tout lien avec l'Occident servait de base d'accusation d'espionnage industriel et scientifique. Jamais le concept de « sécurité nationale » n'avait été aussi large¹⁶. Cela permettait, soit de libérer une place pour y placer un nouveau membre du FSB, soit de gagner en interne une promotion, même si cette accusation était souvent montée de toute pièce. La justice ne donne presque jamais raison à une requête à l'encontre des constats du FSB. Il n'y eut jamais de véritable prise, mais cela entretenait le climat de paranoïa. Le revers de la médaille fut que des officiers relativement médiocres furent promus à des postes élevés. Ces derniers, de la vieille génération, ne s'étaient pas montrés assez compétents pour être recrutés par le privé, mais forment

www.tandfonline.com,

<https://doi.org/10.1080/08850609808435363>.

¹³ « Des amis hauts placés ». *Les héritiers du KGB : enquête sur les nouveaux boyards*, par Andreï Soldatov et al., Nouveau monde éditions, 2022.

¹⁴ En 2004, une prise d'otage dans la plus grande école de Beslan tourne au drame, quand une explosion à l'origine inconnue provoque un mouvement de panique chez les enfants, qui sont fusillés par les preneurs d'otages. On

jugera l'intervention par la suite des forces spéciales particulièrement chaotique, tandis qu'en 2017, la Cour Européenne des Droits de l'Homme condamne la Russie pour son manque de diligence pour éviter le massacre.

¹⁵ « Des amis hauts placés ». *Les héritiers du KGB : enquête sur les nouveaux boyards*, par Andreï Soldatov et al., Nouveau monde éditions, 2022.

¹⁶ Waller, J. Michael. *Secret empire: the KGB in Russia today*. Westview Press, 1994.

aujourd'hui une part de l'entourage et des conseils du chef de l'exécutif, ayant la main sur les ressources héritées du KGB.

Le retour de l'Institution

Le nouveau chef du Kremlin va progressivement remettre au-devant de la scène le FSB. Vladimir Poutine, après avoir été agent du KGB en Allemagne, a eu un poste dans gouvernement de Saint-Pétersbourg, l'un des plus liés avec la pègre. Beaucoup d'agents y vendaient leurs services sous prétexte « d'infiltration » dans le crime organisé. Il connaît donc bien les ressorts et préfère les employer à son avantage, en utilisant l'argent issu de ce rapprochement avec le marché noir pour des mesures populistes, s'attirant ainsi la sympathie de l'opinion publique. En parallèle, une tendance à la création d'institutions internes, entamée depuis les années 1990 permet au FSB de surpasser ses prérogatives constitutionnelles. Inéluctablement, le FSB reprend la place de « *superagency* » qu'avait autrefois le KGB¹⁷. En 2004, un décret présidentiel, où le sommet du FSB a pu donner son avis, donnait une capacité d'auto gouvernance au FSB, un État dans l'État, lui permettant d'intervenir dans toutes situations¹⁸. Accompagné de son indépendance économique, ce décret a permis aux agents de s'impliquer dans l'économie et la politique à bras le corps.

Problématique inhérente au nouveau service

Mais cette expansion de pouvoir et de capacités a mené à la corrosion de la mission originelle, voulue par Eltsine, 35

ans après. Le FSB n'est certainement pas devenu monolithique, empêtré dans des conflits internes ; une grande rivalité est née au sein du service, aussi bien à cause des conflits d'intérêts que des rivalités encouragées par le Président.

Premièrement, l'imbrication entre monde du renseignement et entreprises privées conduit le FSB à devenir un lieu de lobbying au profit des grandes compagnies russes. Chaque groupe privé a son agent du FSB pour porter sa voix.

Deuxièmement, la question de la loyauté est devenue une véritable source de tension entre les anciennes et nouvelles générations. En effet, les plus vieux officiers, jugeant mériter, au vu de la décennie catastrophique des années 90, certains privilèges, et le gouvernement souhaitant acheter leur loyauté, il y a eu une vente massive des maisons le long de la Roubliovka, à prix bradés¹⁹. Mais que restait-il pour acheter la fidélité des nouveaux agents ? L'administration des services secrets se retrouvera bientôt face à cette question, alors que la plupart de l'ancienne génération arrive bientôt à la retraite.

Troisièmement et finalement, la place centrale qu'a prise le FSB en fait une clé de voûte, dont l'effondrement pourrait avoir des risques systémiques. En effet, si le contrôle du FSB se fait par le Président et son Conseil de Sécurité, Vladimir Poutine s'est toujours assuré de mettre en balance chacun de ses officiers avec un autre. Le FSB a évolué en une agence où une opération manquée, causant la mort de plusieurs centaines de personnes, n'est pas réprimée, là où une émeute contre le

¹⁷ Council, Atlantic. *LUBYANKA FEDERATION: How the FSB determines the politics and economics of Russia*. Atlantic Council, 2020. JSTOR, <https://www.jstor.org/stable/resrep26691>.

¹⁸ Presidential Decree of the Russian Federation N 807 of June 11, 2004, "On issues of the Federal Security Service

of the Russian Federation," President of Russia https://www.consultant.ru/document/cons_doc_LAW_48357/.

¹⁹ Borogan, Irina. *Les Tchékistes travaillent comme des forçats*. Novaïa Gazetta, 2006.

pouvoir non anticipée peut coûter des carrières²⁰. Avant tout devenue une garde pour le gouvernement et tout particulièrement pour le Président, le FSB est tout autant dépendant de ce gouvernement. Le Président l'emploie pour redistribuer les ressources économiques à ses favoris, prenant bien soin de montrer une image paisible et libérale de l'économie russe afin de ne pas couper ses liens avec l'économie occidentale²¹. Il faut garder à l'esprit que le libéralisme économique, lié aux démocrates, est vivement critiqué et détesté par le microcosme de l'ex-KGB. Poutine en est le parfait produit de l'époque et il souhaite donc l'éviter à tout prix. En parallèle, le président se montre en arbitre entre les différents services du FSB et entre le FSB et les personnalités privées, demandant des services. Il souhaite justement imposer plus de communication avec les membres du FSB à tous les échelons, mais dans cette guerre de clans administratifs, c'est souvent le premier qui atteint l'oreille de l'arbitre avec sa propre

version qui l'emporte. Cela entraîne évidemment un biais dans les récits que le Président entend, qui sont nombreux, mais jamais véritablement corrects.

Pour finir, la vitesse de développement de ce second gouvernement, qui s'isole en maintenant son pouvoir sur la société, génère une grande inquiétude : quelle est la capacité de résilience de ce système en cas de changement du pouvoir gouvernemental ? Aujourd'hui incarné par Vladimir Poutine, mais en 1953 incarné par Staline, le système qui avait écarté toutes les autres agences étatiques avait dû faire face à beaucoup de tumultes après la mort de son *leader* initial. Les soubresauts de la chute n'avaient pas été sans conséquences pour la société russe de l'époque²².

L.-A.L.

²⁰ *La justice a amnistié les policiers de Beslan* Novaïa Gazzetta, 29 mai 2007

²¹ Avant les événements en Crimée de 2014

²² Council, Atlantic. *LUBYANKA FEDERATION: How the FSB determines the politics and economics of Russia*. Atlantic Council, 2020. JSTOR, <https://www.jstor.org/stable/resrep26691>.

Les cinq de Cambridge

Auteurs : Julien Allo Masterant en Relations Internationales, Francophonie et Transition Écologique et Lalie Pasquet Masterante en Relations Internationales et Diplomatie.



