Institut EGA

La Revue Diplomatique

SOUS LA DIRECTION DE
MANON CHEMEL ET ALEXANDRE NEGRUS

Revue trimestrielle - Janvier-Mars 2023

N°20 - 9.80 €

RENSEIGNEMENT ET GÉOPOLITIQUE LES ENJEUX CONTEMPORAINS

TRACFIN
TRACFIN et la lutte contre le financement du terrorisme

BRUNO CLEMENT-PETREMANN
Le renseignement pénitentiaire et la lutte contre le terrorisme

LAURANE RAIMONDO
Renseignement et géopolitique : Les enjeux contemporains

Gérald ARBOIT • **Romain BERTOLINO** • **Lucien CHAYA PODEUR** • **Franck DECLOQUEMENT**

Julien DREVETON • **F.-X Noah EDZIMBI** • **Louise MASSON** • **Emerancia NTUMBA**

Berthe Mélika OBAMA MEWALI • **Karine ROUSSEAUX** • **Emmanuel VERON**

www.institut-ega.org

AVERTISSEMENT

Renseignement et géopolitique : Les enjeux contemporains

Les propos exprimés par chaque contributeur n'engagent ni l'Institut d'études de géopolitique appliquée, ni les rédacteurs entre eux, ni le comité de relecture.

Aucune personne physique ou morale citée dans le texte d'un contributeur n'a pour objectif d'identifier l'Institut d'études de géopolitique appliquée ou les autres contributeurs.

Comment citer cette publication :

Renseignement et géopolitique : Les enjeux contemporains, (dir. Manon Chemel, Alexandre Negrus), *Institut d'études de géopolitique appliquée*, *Revue Diplomatique*, n°20, Paris, 2023.

ISSN : 2739-2341

Institut d'études de géopolitique appliquée
121 rue du Vieux Pont de Sèvres 92100 Boulogne-Billancourt
Courriel : contact@institut-ega.org
Site internet : www.institut-ega.org

Institut
EGA

FORMATION

Renseignement : Quelles adaptations pour quelles menaces ?

L'Institut d'études de géopolitique appliquée (lega) propose une formation certifiante sur l'étude des enjeux contemporains en matière de renseignement et de l'adaptation des services aux différentes menaces.

Cette formation s'adresse à des étudiants et des professionnels de tout niveau souhaitant acquérir une vision pluridisciplinaire des activités de renseignement. Les auditeurs pourront acquérir des connaissances et bénéficier d'une expertise sur les nouvelles menaces contre la paix et la sécurité internationales ainsi que sur le rôle et l'adaptation des activités de renseignement.

Les séances sont dispensées par des experts, praticiens et enseignants sur les questions de sécurité intérieure et internationale, sur le cadre légal français, européen et international ainsi qu'en matière de défense.

Sont abordés les enjeux relatifs au renseignement sous différents angles afin d'acquérir des compétences polyvalentes sur un domaine à la fois technique et d'actualité.

Modules du tronc commun

- **Module n°1** - La lutte contre les ingérences étrangères en France
- **Module n°2** - Cyber-menaces et crime organisé
- **Module n°3** - Renseignement économique : contre-espionnage et contre-ingérence
- **Module n°4** - Renseignement et sécurité intérieure
- **Module n°5** - Renseignement militaire : de la basse intensité à la haute intensité

Options

- **Atelier** - OSINT : méthodologie et outils de renseignement
- **Atelier** - Intégrer un service de renseignement : conseils d'un praticien
- **Revue** - Renseignement et géopolitique : les enjeux contemporains
- **Formation** - Menaces terroristes et montée des radicalités
- **Formation** - Renseignement et terrorisme / Renseignement et géopolitique / Renseignement et droit (correspondant à plus d'une dizaine de modules supplémentaires)

Les modules sont accessibles **en différé** depuis une plateforme pédagogique en ligne donnant accès aux modules et options sans conditions horaires pendant un mois.

La formation proposée donne lieu à la remise d'un certificat remis par l'lega attestant du suivi de la formation. La remise du certificat n'est pas conditionnée par la réalisation d'exercices.

La formation s'inscrit dans un parcours professionnalisant destiné à des étudiants et des professionnels de tout niveau souhaitant acquérir des bases solides en la matière.