Kim Philby (à droite) en 1955 après l'éclatement de l'affaire Mclean et Burgess alors que l'étau se resserre autour de lui, [Skynews](#)

Le XX^{ème} siècle, marqué par des bouleversements politiques et idéologiques majeurs, a également été le théâtre d'intenses guerres d'espionnage. Parmi les figures les plus emblématiques de cette lutte figurent les Cinq de Cambridge, plus connus sous le nom de « Magnificent Five ». Ces hommes sont parvenus à infiltrer les plus hautes sphères des institutions britanniques, permettant ainsi de transmettre des informations sensibles à l'Union soviétique.

Origine et recrutement

Les Cinq de Cambridge étaient un groupe d'hommes ayant étudié à l'université de Cambridge pendant l'entre-deux-guerres. Ce cercle était composé de Kim Philby, Anthony Blunt, Guy Burgess, John Cairncross et Donald Maclean. Issus de l'élite anglaise¹, ils ont été approchés par l'Union soviétique dans un contexte où, avec la crise économique de 1929, qui a frappé les classes populaires anglaises et a facilité la montée des mouvements fascistes en Europe, un profond désir de changement se dessine parmi la jeunesse intellectuelle².

¹ O. Neuray, V. Lemaire (2021), *Les cinq de Cambridge*, Casterman, p. 3

² *Ibid.*, p. 3

En effet, pour certains qui percevaient le monde comme figé, ou pour d'autres qui voyaient un déclin de l'Occident, le socialisme soviétique représentait alors une alternative au modèle de vie collective.

Ainsi, un engouement pour cette idéologie s'est développé au sein de l'université anglaise, notamment au travers d'espaces de discussion et d'idéalisation du communisme qui apparaissait comme « un rempart contre la montée du totalitarisme³ ». L'Union soviétique y voit alors une opportunité de renforcer son réseau d'espionnage.

Arnold Deutsch, agent du NKVD (la police politique et de sécurité de l'Union soviétique), décide de cibler Cambridge pour le recrutement d'espions. Il était à la recherche d'individus capables « de pénétrer les institutions bourgeoises⁴ », tout en utilisant le communisme comme une « fantaisie passagère de la jeunesse⁵ ». En 1934, le premier à être recruté est Kim Philby, devenu à son tour un agent de recrutement pour le compte du NKVD. C'est ainsi qu'il est parvenu à rallier Donald Maclean, Guy Burgess, Anthony Blunt et John Cairncross à la cause soviétique. Afin d'éviter tout soupçon, il leur est demandé de se tenir à l'écart du Parti communiste de Grande-Bretagne, à l'exception de Maclean qui y était déjà engagé avant son recrutement⁶.

Les cinq hommes vont alors réussir à infiltrer presque toutes les institutions majeures du gouvernement britannique, et notamment, le Secret Intelligence Service (SIS), le Security Service (MI5), le Foreign Office, le Ministère des Finances et enfin, Bletchley Park, le centre de décryptage du code Enigma. Leur infiltration est alors facilitée par le manque de rigueur des politiques de recrutement qui sont basées sur la croyance selon laquelle les hommes de bonne souche sont irréprochables⁷. À titre d'exemple, Maclean a été recruté au Foreign Office, où il va avoir un accès illimité à des informations sensibles, alors qu'il est de notoriété publique, communiste et investi dans le Parti communiste de Grande-Bretagne⁸.

Espionnage de grande ampleur

Les cinq hommes réussirent à dérober et transmettre à l'Union soviétique de nombreux secrets et informations cruciales, allant des stratégies de guerre à la recherche atomique, en passant par les opérations des services secrets britanniques.

Maclean, après avoir rejoint le Foreign Office en 1935, est affecté à l'ambassade de Washington. Il avait alors accès à des détails hautement confidentiels, notamment sur les armes nucléaires, sur les discussions anglo-américaines, la quête de la bombe atomique ainsi que la stratégie nucléaire américaine. Ses rapports ont permis à l'URSS d' « ajuster ses propres

³ *The Cambridge Five : The British elites who spied for the Soviets.* (s. d.). History Skills. [En ligne]. Consulté le 10 mars 2025. Disponible sur : <https://www.historyskills.com/classroom/year-10/cambridge-five/?srsltid=AfmBOopiRRCrttGIBSW8iinsLSE0G-o1gpv65SIAiGNMODCFGa0b4zrW>

⁴ McComas, Jenna G. *The Cambridge Five Spy Ring: The Notorious Bane of the British Government.* Young Historians Conference, Portland State University, 2024, p. 1

⁵ *Ibid.*, p. 2

⁶ *Ibid.*, p. 3

⁷ *The Cambridge Five : The British elites who spied for the Soviets.* (s. d.). *op.cit.*

⁸ Drouelle, F. (2021). Les cinq de Cambridge (1). *France Inter.* [En ligne]. Consulté le 3 mars 2025. Disponible sur : <https://www.radiofrance.fr/franceinter/podcasts/affaires-sensibles/affaires-sensibles-du-jeudi-23-decembre-2021-3080100>

stratégies nucléaires, égalisant les chances dans la course aux armements⁹».

Guy Burgess, en tant que secrétaire d'Hector McNeil, ministre d'État des Affaires étrangères, fournissait à l'URSS des éléments clés sur les positions et stratégies diplomatiques occidentales¹⁰.

Kim Philby, après une carrière au journal *Times*, intègre le Secret Intelligence Service où il devient responsable de la « section URSS¹¹ ». Recrutant des taupes pour le Royaume-Uni, puis, devenant chef de liaison pour le SIS, il révéla des détails sur l'opération « *Valuable* » qui consistait à renverser le régime soviétique en Albanie et qui se solda par un échec.

Blunt, recruté au MI5, était chargé de la rédaction du manuel des procédures de l'organisation. Il transmet l'intégralité de ce document aux Soviétiques, offrant ainsi un aperçu du contre-espionnage britannique.

Enfin, Cairncross infiltra Bletchley Park et permit à l'URSS d'obtenir des informations clés sur les préparatifs de la Luftwaffe en amont de la bataille de Koursk en 1943.

En tout, il est estimé que près de 20 000 pages de documents classifiés ont été transmises à l'URSS grâce à ce réseau d'espions¹². Ces révélations ont donné à l'URSS un avantage stratégique

considérable sur les intentions et capacités de ses adversaires occidentaux.

Découverte et chute du réseau

Comment le pot aux roses a-t-il été découvert ? À partir de 1948, le MI5 soupçonnait déjà la présence d'espions au sein de l'agence. Cependant, ce n'est qu'en 1951 que les suspicions se révèlent fondées à travers le décryptage du code Venona, code qu'utilisent les soviétiques pour crypter leurs télégrammes¹³. Ce projet mené conjointement par les Américains et les Anglais à travers les Five Eyes permit l'identification d'un certain Homer, un agent opérant au sein des services secrets britanniques¹⁴. Homer est en réalité le nom de code de Maclean, ce que comprend rapidement Philby, intégré à l'affaire, et, qui l'avertit avant qu'il ne soit découvert¹⁵. Aux côtés de Burgess, celui-ci s'exfiltra alors vers la France à bord d'un cargo polonais et prit la fuite vers l'URSS¹⁶.

Philby s'inquiète à son tour. Pourtant, proche de James Angleton, directeur du service de contre-espionnage américain, celui-ci échappe aux soupçons¹⁷. De surcroît, le renseignement britannique ne pouvait croire que Philby soit l'informateur secret de Maclean et Burgess¹⁸. La pression des journalistes, du FBI et de la CIA étant trop forte, Philby n'avoua sa double vie que quelques années plus tard après sa démission. Néanmoins,

⁹ *The Cambridge Five : The British elites who spied for the Soviets*. (s. d.). *op.cit.*

¹⁰ *Ibid.*

¹¹ Boulanger, P.(2023) . KAUFFER Rémi : Les espions de Cambridge. Cinq taupes soviétiques au cœur des services secrets de Sa Majesté ; Éditions Perrin, 2022, 384 pages. *Revue Défense Nationale*, N° 858(3), p. 132.

¹² Drouelle, F. (2021). Les cinq de Cambridge (1), *op.cit.*

¹³ *Les Cinq de Cambridge (Magnificent Five)*. (s. d.). Histoire pour Tous | de France et du Monde. <https://www.histoire-pour-tous.fr/dossiers/3656-les-cinq-de-cambridge.html>

¹⁴ McComas, Jenna G. *The Cambridge Five Spy Ring: The Notorious Bane of the British Government*, *op.cit.*

¹⁵ *Ibid.*

¹⁶ *Les cinq de Cambridge : la gentry au service du KGB*. (s. d.). Point de Vue. <https://www.pointdevue.fr/histoire/histoire-du-monde/les-cinq-de-cambridge-la-gentry-au-service-du-kgb>

¹⁷ McComas, Jenna G. *The Cambridge Five Spy Ring: The Notorious Bane of the British Government*, *op.cit.*

¹⁸ *Ibid.*

l'homme affirme qu'il ne fut en activité que de 1936 à 1946, un mensonge que le renseignement britannique accepte, ce qui permit à l'agent de prendre la fuite vers l'URSS le 1^{er} juillet 1963¹⁹.

La réelle identité de Blunt ne fut révélée au grand public qu'en 1979²⁰. Dénoncé par un étudiant recruté des années plus tôt, Margaret Thatcher le fustiga ouvertement et lui retira toutes ses distinctions²¹. Quant à Cairncross, le gouvernement britannique dissimula son identité jusqu'à sa mort.

Impacts et répercussions

Ce scandale fait office d'onde de choc au sein des services de renseignement britanniques. Tout d'abord, cela a remis en cause la crédibilité du MI5 et du MI6 à l'époque²². Comment des agents soviétiques ont-ils pu accéder à des fonctions si élevées dans l'appareil démocratique britannique ? Une forme de paranoïa s'est par la suite installée au Royaume-Uni : les procédures de recrutement ont été modifiées, tout comme le protocole de sécurité interne qui a été renforcé²³. Un « club des cinq, nouvelle génération » serait en effet inacceptable.

Alors que cette affaire a révélé au grand jour les vulnérabilités des services secrets britanniques pendant la guerre froide, la confiance qui régnait entre le MI5 et le MI6 a été entachée²⁴. De la même manière, la CIA se montra bien plus réticente à partager des informations avec les Anglais, notamment au sujet du nucléaire, ne souhaitant pas que les soviétiques s'en saisissent²⁵.

De nos jours, cet épisode semble attiser la curiosité d'un certain public. En effet, cette affaire a déjà été adaptée au grand écran avec des films comme *Tinker, Tailor, Soldier, Spy* (1979) ou *A question of Attribution* (1991)²⁶, ce qui illustre l'intérêt toujours aussi vif pour cette affaire. Malgré tout, certains historiens estiment que ce scandale ne se limiterait pas seulement à cinq agents mais bien plus, ce qui expliquerait notamment leur recrutement au sein du renseignement britannique²⁷, preuve que cette affaire n'a peut-être pas encore révélé tous ses secrets.

J.A., L.P.

¹⁹ *Ibid.*

²⁰ *Les Cinq de Cambridge (Magnificent Five)*. Histoire pour Tous, *op.cit.*

²¹ *Ibid.*

²² *The Cambridge Five : The British elites who spied for the Soviets.* (s. d.). History Skills. <https://www.historyskills.com/classroom/year-10/cambridge-five/?srsltid=AfmBOopiRRCrttGIBSW8iinsLSE0G-o1gpv65SIAiGNMODCFGa0b4zrW>

²³ *Ibid.*

²⁴ YL Yeung, I. (2007, février). *The Cambridge Spy Ring : its creation, significance, and effects on Britain and the*

West.

https://www.researchgate.net/publication/347934456_The_Cambridge_Spy_Ring_its_creation_significance_and_effects_on_Britain_and_the_West

²⁵ *Ibid.*

²⁶ Willmets, S., & Moran, C. (s. d.). Filming Treachery : British Cinema and Television's Fascination with the Cambridge Five. *Journal of British Cinema and Television*, 10(1).

²⁷ *Les Cinq de Cambridge (Magnificent Five)*. Histoire pour Tous, *op.cit.*

Le rôle du renseignement dans la non-prolifération nucléaire à travers l'exemple irakien

Auteur : Alice Caussou, Mastérante en Prévention et Gestion des Risques.

Le Livre blanc sur la défense et la sécurité nationale français, publié en juin 2008, identifie le système international multipolaire « incertain et imprévisible¹ » comme menace stratégique, en insistant particulièrement sur les risques sécuritaires liés à la prolifération nucléaire. Le document souligne en outre combien la connaissance et l'anticipation s'imposent comme des impératifs majeurs, faisant du renseignement un levier essentiel pour maîtriser les menaces et orienter les choix stratégiques de la Nation. À ce titre, il estime nécessaire à l'efficacité de la lutte contre la prolifération nucléaire une coopération opérationnelle incluant les services de renseignement.

Il convient en ce sens d'opérer une distinction cruciale entre ceux que nous désignons « services de renseignement » et les acteurs internationaux de la lutte contre la prolifération, institutions qui porteront toutes deux la structure de cet article.

Il est ainsi communément entendu par « Renseignement » les services nationaux de renseignement œuvrant à la recherche et l'analyse d'informations afin de prévenir les atteintes aux intérêts de la Nation². Leur mission diffère donc largement de celle d'institutions

internationales dont, si la mission est elle aussi la collecte d'informations, l'objectif recherché est la préservation de la sécurité internationale nucléaire. La différence du champ de compétence octroyé à chacun impose une certaine rigueur de terminologie, illustrée dans cet article par l'utilisation succincte de « renseignement » (qualifiant la mission des services nationaux) et « vérification » (qualifiant celle de l'Agence Internationale de l'Énergie Atomique, organisation internationale chargée du contrôle du respect du TNP par le biais d'inspections).

Leur implication certes différente mais commune dans la lutte contre la prolifération nucléaire invite à s'interroger quant à leur rôle dans la reconnaissance de la primordiale de la collecte d'information dans le maintien d'une sécurité nucléaire. L'affaire des armes de destruction massive en Irak offre, justement, un cadre d'étude pertinent dans l'appréhension des enjeux liant renseignement et non-prolifération.

« I feel impelled to speak today in a language that in a sense is new (...) That new language is the language of atomic warfare³. »

En adressant devant l'assemblée générale des Nations-Unies son célèbre

¹ Présidence de la République. (2008). *Livre blanc sur la défense et la sécurité nationale 2008*. Paris : Odile Jacob.

² De Bousquet, P. (2019). *Stratégie Nationale du Renseignement*.