CANDIDATURE SUR CE LIEN

Institut
EGA

SOMMAIRE

Renseignement et géopolitique : Les enjeux contemporains

TRACFIN – TRACFIN et la lutte contre le financement du terrorisme **P. 1**

Gérald ARBOIT – Déstabiliser l'Europe par l'information : un exemple sous le Premier empire **P. 7**

Louise MASSON – Le rôle des services de renseignement français dans la lutte contre les groupes terroristes **P. 10**

Emerancia NTUMBA – Le renseignement international dans la lutte contre le trafic illicite des biens culturels **P. 14**

Franck DECLOQUEMENT – Quand le recueil de renseignement à partir d'informations de sources ouvertes impacte la conduite des conflits modernes **P. 21**

Lucien CHAYA PODEUR – Menaces cyber et renseignement **P. 25**

Bruno CLEMENT-PETREMANN – Renseignement pénitentiaire et lutte contre le terrorisme – **P. 28**

Romain BERTOLINO – Les vecteurs aériens et spatiaux du renseignement militaire français : composition et enjeux **P. 32**

Laurane RAIMONDO – Renseignement et géopolitique : Les enjeux contemporains **P. 36**

Karine ROUSSEAUX – Le Métavers : quels enjeux, quels défis pour le renseignement français ? **P. 42**

Emmanuel VÉRON – La « cybercrature » chinoise : une menace interne et extérieure ? **P. 46**

Julien DREVETON – Politique et géopolitique des services de renseignement au Moyen-Orient **P. 50**

François Xavier NOAH EDZIMBI – Face aux guerres probables du XXIe siècle, l'intelligence économique doit être sociétale en Afrique **P. 54**

Berthe Mélika OBAMA MEWALI – La communication comme un outil efficace pour le renseignement dans la lutte contre la violence hybride : Le cas du Cameroun **P. 62**

TRACFIN et la lutte contre le financement du terrorisme

Rédigé par TRACFIN
Service de renseignement placé sous l'autorité du ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique. Il concourt au développement d'une économie saine en luttant contre les circuits financiers clandestins, le blanchiment d'argent et le financement du terrorisme.

Après les attentats de septembre 2001 commis aux États-Unis, la lutte contre le financement du terrorisme est devenue un axe prioritaire du dispositif antiterroriste, tant à l'échelle nationale qu'aux plans européen et international. Le changement de dimension de la menace terroriste en France et la priorité gouvernementale accordée à la lutte contre le terrorisme et son financement se sont intensifiés en 2015. Dans un contexte marqué par l'évolution et la numérisation des vecteurs de financement, l'émergence de nouvelles formes de criminalité financière et l'internationalisation des flux financiers, TRACFIN a repensé son organisation et ses méthodes d'analyse et d'investigation pour renforcer l'efficacité opérationnelle de son action.

La lutte contre le financement du terrorisme, une mission historique et prioritaire de TRACFIN

Attribuée lors de la création de TRACFIN le 9 mai 1990, la mission de lutte contre le blanchiment de capitaux a été enrichie, en 2001, d'une mission d'entrave du financement du terrorisme. Cette mission prioritaire, qui s'est initialement concentrée sur l'identification de transferts de fonds à destination de la péninsule arabique et de groupes ou individus affiliés à des organisations terroristes liées au groupe Al-Qaïda, a été renforcée en 2009 avec la transposition de la 3e directive européenne relative à la lutte contre le blanchiment de capitaux et le financement du terrorisme et l'adoption de l'ordonnance du 30 janvier 2009 développant les possibilités légales, pour TRACFIN, d'accéder aux informations administratives et judiciaires et de diffuser les données qu'il agrège aux services de renseignement.

TRACFIN exerce à la fois un rôle de prévention de la menace par une capacité de détection des flux atypiques s'inscrivant dans des schémas de financement du terrorisme, mais également d'entrave de phénomènes terroristes. La réception de déclarations de soupçon, en augmentation constante depuis 2017[1], permet à TRACFIN d'exercer une veille quotidienne sur un flux d'informations, complétée par des investigations approfondies (analyse des comptes bancaires et transferts de fonds, détection d'utilisation suspicieuse de cryptoactifs) dont les résultats sont transmis aux services de la communauté du renseignement.