³ Eisenhower, D. D. (1953, 8 décembre). *Atoms for Peace*. Assemblée Générale des Nations Unies, New York, États-Unis.

discours « Atoms for Peace » le 8 décembre 1953, le président américain Eisenhower défend, dans un monde instable marqué par la course aux armements nucléaires, un usage pacifique de l'atome à des fins strictement civiles. Il pose ainsi les jalons de la création de l'Agence internationale de l'énergie atomique (AIEA), institution spécialisée liée à l'Organisation des Nations unies (ONU) et qui porte, depuis 1957 et jusqu'à aujourd'hui, la lutte contre la prolifération nucléaire à des fins militaires.

Cette mission est entérinée et substantiellement renforcée lorsque les négociations internationales aboutissent enfin, en 1968, à la signature du Traité de non-prolifération nucléaire (TNP), qui confère à l'AIEA un droit de regard sur les États signataires non dotés de l'arme nucléaire, dits ENDAN, afin d'assurer leur usage strictement civil et pacifique du nucléaire. Ils s'engagent ainsi, par leur signature au TNP, à conclure avec l'Agence un accord de garanties généralisées, instrument légal contraignant facilitant ses mesures de contrôle effectif.

Des vulnérabilités structurelles révélées par le programme nucléaire irakien

En 1991, en même temps que s'achève la première guerre du Golfe, le monde prend conscience de l'ampleur du programme nucléaire militaire irakien.

Dans les années 1980, l'Irak de Saddam Hussein avait initié des programmes de recherches en vue de développer une bombe au plutonium ; pour autant, les ambitions irakiennes dans le

secteur du nucléaire remontent à quelques dizaines d'années auparavant. Dans le cadre d'une coopération avec les États-Unis, puis avec l'Union Soviétique, puis enfin avec la France, Bagdad avait poursuivi un programme de réacteurs dont l'objectif officiellement annoncé était le développement d'une filière nucléaire civile, permettant de subvenir à ses besoins énergétiques une fois ses réserves de pétrole écoulées⁴.

Pourtant, la défaite irakienne face aux forces de la coalition en février 1991 et l'adoption subséquente de la résolution 687 au Conseil de sécurité des Nations unies ont permis à l'AIEA, accompagnée de la Commission spéciale des Nations unies (UNSCOM), d'explorer les plans d'arsenalisation des matières nucléaires en Irak. Ces inspections révèlent alors l'existence d'un programme nucléaire militaire dont les moyens de dissimulation démontraient une exploitation maîtrisée des failles des moyens de renseignement internationaux – notamment en matière de garanties nucléaires⁵.

L'AIEA traverse alors une crise d'une ampleur conséquente, pointée du doigt par l'opinion publique internationale pour n'être parvenue à entraver ces activités clandestines ; ceci alors même que l'Irak, signataire au TNP, en recevait les inspecteurs deux fois par an au titre de son accord de garanties.

L'incapacité de l'AIEA à produire un travail de renseignement en profondeur

⁴ Saint-Mleux, M. (2004). Le nucléaire en Irak. *Politique Étrangère*, 69(1), 53-65.
<https://doi.org/10.3406/polit.2004.1268>

⁵ Les Irakiens ont notamment eu recours à la méthode du double usage, qui consiste à dissimuler l'activité nucléaire

militaire illégale derrière une activité nucléaire civile qui serait elle légale, en employant des équipements à double usage (civil et militaire).

Le caractère même de son mandat bridait sans nul doute le champ de compétence dont disposait l'Agence. Ses mécanismes de contrôle dépendent ainsi autant de la bonne volonté que de la bonne foi des États parties.

Le professeur Grümme, ancien directeur général adjoint chargé du Département des garanties de l'AIEA, observait déjà lors de l'opération Opéra – menée par l'armée israélienne aux fins de détruire le réacteur nucléaire irakien Osirak – des complexités dans la capacité de son département à exercer la mission de surveillance qui lui avait été confiée une dizaine d'années auparavant⁶.

En tant qu'organisation internationale, l'AIEA ne disposait effectivement d'aucune capacité autonome de renseignement comparable à celle des États : la mise en œuvre de son contrôle était ainsi conditionnée par la conclusion d'accords de garanties entre l'Agence et un État qui, bien que signataire au TNP, demeure souverain.

En outre, une seconde barrière s'ajoutait à l'effectivité des inspections internationales, que le professeur Grümme relevait également : « le risque de prolifération le plus grand se situe hors du champ d'application des garanties⁷ ». Le choix des installations nucléaires soumises aux accords de garantie relevant de la souveraineté de l'État, les inspecteurs ne pouvaient donc accéder aux installations présentant un réel risque de prolifération.

L'Irak comme vecteur du repositionnement stratégique renseignement - non-prolifération

Le cas irakien sonna le signal d'alarme des paradoxes auxquels faisait face l'AIEA, mais il fut aussi une prise de conscience collective quant à la possibilité pour un État de dissimuler avec succès ses installations nucléaires. Dès 1997 a donc été décidé l'augmentation des moyens alloués à l'Agence, mais surtout l'octroi de plus de prérogatives en matière d'inspection par l'adoption du Protocole additionnel pour la vérification de garanties.

Ce protocole additionnel permet de fait à l'AEIA un contrôle plus extensif et facilité : il autorise ses inspecteurs à approcher et collecter davantage d'informations avec les États choisissant d'en conclure. De surcroît, il permet à l'Agence d'accéder à un nombre plus extensif de localisations tout en lui conférant la possibilité d'agir sur des soupçons bien moindre⁸.

Dans le même temps, les États – dont les services de renseignement surveillaient déjà les programmes nucléaires étrangers – prirent plus amplement conscience des enjeux posés par la prolifération verticale, et la nécessaire dépendance à leurs propres capacités de renseignement pour protéger leurs intérêts nationaux face à cette menace⁹.

La crainte de la prolifération nucléaire, moteur du Renseignement stratégique

⁶ Grümme, H. (1982). Possibilités et limites des garanties internationales. *Bulletin de L'AIEA*, 40-43.

⁷ Grümme, H., *op.cit.*

⁸ Gibbons, R., & Robinson, T. (2021). Twenty-five years safer? Assessing the IAEA's Model Additional Protocol and its role in international politics. *The Nonproliferation*

Review, 28(4-6), 297-318. <https://doi.org/10.1080/10736700.2022.2064516>

⁹ Delpech, T. (2003). Armes de destruction massive : à quoi sert le renseignement. *Critique internationale*, no 20(3), 18-27. <https://doi.org/10.3917/cii.020.0018>.

En 2003, la politiste française Thérèse Delpech faisait déjà remarquer que le caractère par nature clandestin de l'armement nucléaire, lié à l'impératif de sécurité nationale qu'est l'anticipation des risques nucléaires, impose un renseignement poussé pour assurer les normes de non-prolifération¹⁰.

Dans les années 2000/2010, la préoccupation particulière d'un nombre grandissant d'États quant à la menace de la prolifération des armes de destruction massive, comme exposé dans le Livre blanc de la France de 2008, mais aussi repris dans celui de 2013, fut moteur de l'accroissement d'un rôle spécifique du Renseignement dans la lutte contre la prolifération nucléaire et la surveillance de programmes pouvant être considérés comme portant atteinte aux intérêts fondamentaux de la Nation.

L'inquiétude suscitée par la découverte tardive du programme nucléaire irakien est donc à directement lier à une recrudescence de l'investissement par les États dans leurs services de renseignement et leur rôle dans la surveillance nucléaire. La France, dans la continuité des préoccupations énoncées par le président de la République dans le Livre Blanc de 2008, a institué en 2015 le Service de contre-prolifération au sein de la direction générale de la Sécurité extérieure (DGSE), consacré à la surveillance étrangère du développement de programmes nucléaires militaires chez les ENDAN.

La DGSE couvre ainsi aujourd'hui l'ensemble du « spectre NRBC » (nucléaire, radiologique, biologique, chimique) des armes de destruction massive¹¹ : elle permet à la France d'identifier les États représentant une menace nucléaire potentielle ou avérée. Le 29 novembre 2024, son patron Nicolas Lerner annonçait de ce fait la prolifération atomique en Iran comme « menace critique¹² ».

Le cas irakien demeure donc pertinent afin d'analyser correctement les enjeux qu'entraîne une connaissance accrue de la présence d'armes de destruction massive dans un territoire hostile. Reposent en effet sur la conjoncture nucléaire irakienne non seulement la garantie du statu quo du nucléaire iranien, mais aussi l'éventualité d'un désarmement israélien ; c'est en effet sur la garantie de l'absence d'armes de destruction massive sur le sol irakien que la communauté internationale espère dissuader l'Iran de développer son propre programme tout en convaincant Israël d'abandonner le sien, en l'absence de menace à ses intérêts. Sur la qualité du renseignement reposent donc les auspices de la contre-prolifération au Proche-Orient.

Compte tenu de son rapport avec le pouvoir politique, la neutralité du renseignement doit être une considération préoccupante dans un domaine où règne le secret. Les erreurs commises par la CIA dans l'appréhension de l'état réel du programme nucléaire irakien après 1991 ont porté des conséquences politiques, dont les effets ne peuvent donc être minimisés. L'utilisation politique par l'administration

¹⁰ *Ibid.*

¹¹ DGSE, . (2018). La DGSE au cœur des cinq fonctions stratégiques : enjeux et perspectives. *Revue Défense Nationale*, 813(8), 14-19. <https://doi.org/10.3917/rdna.813.0014>.

¹² Reuters. (2024, 29 novembre). France : La DGSE voit dans une éventuelle prolifération atomique en Iran une menace critique. *Challenges*. https://www.challenges.fr/top-news/france-la-dgse-voit-dans-une-eventuelle-prolifération-atomique-en-iran-une-menace-critique_913014

Bush de son service de Renseignement afin de justifier l'intervention militaire en Irak pèse dans la conscience collective en faveur du développement d'un service international indépendant.

Toutefois, les limites structurelles dont souffre l'AIEA ne peuvent espérer être dépassées, tenant aux dynamiques politiques internationales.

La pérennité de la prépondérance du Renseignement dans la lutte contre la prolifération des armes de destruction massive demeure dès lors l'hypothèse la plus plausible dans un futur proche¹³.

L'interdépendance des enjeux sécuritaires dans un monde multipolaire devrait cependant faire peser dans l'équation la perspective d'un

renseignement mutualisé des puissances atomiques dans leurs efforts de non-prolifération ; la coopération internationale des services de renseignement est primordiale pour obtenir une vision exhaustive de l'état des programmes nucléaires dans le monde¹⁴.

Le cas irakien, autant dans ses efforts de dissimulation auprès de l'AIEA que dans les erreurs commises par un service de renseignement intimement lié au politique, souligne la nécessité d'une discussion internationale sur l'avenir de la lutte contre la prolifération nucléaire à travers une clé essentielle à sa mise en œuvre trop peu appréhendée : le Renseignement.

A. C.

¹³ Ogilvie-White, T. (2014). The IAEA and the International Politics of Nuclear Intelligence. *Intelligence & National Security*, 29(3), 323-340. <https://doi.org/10.1080/02684527.2014.895591>

¹⁴ DAHAN, P., & MINIOT, A. (2010). Les retrouvailles de la diplomatie et du renseignement dans la lutte contre la prolifération. Vers une diplomatie de la nécessité ? Dans *AFRI : Vol. XI*. La Documentation française.



Scénario

Scénario : 2040 ou la fin des secrets d'Etat

Auteur : Gauthier Capdecorme, Mastérand en Relations Internationales et Diplomatie.

Avant-propos

En 2040, le monde est plus connecté que jamais. Chaque individu a un accès illimité à l'information via son smartphone ou son ordinateur. Dans cette société de transparence extrême, les secrets d'État deviennent de plus en plus rares. Loin de l'univers dystopique imaginé par Orwell, où le pouvoir surveille les citoyens, c'est désormais la population qui scrute le moindre fait et geste des gouvernants. Un renversement total du paradigme de la surveillance, où l'œil collectif remplace Big Brother. Ce scénario interroge la place du secret, les fondements de la démocratie et la raison d'État.

Début du scénario

23 janvier 2025

Le président américain Donald Trump signe un décret sur la déclassification des archives gouvernementales concernant les assassinats du président John F. Kennedy en 1963, de son frère Robert F. Kennedy en 1968 et Martin Luther King la même année. C'était une promesse faite lors de sa campagne de 2017 et renouvelée en 2024. « Tout sera révélé », a-t-il affirmé avec son assurance habituelle. Cette idéologie extrême de l'information à tout prix avait comme plus fervent ambassadeur le milliardaire Elon Musk, proche conseiller du président et propriétaire du réseau social X qui se voulait être la plateforme

d'exposition de toutes les opinions. Toutefois la mise en lumière de ces informations cachées depuis des décennies au public eurent un effet insoupçonné. Les soupçons pesant sur l'implication de la CIA, l'agence de renseignement la plus réputée aux États-Unis, furent confirmés par les documents à propos de l'ensemble des assassinats, dont les gouvernements successifs auraient eu connaissance.

Ces révélations eurent l'effet d'une bombe à l'échelle planétaire. Les populations avaient soif de vérité avec une question unique : À quel point l'Etat, les gouvernements nous mentent-ils ? Le président Trump, surfant sur sa vague de popularité, étant devenu l'égérie d'un gouvernement transparent auquel les citoyens pouvaient accorder leur confiance, continua à foison les révélations de secrets d'Etats.

Par ailleurs, la question suivante entraînait dans les esprits, à savoir qu'est-ce qu'un secret d'Etat ? C'est une information qui par sa nature est gardée secrète afin d'assurer la sécurité de tous ou protéger les intérêts stratégiques d'un Etat. Ainsi dans sa définition, le secret d'Etat est un principe positif assurant la pérennité d'un Etat, la sécurité et le bon fonctionnement de sa population. Dès lors Donald Trump, en questionnant ce principe, questionne indirectement la nécessité d'un Etat car la population assurerait sa propre sécurité en annihilant les secrets d'Etat.

La fin des secrets d'État serait donc la première étape vers la chute de l'État

moderne. Ainsi, que ce soit le fait que la CIA savait que des attentats allaient avoir lieu le 11 septembre 2001 et qu'elle ne les avait pas empêchés, ou les preuves des manipulations en 2003 pour partir en guerre contre l'Irak, tout devait être su. Cependant deux affaires monopolisèrent les réactions, en premier la complicité dévoilée de la République Populaire de Chine de Xi Jinping et des Etats-Unis de Barack Obama avec la Fédération de Russie de Vladimir Poutine dans l'annexion de la Crimée, région ukrainienne jusqu'alors,.

La deuxième, la mise en place d'un marché noir de la bombe nucléaire par la RPC, la Corée du Nord et le Pakistan, sur le modèle lancé par Abdul Quadeer Khan dans les années 1970, lui qui est considéré comme le père de la bombe atomique pakistanaise, et que les Etats-Unis laissaient faire ce marché afin de justifier son interventionnisme mondial. A partir de ce moment précis, une pression populaire mondiale prit forme: des révoltes spontanées apparurent dans divers pays, menaçant par conséquent les gouvernements. La recherche de la vérité poussant à défier les régimes en place.