Une intégration renforcée au sein de la communauté du renseignement française

L'année 2008 a marqué l'intégration de TRACFIN en tant que service spécialisé de renseignement au sein du premier cercle de la communauté du renseignement[2] dont l'activité, encadrée par le code de sécurité intérieure, consiste à défendre et promouvoir les intérêts fondamentaux de la Nation, l'indépendance nationale et l'intégrité du territoire. TRACFIN en constitue un maillon essentiel par son expertise financière. En 2015, la loi dite « renseignement »[3] a apporté un nouveau cadre légal aux activités des services de renseignement (techniques de surveillance, régime d'autorisation) et

[1] En 2021, TRACFIN a reçu 165 171 informations en provenance des professionnels assujettis au dispositif de lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT) soit une augmentation de 55% du volume d'informations reçues depuis 2017.

[2] Les services de renseignement du premier cercle sont : la DGSE, la DGSI, la DNRED, la DRM, la DRSD et TRACFIN.

[3] Loi n° 2015-912 du 24 juillet 2015 relative au renseignement.

a permis à TRACFIN d'accéder à de nouvelles techniques d'investigation tout en offrant un cadre d'action permettant d'améliorer la coordination avec les autres services de renseignement dans une logique de mutualisation des moyens.

Symbole de cette intégration accrue à la communauté du renseignement français, TRACFIN siège au sein de différentes cellules inter-agences de lutte contre le terrorisme telle que la cellule ALLAT, qui réunissent l'ensemble des membres de la communauté du renseignement (DGSI, DGSE, DRSD, DRM, DNRED, TRACFIN, SCRT, DRPP, SNRP, SDAO) dans le but de mutualiser les informations issues de différentes sources et y dispose d'un officier de liaison permanent. Ainsi, entre janvier 2019 et avril 2022, 2 857 notes relatives à des dossiers liés à des enjeux de financement du terrorisme ou de radicalisation ont été adressées par TRACFIN à ses partenaires.

Depuis 2018, TRACFIN co-pilote également, avec la DGSI, le Groupe d'action sur le gel à but antiterroriste (GABAT). Placé sous l'égide du Secrétariat général de la défense et de la sécurité nationale (SGDSN), ce groupe assure la coordination à l'échelle nationale des différentes autorités chargées de la lutte contre le terrorisme, de la préparation et de la mise en œuvre des mesures de gel des avoirs. La création de ce groupe de travail, destinataire de 275 transmissions de TRACFIN depuis 2018, a permis une augmentation significative des gels de comptes bancaires voire de biens immobiliers de personnes suspectées de s'être livrées à des activités terroristes.

Une exploitation judiciaire structurée et systématique des informations transmises par TRACFIN au parquet national antiterroriste

En tant qu'infraction distincte indépendamment de procédures suivies des chefs d'infraction de nature terroriste[4], le financement du terrorisme peut motiver l'ouverture d'enquêtes judiciaires sans qu'une enquête soit ouverte pour des faits de terrorisme. TRACFIN travaille en étroite coopération avec le parquet national antiterroriste (PNAT), créé en 2019[5]. Ce travail permet d'enrichir des dossiers relatifs à des actes de terrorisme au sens de l'article 421-1 du code pénal ou de porter à l'attention de l'autorité judiciaire une expertise financière. En assurant une concertation régulière et la dissémination d'informations entre le PNAT et TRACFIN, les autorités françaises ont mis sur pied un travail d'entrave judiciaire permettant de corroborer la présence de ressortissants français en zone syro-irakienne, d'en détecter de nouveaux, mais aussi d'empêcher les soutiens financiers les plus significatifs apportés à des combattants en zone syro-irakienne par des ressortissants ou résidents français. Entre 2019 et 2022, 322 notes ont été adressées au PNAT[6].

Les typologies de financement du terrorisme identifiées par TRACFIN revêtent un caractère essentiellement transnational

Les capteurs de TRACFIN lui ont conféré un rôle de vigie, capable d'anticiper et d'identifier de nouvelles typologies et de vecteurs innovants de financement du terrorisme par le traitement de signaux faibles.

La persistance des réseaux de collecteurs de fonds internationaux

Observé dès 2013, soit l'année précédant la proclamation du « califat » par Abou Bakr Al Baghdadi sur les territoires de l'État islamique, le phénomène de collecteurs de fonds[7] s'est maintenu avec un degré constant d'intensité. Les collecteurs sont des intermédiaires financiers qui utilisent les

[4] Au sens de l'article 421-2-2 du code pénal qui prévoit que constitue un acte de terrorisme le fait de financer une entreprise terroriste en fournissant, en réunissant ou en gérant des fonds, des valeurs ou des biens quelconques ou en donnant des conseils à cette fin, dans l'intention de voir ces fonds, valeurs ou biens utilisés ou en sachant qu'ils sont destinés à être utilisés, en tout ou partie, en vue de commettre l'un quelconque des actes de terrorisme prévus au présent chapitre, indépendamment de la survenance éventuelle d'un tel acte.

[5] Le PNAT a été créé par la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.

[6] Il est à noter que 228 d'entre elles ont également été transmises aux services compétents du ministère de l'Intérieur à des fins de gel des avoirs.

[7] Également renommés Syrian Wallets.

services de transmission de fonds pour centraliser des espèces en Europe, puis les transférer vers des pays frontaliers des zones de conflits. Les espèces sont alors retirées et transportées physiquement jusqu'aux commanditaires ou bénéficiaires. Les réseaux de collecte de fonds peuvent également avoir recours à la transmission de fonds par des systèmes de compensation régionaux, informels ou coutumiers de type *hawala*[8]. Ces mécanismes sont utilisés tant pour acheminer des financements vers les zones de conflit, que pour financer des cellules opérationnelles projetées à l'étranger. Les montants moyens envoyés par ces réseaux se situent entre plusieurs dizaines et quelques centaines d'euros. Ils impliquent une vigilance extrême sur toutes les opérations, y compris celles de faible intensité susceptibles d'alimenter un réseau de collecteurs.

L'évolution des méthodes de collecte de fonds sous l'effet de l'apparition des crypto-actifs et de nouveaux intermédiaires nés de la numérisation des services de paiement et de transfert de fonds

Le développement des plateformes de financement participatif, notamment des cagnottes en ligne, a offert de nouvelles possibilités aux réseaux de collecte de fonds pour compléter, par des vecteurs numériques, les circuits traditionnels de financement du terrorisme. TRACFIN a constaté plusieurs utilisations des cagnottes en ligne afin de collecter des dons, généralement de faible montant, dans le but de financer des organisations radicales. Face aux risques identifiés, TRACFIN a soutenu le renforcement du cadre réglementaire concernant les cagnottes en ligne françaises[9]. En tant qu'intermédiaire en financement participatif, les cagnottes françaises sont désormais pleinement assujetties aux obligations de LCB-FT[10], ce qui n'est pas encore le cas au plan européen puisque le nouveau statut unique européen de prestataire de services de financement participatif[11] exclut les activités non lucratives, dont les sites de cagnottes en ligne, du champ d'assujettissement aux obligations LCB-FT.

De la même manière, les collecteurs de fonds ont transposé les circuits de financement d'organisations terroristes dans la sphère des crypto-actifs, laquelle favorise l'anonymat et la dissimulation des transactions ainsi que de leurs bénéficiaires. En 2020, les investigations de TRACFIN ont mis en évidence un circuit international sophistiqué de financement de combattants djihadistes en zone syro-irakienne qui conjuguait une monnaie électronique stockée sur des supports physiques de paiement (coupons prépayés), l'utilisation d'actifs numériques et le recours à un système de compensation informel de type *hawala*. Dans ce circuit, les achats de coupons prépayés étaient exclusivement destinés à être convertis en crypto-actifs. Une fois convertis, les crypto-actifs acquis étaient transférés sur des plateformes d'échanges situées dans des pays à proximité immédiate de la zone syro-irakienne. À ce titre, TRACFIN a été la première cellule de renseignement financier à détecter cette nouvelle menace au niveau mondial, ce qui a permis l'organisation d'une opération de police judiciaire de grande envergure pilotée par le PNAT en septembre 2020. Le service s'est également mobilisé afin de consolider l'encadrement des transactions en crypto-actifs et le dispositif national de LCB-FT par des mesures prévoyant notamment l'extension du champ d'assujettissement des prestataires de services sur actifs numériques, l'interdiction de recourir à la monnaie électronique anonyme pour acheter des actifs numériques et

[8] Le système de compensation *hawala* est un système basé sur la confiance, utilisé traditionnellement pour transférer de l'argent d'un pays à un autre. Il utilise un réseau d'agents dans plusieurs pays. Une personne donne une somme d'argent à un « hawaladar », celui-ci contacte un autre « hawaladar », proche du destinataire final de la somme et lui demande de verser cette somme (moins une commission) en échange de la promesse de le rembourser ultérieurement.