Tous, opprimés de toutes parts, finirent par laisser libre accès aux archives classifiées et une explosion de vérité recouvra le monde. Les régimes autoritaires, plus coupables encore que les régimes démocratiques, subirent des soulèvements renouvelés, les faisant tomber tour à tour entre 2026 et 2031. Ce phénomène mondial s'octroya le nom de «Truth's Storm» .

2028 - 2030'

Avec la chute des régimes autoritaires, la recherche de la démocratie parfaite devint l'objectif des peuples libérés de toutes contraintes institutionnelles. Ce modèle de perfection où la transparence serait le credo sur l'ensemble des actions menées devait faire disparaître les concepts de secret et raison d'Etat. Dorénavant la raison d'Etat serait le peuple et s'appuierait sur des principes comme l'égalité, la transparence ou encore les droits humains. Le référendum, procédé jusqu'alors rarement utilisé, devient l'arme de contrôle emblématique populaire envers les élus. Chaque projet, chaque action majeure doit être soumise au vote.

En parallèle, les Etats tels que nous les connaissons disparaissent petit à petit, les anciennes organisations internationales deviennent les seules plateformes d'échanges entre les nations et tous les échanges tendent à être contrôlés lors des sessions quotidiennes.

2040

Le visage du monde n'est plus que méfiance. Contrairement à l'œuvre dystopique de George Orwell, 1984, ce n'est pas la surveillance de masse qui exerce son pouvoir sur le peuple, mais bien la surveillance par la masse des élites dirigeantes. Chaque citoyen possède un contrôle équitablement réparti sur ses élus. La délation et le soupçon sont devenus les plus grandes armes des sociétés. Les innovations technologiques et l'information en temps réel à travers les smartphones, les ordinateurs ou tout autre support permettent ce contrôle de tout instant. La vie de tous est scrutée et la vie privée semble ne plus avoir réellement sa place. De plus, la suppression des législations sur la protection des

données personnelles comme le RGPD en Europe ne laisse aucune marge d'erreur que ce soit en ligne ou dans la vie réelle. S'ajoutent aussi les innovations liées aux intelligences artificielles qui tentent de calculer avec les informations des citoyens les probabilités dans le futur qu'ils ont de devenir des menaces potentielles pour le système. Tout passe par des Politburos qui filtrent les accusations et mènent les enquêtes nécessaires, ils possèdent un pouvoir presque total et chassent les moindres petits secrets. Cet organe représentatif de l'œil collectif, scrutant constamment les moindres faits et gestes des politiques ne permet plus aucune liberté à ces derniers, s'ils sont accusés de ne pas suivre la voie du peuple, leur mission s'arrête.

Cette société de transparence totale et de contrôle global se présente comme l'héritière de l'idéologie communiste présentée par Karl Marx et Friedrich Engels dans leur manifeste publié en 1848. Cependant au détail près que l'Etat n'est plus qu'un organe végétatif obéissant aux décisions de la population, se rapprochant donc davantage d'une société anarchique que communiste.

Par ailleurs, les gouvernements n'étant plus que fantoches, c'est dorénavant au sein de la nouvelle organisation internationale que l'ensemble des jeux géopolitiques mondiaux sont décidés. La Société Internationale Moderne des Populations (SIMP), inaugurée en 2037 par les représentants des 122 Républiques populaires existantes gouvernent ensemble, liées par la pression de se voir remplacer au moindre faux pas. Les représentants élus au suffrage universel direct, doivent aborder à l'ordre du jour de chaque séance les sujets votés au préalable par un comité de citoyens

eux-mêmes élus, comité qui se voit renouvelé tous les six mois afin d'éviter tout risque de monopolisation d'un quelconque pouvoir. Depuis la mise en place de ce système strict au sein de cette nouvelle organisation, aucune tentative de corruption n'a été recensée, ou à minima présentée, cela est mis comme preuve de l'efficacité de la transparence.

Concernant le multipartisme et la tolérance des différentes opinions, cela semble n'être devenu qu'un rêve lointain. En effet comme au temps du MacCarthysme aux Etats-Unis dans les années 1950 qui étaient en lutte avec le soviétisme russe, idéologie gauchiste, cette fois la chasse aux sorcières est portée contre l'extrême droite, aux valeurs opposées. Toute personne semblant avoir un quelconque lien avec cette idéologie divergente sera emmenée à un Politburo et les actions nécessaires seront menées afin qu'elle ne soit plus jamais un quelconque risque pour la société.

C'est toutefois quelque chose d'étonnant que ce soit la droite et l'extrême droite plus particulièrement qui subissent cette aliénation constante quand on se rappelle de qui provient la succession des événements. Donald Trump, président républicain américain controversé aux allures d'impérialiste, et son conseiller Elon Musk, fou sous kétamine soutien de l'extrême droite mondiale qui prônait une liberté d'expression totale. Liberté d'expression qui finalement est morte car se trouve scellée dans une cage gardée par l'œil collectif.

Quelques anciennes démocraties subsistent tant bien que mal, mais vivent recluses en autarcie comme en Terre de Feu ou autour du Détroit de la Pérouse, elles restent discrètes afin de ne pas attirer l'oeil inquisiteur collectif dans leur direction, sachant pertinemment qu'elles ne sont que tolérées car servent de refuges pour tous ceux fuyant ce monde de vérité forcée, de transparence.

Cependant à partir de ces États de fortune, certains se targuent d'organiser des actions révolutionnaires afin de redonner aux démocraties leur place légitime, car seul régime ayant le potentiel de respecter entièrement les droits humains, l'Etat de droit, l'égalité, l'indépendance de la justice et autres valeurs humanistes. Pour cela leur action phare qui est pourtant simple car se sert du système de cette société anarchique, se fonde sur les soupçons. C'est à dire qu'ils appliquent tout simplement, sous le coup de fausses identités, le devoir de tout citoyen quand celui-ci trouve qu'un individu cache des intentions qui pourraient être dangereuses pour la population, de la délation auprès du Politburo.

Ainsi c'est à coup de plusieurs centaines de dénonciations hebdomadaires que ces révolutionnaires tentent d'enrayer cette machine afin de démontrer que cette voie du contrôle total n'est que perversion. Cependant la propagande faisant passer les

démocraties pour des sociétés d'un ancien temps, couplée à une peur omniprésente d'être la cible d'une future dénonciation détruisant dans la foulée la vie du citoyen, ne laisse que peu de place à la réflexion. L'individu n'est plus, l'uniformisation complète de la société lui a fait perdre son identité.

Ainsi dans ce monde ultra-connecté de 2040 où chaque individu devient gendarme d'un système répressif, le paradigme de la surveillance se retrouve complètement inversé par rapport à celui que nous connaissons. La « Truth's Storm » aura déclenché une ère où l'information doit être transparente quoi qu'il en coûte et le moindre secret devient justification de mise sous silence. Le renseignement n'est dès lors plus au service de la protection de l'Etat mais l'instrument de contrôle des élites par la masse, l'Etat pouvant être renouvelé sans que cela n'inquiète ses différentes missions. L'information est devenue l'arme citoyenne majeure de contrôle et le secret n'a plus qualité à exister dans ce monde. Cependant combien de temps ce modèle tiendra avant que la nature de l'Homme ne reprenne le dessus sur cette imposition de l'ordre de la vérité ?

G.C.