[9] D'après l'ordonnance n°2021-1735 du 22 décembre 2021 modernisant le cadre relatif au financement participatif.

[10] Le décret n°2022-110 du 1er février 2022 modernisant le cadre applicable au financement participatif a toutefois introduit une exonération à cet assujettissement pour les projets de cagnottes d'un montant inférieur ou égal à 150 euros.

[11] PSFP ou *European Crowdfunding Service Provider* créé par le règlement (UE) 2020/1503 du Parlement européen et du Conseil du 7 octobre 2020 relatif aux prestataires européens de services de financement participatif, complété par la directive européenne (UE) 2020/1504 entrée en vigueur le 10 novembre 2020.

l'identification des clients dès le 1er euro pour toute transaction, y compris occasionnelle.

L'identification des typologies de financement du terrorisme repose sur d'indispensables partenariats à l'échelle nationale comme internationale

L'identification des vecteurs, y compris les plus innovants, de financement du terrorisme par TRACFIN repose sur un partenariat public-privé à l'échelle nationale ainsi que sur une étroite coopération avec les instances internationales en charge de la lutte contre le financement du terrorisme, et ses homologues étrangers.

À l'échelle nationale, un partenariat public-privé avec les professionnels déclarants ayant la preuve de son efficacité

Afin d'identifier et d'établir ces typologies émergentes, TRACFIN analyse les déclarations de soupçon dont il est destinataire et qui lui sont adressées par l'ensemble des professions assujetties. La pertinence des informations reçues, analysées et enrichies par le Service, dépend largement de la sensibilisation des professions déclarantes aux typologies et risques liés notamment au financement du terrorisme. Ainsi, TRACFIN poursuit une action de pédagogie auprès de ces professions ayant vocation à les sensibiliser sur cette thématique et permettant d'améliorer leur capacité de détection. À ce titre, un comité dédié à la lutte contre le financement du terrorisme (comité LFT) a été mis en place en décembre 2019. Ce comité, composé des principaux établissements de crédit et de paiement et de TRACFIN, est un lieu d'échanges opérationnels sur la thématique LFT (échange sur les critères de détection du risque, sur les nouvelles menaces et la présentation de cas typologiques). Innovation majeure dans les relations entre TRACFIN et les assujettis du secteur financier, la création de ce comité représente une étape substantielle en matière de coopération entre le secteur privé et les pouvoirs publics dans la lutte contre le terrorisme.

Le caractère transnational des réseaux de financement du terrorisme requiert une action coordonnée de l'ensemble des instances internationales et des cellules de renseignement financier

La lutte contre le terrorisme et son financement ont été placés au cœur des priorités sur la scène internationale. TRACFIN a été, dès sa création, impliqué dans le développement d'instances internationales favorisant la coopération, les échanges opérationnels et l'intégration des cellules de renseignement financier (CRF) au sein de ces réseaux.

Créé en 1989, le Groupe d'action financière (GAFI) a pour mission principale l'évaluation du dispositif LCB-FT de chaque pays membre et des progrès réalisés en termes de mise en œuvre des normes dans leurs systèmes législatifs, réglementaires et opérationnels. Membre de la délégation française conduite par la Direction générale du Trésor, TRACFIN apporte une contribution particulière en tant que service opérationnel et développe des typologies relatives au financement du terrorisme qui participent à l'évaluation de la compréhension des risques en la matière.