Hors-série

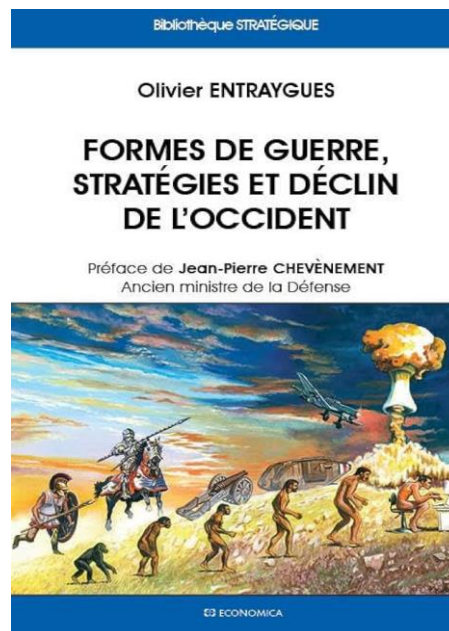
Hors-série : Du déclin de la pensée stratégique occidentale

Auteur : Marin de Lambert, Mastérent en Relations Internationales, Sécurité et Défense.

Cet article au titre quelque peu intrigant, si ce n'est provocateur, tire sa genèse de la lecture de l'ouvrage *Formes de guerre, stratégies et déclin de l'Occident*, publié par le colonel Olivier Entraygues en 2014. Entre philosophie et théorie stratégique, l'auteur y propose une étude portant sur la nature de la guerre, à travers l'Histoire et l'usage de différents concepts et néologismes tels que le « diapolème », la « chronostratégie » ou encore le « *kairos* ». Certains de ces concepts seront mobilisés plus tard dans l'article, ce dernier se voulant être une exégèse de l'ouvrage, dont le sujet complexe et vaste mériterait d'être abordé au travers d'un travail plus sérieux et profond, qu'un article étudiant.

L'occidentocentrisme du présent article est pleinement assumé, il s'agit ici de réfléchir à nos propres failles ; en outre, l'amalgame qui y est fait entre les différentes cultures stratégiques des États occidentaux est aussi assumé, l'objet de l'article étant l'Occident en tant qu'entité collective.

Alors que les armées occidentales sortent de deux décennies de « guerre au terrorisme » et que la guerre de haute intensité a fait un retour fracassant sur le sol européen, il est possible de considérer que la période que nous traversons relève du « *kairos* ». En grec, cette notion philosophique ne désigne pas seulement le temps (*chronos*), qui relève d'une

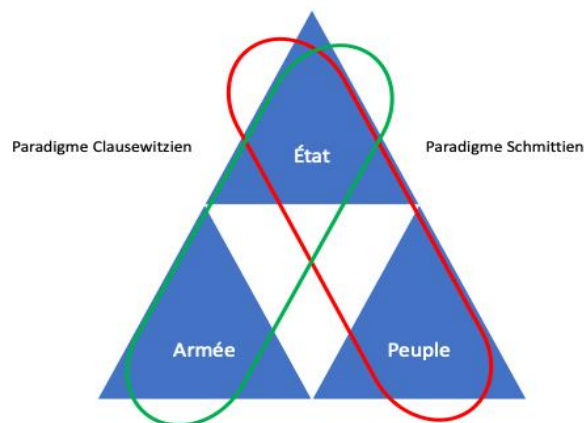


dimension linéaire, mesurable et quantitative ; mais il se réfère plutôt à une temporalité qualitative, décisive, correspondant à un moment opportun, dont les conditions présentes sont éphémères mais favorables pour l'action. Nous vivons donc une période charnière, propre à l'action mais pourtant les États occidentaux et surtout européens semblent plus que jamais attentistes quant à leur avenir, ballotés entre Moscou et Washington (dont la tentation isolationniste du second mandat Trump, peut interroger). Si la faillite est évidemment politique, l'absence de véritable solution stratégique est criante.

Aux origines du déclin de la pensée stratégique occidentale : la guerre froide. Alors que la destruction mutuelle assurée paralysait tout type d'action directe entre les deux blocs, les théâtres d'affrontements secondaires se sont multipliés et l'on a pu y assister à l'émergence du partisan, devenu une figure centrale des conflits de la

seconde moitié du XX^{ème} siècle. Ce dernier est caractérisé selon Carl Schmitt par son irrégularité, l'intensité politique de son combat, sa mobilité et son ancrage sur un territoire donné. C'est à ce moment que selon Olivier Enraygues, s'est joué le passage d'un paradigme Clausewitzien, où l'étrange trinité État-peuple-armée restant centrée sur l'État et l'armée (la population n'étant pas acteur du conflit, seulement son objet et/ou sa victime), à un paradigme Schmittien, cette fois centré sur l'État et les populations, devenues actrices au travers de la figure du partisan mais aussi enjeux des conflits, la conquête « des cœurs et des esprits » étant devenu l'un des objectifs centraux des opérations de contre-insurrection (COIN).

stratégiques. Ce constat est d'autant plus paradoxal qu'une étude de l'évolution des styles de combats en Europe à travers les âges, explicite ce que le général Fuller qualifiait de « loi du facteur tactique constant » (soit la systématique mise au point d'une contre mesure à tout nouveau perfectionnement militaire) c'est-à-dire une évolution technologique et organisationnelle constante : de l'infanterie légère antique, à la cavalerie cuirassée moyenâgeuse, à la prédominance des armes de jets d'Azincourt jusqu'à l'avènement des formations blindées durant la Première Guerre mondiale. Et alors que l'Occident était arrivé à un âge de perfectionnement



Représentation de l'étonnante trinité de Clausewitz et deux paradigmes Clausewitzien et Schmittien de la guerre.

Ainsi, le paradigme Clausewitzien a persisté tout au long de la guerre froide, mais incarné par l'État et les forces nucléaires, ces dernières neutralisant toute possibilité de guerre directe, tandis que l'Occident s'est retrouvé à faire face à des conflits asymétriques de faible intensité, préludes des opérations de COIN modernes, et dont les issues n'ont que rarement été favorables. Face à la modernité technique occidentale, les partisans ont opposé un archaïsme des moyens et méthodes avec lequel nos armées, souvent victorieuses tactiquement, n'ont pu atteindre de succès

militairement avancé et caractérisé par les armes nucléaires, puis la *Revolution in Military Affairs*, cette modernité a fini par générer une évolution régressive chez nos adversaires : le retour du primat de l'infanterie légère avec des groupes armés à la fois *low-cost* mais de plus en plus *high tech* (des *Stingers* des Moudjahidines aux drones de l'État islamique).

L'Occident, toujours écrasant tactiquement, n'a pourtant pas su développer de stratégie adaptée, qui aurait dû concrétiser le lien entre son engagement

militaire et le sens politique donné à ces conflits. Cette « éclipse de la stratégie », selon Michel Yakovleff dans son ouvrage *Tactique théorique* (2016), est d'autant plus grave que notre supériorité tactique n'est plus assurée dans les potentiels conflits à venir ; le retour de la perspective d'une confrontation de haute intensité en Europe ne signifie donc pas le retour à une « situation normale », comme si les échecs connus depuis le début de la décolonisation n'avaient été dus qu'à la nature des conflits rencontrés et à une mauvaise compréhension de l'interaction entre guerre et politique.

Ce déclin de la pensée stratégique occidentale consiste en trois idées principales. Tout d'abord l'obsession pour le « modèle » stratégique du « conflit violent visant la victoire » que décrit le général André Beaufre dans son *Introduction à la stratégie* (1963). Il explique que ce « concept clausewitzien-napoléonien » considéré à tort « comme la seule stratégie orthodoxe », a conduit les États européens dans de nombreuses impasses stratégiques à commencer par les deux guerres mondiales. La recherche d'une décision acquise par l'action militaire, n'a conduit qu'à des guerres d'usures dépassant largement les enjeux initiaux et n'ont donc été selon Beaufre, que l'exaltation d'un modèle ayant pour fondement la fascination pour les victoires de Napoléon, ce modèle ayant pourtant montré ses limites dès l'origine, puisque l'Empereur n'a pu vaincre le Royaume-Uni et la Russie par le seul recours au conflit direct.

Ensuite, les deux guerres mondiales ayant résulté du « modèle stratégique » précédemment décrit, sont qualifiées par Olivier Enraygues de « guerres hyperboliques », englobant

massivement des vies humaines et les ressources allouées par les États. L'ampleur des massacres et des destructions qu'ont occasionné les « guerres hyperboliques », ont laissé une cicatrice profonde dans la mémoire collective occidentale, nos sociétés ayant progressivement développé une « polémophobie », également expliquée par la montée de l'individualisme. Ainsi, les opinions publiques mais aussi les outils militaires occidentaux ont contracté une phobie de la mort et une aversion aux risques paralysant notre pensée stratégique : comment penser la guerre si nous refusons de concevoir ses conséquences intrinsèques ?

Finalement, notre pensée militaire toujours conditionnée par l'exponentielle croissance de nos progrès technoscientifiques, est devenue matérialiste, centrée sur la destruction physique de l'adversaire comme moyen voire même but principal de la guerre. L'illustration la plus frappante de ce phénomène pourtant commun à tous les Occidentaux, reste la technophilie américaine, pour qui la dernière technologie en date devient la solution miracle à tous les problèmes du champ de bataille, l'ennemi n'étant plus qu'une force morte sur qui appliquer des moyens technologiques. Ce mal a culminé lors de la « guerre au terrorisme », où le sens politique des opérations militaires restait flou et où la seule stratégie se limitait bien souvent à la production d'effets cinétiques sur l'adversaire, essentialisé en « terroriste ». Selon Michel Yakovleff, ce biais scientifique nous a également amené à concevoir nos opérations militaires selon une méthode rationnelle et méthodique dépendante d'une planification arrêtée et prévisible pour nos adversaires.

Pour résumer, la difficulté à penser la guerre en dehors d'une vision clausewitzienne, d'une conflictualité tendant vers la « guerre totale » ; la polémophobie des sociétés occidentales ; et enfin la lubie matérialiste et scientiste de notre conception de la guerre sont la concrétisation du déclin de la pensée stratégique occidentale.

Si le retour possible de la guerre de haute intensité adoucit le décalage existant entre la pensée stratégique occidentale et l'environnement où elle doit se déployer, une réforme interne doit finir de nous réarmer moralement pour la guerre.

D'abord une réforme intellectuelle autour de la guerre, qui doit rester un outil du politique, alors que la pensée stratégique, quant à elle, a vocation à une certaine autonomie. En démocratie, le politique, contraint par l'alternance et donc au court terme, subit une myopie stratégique, alors que la pensée stratégique se doit d'être stable, continue et de long terme : elle ne peut donc se laisser conditionner par des impératifs politiques variant au gré des préoccupations du moment (vu du politique, chaque nouvelle préoccupation semble être une révolution qui nécessiterait un changement radical : dissuasion nucléaire, dividendes de la paix, « guerre au terrorisme » ...)

Ainsi, la pensée stratégique se doit d'être autonome, englobante et non conditionnée par le climat politique du moment, elle doit être tournée vers ce que le colonel Entraygues qualifie de « chronostratégie » : c'est-à-dire dire d'une prise décision basée sur une prise en compte d'une temporalité singulière, basée sur le *kairos*. Anticiper, réfléchir l'action dans un intervalle de temps particulier et favorable,

identifier les facteurs défavorables... La chronostratégie cherche donc à nous dire comment agir mais aussi quand agir, et cette conception globale, fondée sur une prise en compte de la temporalité, peut donc nous inviter à revoir la simple dichotomie paix-guerre. Il en découle une nécessité de repenser la guerre au-delà du seul modèle de « conflit violent visant la victoire », évoqué par le général Beaufre. Les stratégies indirectes qu'il met en avant sont ainsi des pistes à explorer, prenant place dans cette zone d'incertitude, entre guerre et paix dans laquelle les adversaires de l'Occident n'ont pas hésité à s'impliquer contournant ainsi « par le bas » notre puissance militaire « classique » (conventionnelle et nucléaire). La puissance occidentale génère donc non seulement de l'archaïsme mais aussi de l'hybridité. Il semble intéressant de relever que dans le cas français, ce constat a déjà été fait : on parle donc du triptyque « compétition / confrontation / affrontement » et de « gagner la guerre avant la guerre ».

L'interaction stratégique avec l'adversaire doit également être étudiée selon ce prisme de la chronostratégie, ce dernier évoluant dans sa propre temporalité (la perception de cette temporalité découlant de l'Histoire et de la culture stratégique de l'adversaire), le comprendre est donc nécessaire pour ne pas créer d'occasion historique favorable, de *kairos* pour l'adversaire.

Et finalement, une réforme sociétale est nécessaire, or, en cherchant à expliquer les défaites consécutives de la France face à l'Allemagne, le colonel Entraygues pose trois conditions à la capacité d'une société à se défendre, qui peuvent constituer des pistes de réflexion. Tout d'abord une prise de conscience du danger qui la guette, ensuite une implication intergénérationnelle

de la société pour faire face à la guerre à venir et enfin la mise en place de budgets et de moyens suffisants grâce à un effort accepté par la population.

Pour conclure, *Formes de guerre, stratégies et déclin de l'Occident* est un ouvrage original présentant une réflexion sur la philosophie de la stratégie, qui mérite d'être lu. Le présent article propose un commentaire ne se concentrant que sur une mince partie de l'ouvrage : la question du déclin stratégique de l'Occident, examiné au travers de la chronostratégie. Le sujet n'ayant été ici qu'effleuré, le lecteur intéressé devra approfondir la réflexion par d'autres lectures et recherches autour de cette vaste mais importante thématique.

« Pour trouver un second souffle, notre civilisation devra inventer le nouveau paradigme guerrier établissant sa supériorité dans le nouveau contexte. »

Général Michel Yakovleff

M. de L.

Postface

Nous tenons à remercier nos chers rédacteurs, tous étudiants en Relations Internationales, pour leurs articles passionnants qui nous ont permis de mettre en œuvre une revue complète sur les enjeux qui animent la théorie des alliances. Nous tenons particulièrement à remercier M. Thierry Maurin d'avoir accepté de réaliser une interview avec nous et d'avoir partagé son expérience en tant qu'Officier Renseignement.

Merci également aux enseignants et chercheurs qui ont accepté de relire les articles de nos rédacteurs et de les avoir conseillés et plus particulièrement :

Mme Elodie Barbier-Para, M. François David, M. Douglas de Quadros Rocha, M. Thibault Fouillet, M. Sylvain Gaillaud, M. Anton Gopko, M. Benoît Léthenet, Mme Iris Marjolet, M. Nicolas Moinet et Mme Muriel Salle.



Les rédacteurs sont joignables individuellement par LinkedIn ou en s'adressant à l'AMRI (Association du Master de Relations Internationales de Lyon III).

Les images non-sourcées proviennent d'une génération par intelligence artificielle.

Les opinions exprimées dans les articles ou entretiens n'engagent que leurs auteur

Rédacteurs en chef : Ciara Mclaverty et Paulin Devanlay.