TRACFIN est également un des membres fondateurs du groupe EGMONT, lequel réunit 166 CRF à l'échelle mondiale, et siège à ce titre au Comité de pilotage du Groupe. EGMONT est un forum d'échange opérationnel qui favorise l'échange de connaissances typologiques et le partage de bonnes pratiques entre les CRF. L'internationalisation de la menace terroriste a initié et renforcé le rapprochement opérationnel entre les différentes cellules de renseignement financier. La forte prise en compte de la dimension internationale de TRACFIN dans ses enquêtes est soulignée par les CRF homologues avec lesquelles le service coopère quotidiennement. TRACFIN est ainsi en mesure d'enrichir les investigations des CRF homologues en leur fournissant des informations pertinentes identifiées par le service, ou d'apporter aux enquêtes en cours au sein de TRACFIN des données détenues par ses homologues. Cette coopération opérationnelle s'inscrit dans le cadre de trois dispositifs : lorsque TRACFIN présente un besoin urgent d'informations sur une personne résidant à l'étranger ou disposant d'un compte à l'étranger ; lorsque TRACFIN signale un individu résidant sur le territoire d'un partenaire et dont les

investigations révèlent des faits de financement du terrorisme ; enfin lorsque le Service doit répondre diligemment à des demandes de notoriété formulées par ses partenaires. À titre illustratif, sur la seule année 2021, TRACFIN a sollicité ses partenaires étrangers plus de 200 fois concernant des dossiers de financement du terrorisme.

En novembre 2022, l'Inde a accueilli la troisième conférence internationale de lutte contre le financement du terrorisme « No Money For Terror » dont la première édition s'est tenue à Paris en avril 2018 à l'initiative du Président de la République. La finalité de ces rencontres était de poursuivre la mutualisation des connaissances sur les risques identifiés en matière de financement du terrorisme par les représentants des 70 États et agences internationales présents, et de mettre à jour les priorités de l'Agenda de Paris, cinq ans après son adoption.

Une action reconnue de la France et de l'ensemble des acteurs impliqués dans lutte contre le terrorisme et son financement

Le Groupe d'action financière (GAFI) a publié le 17 mai 2022 son rapport d'évaluation du dispositif français de LBC-FT. Au terme de cette procédure qui s'est déroulée sur plus de deux ans, la France a obtenu des résultats positifs et se place ainsi au premier rang des pays luttant efficacement contre la criminalité financière et le financement du terrorisme. L'équipe d'évaluation a salué les forces et atouts du dispositif national et le rôle central de TRACFIN tant sur le volet de la lutte contre le blanchiment de capitaux, que sur le plan de la lutte contre le financement du terrorisme et de la prolifération, reconnue comme une priorité nationale.

Plus particulièrement, la qualité et l'exhaustivité des détections et analyses de TRACFIN en matière de micro-financement du terrorisme et la pertinence des informations transmises au niveau opérationnel ont été soulignées, permettant ainsi une bonne utilisation de ces renseignements financiers par les autorités compétentes. Enfin, le rapport du GAFI met en exergue l'organisation cohérente des acteurs de la lutte contre le terrorisme et son financement favorisant ainsi une coopération et une coordination efficace entre TRACFIN et le PNAT, ainsi que le dynamisme de la coopération du service avec les CRF étrangères qui reconnaissent la qualité des informations apportées par TRACFIN. La France a démontré la grande qualité de sa coopération en matière d'enquêtes et poursuites pour financement du terrorisme.

En 2023, TRACFIN recrute.
Rejoignez le Service de renseignement financier de la France

TRACFIN est un service à compétence nationale rattaché au ministre chargé de l'Économie et au ministre chargé du Budget. Il est à la fois l'un des services de renseignement du « 1er cercle » mais aussi la cellule de renseignement financier française (CRF).

TRACFIN poursuit trois missions majeures : la lutte contre la criminalité économique et financière, la lutte contre la fraude aux finances publiques, la défense et la promotion des intérêts fondamentaux de la Nation. À ce titre, TRACFIN recueille et enrichit les informations relatives à des opérations financières suspectes qu'il reçoit d'autres administrations ou des professionnels déclarants (banques, assurances, notaires, etc.) Il transmet ensuite le résultat de ses investigations à l'autorité judiciaire, aux administrations partenaires, à d'autres services de renseignement, ou bien encore à ses homologues étrangers.

Ces dernières années, l'activité de TRACFIN a été marquée par l'augmentation considérable du flux d'informations entrantes (+132% en 5 ans). En 2021, le service a reçu 165 171 déclarations de soupçons. Au terme de ses investigations, TRACFIN a transmis 3242 notes à ses partenaires (+24% en 5 ans).

Afin de faire face à cette croissance et aux enjeux imposés par les missions qui lui sont confiées, TRACFIN recrute de nouveaux agents en 2023. Les profils recherchés sont variés, au même titre que les domaines au sein desquels ils seront amenés à évoluer.

Plusieurs postes sont notamment proposés au sein de la Mission Internationale et Études (MIE), unité chargée de définir les priorités et les orientations stratégiques internationales de TRACFIN et de contribuer à son rayonnement au plan international en participant notamment à l'animation de son réseau auprès des institutions, de forums d'échanges ou de ses partenaires étrangers. D'importantes échéances internationales attendent TRACFIN d'ici 2024, notamment autour de la candidature de Paris pour accueillir le siège de la future Autorité européenne de lutte contre le blanchiment d'argent (AMLA) et de l'organisation de la plénière du groupe EGMONT, le forum d'échange opérationnel pour les cellules de renseignement financier, qui doit se tenir à Paris en 2024.

Au ministère de l'Économie et des finances, mettez votre talent au service d'une économie forte et durable #ChoisirLeServicePublic. Retrouvez l'ensemble des opportunités proposées sur passerelles.economie.gouv.fr, ainsi que sur le compte Linkedin @TRACFIN.

DÉSTABILISER L'EUROPE PAR L'INFORMATION : UN EXEMPLE SOUS LE PREMIER EMPIRE

Dr HDR Gérald ARBOIT
Enseignant et chercheur, équipe Sécurité Défense Renseignement, criminologie, crises, cybermenaces (ESDR3c), Conservatoire national des Arts et Métiers, Paris.

Alors que l'Europe semble découvrir que, depuis 2014 au moins, elle est la cible d'une déstabilisation informationnelle de la Russie, il est peut-être utile de revenir sur les ressorts d'une opération similaire parvenue sous le Premier Empire, à une époque où n'existaient pas les services de renseignement, ni les usines à troll. Elle prend place en Espagne et est actionnée par les Britanniques. Cette décision politique s'inscrivait dans la suite des opérations militaires depuis 1807 en mer du Nord, ainsi que dans l'analyse faite à Londres, par l'ancien ambassadeur à Madrid et actuel ministre près la *Junta Suprema de España e Indias* de Séville, John Frere. Malgré la défaite militaire britannique de La Coruña (16 janvier 1809) et le repli défensif sur le Portugal, Londres refusa de s'avouer battue, décidant de « mettre le feu à l'Europe » pour espérer abattre Napoléon. Frere ne mesura certainement pas la portée réelle de ce qu'il allait déclencher en proposant « la publication d'un ou deux livres » sur la situation espagnole[12]. Il souhaitait légitimer l'opération britannique auprès de son « opinion publique » et amener les Espagnols à mettre les gazettes de Cadix, de Valence et de Badajoz au service de cette bataille de l'information. Sur le plan continental, il s'agissait d'influer sur le centre de gravité français qui s'était déplacé sur l'espace germanophone depuis le décentrement impérial de 1805. L'effet final recherché était d'assurer du soutien opérationnel de l'armée britannique les « opinions publiques » européennes qui voudraient suivre l'exemple espagnol. Déjà multiscalaire, ces dernières se formaient des journaux, revues, livres et affiches. Partout contrôlés et censurés, ils étaient souvent conduits à suivre les mêmes routes que la contrebande coloniale. La propagande hispano-britannique se déversa donc sur un continent hermétiquement fermé par les douanes impériales.

L'Autriche prit une place particulière dans la stratégie espagnole britannique[13]. Elle animait des réseaux dormants et des dépôts d'armes clandestins les États de la plaine allemande[14]. Son intérêt pour l'Espagne rebelle fut évident avec le ralliement de son représentant, Wilhelm, Genotte à la *Junta*. Elle disposait ainsi d'une capacité autonome d'analyse des événements espagnols. Non seulement le ministre des Affaires étrangères, Philipp v. Stadion, autorisa la publication de la propagande espagnole[15], mais il mit en œuvre toutes les conditions d'une bonne diffusion dans tout le monde germanophone. En prévision des opérations clandestines prévues au Tyrol et en Allemagne[16], prélude du retour de l'Autriche dans la V^e^ Coalition, la propagande autrichienne s'articula autour d'un pamphlet bourboniste du sous-lieutenant José Palafox offrant la couronne espagnole à l'archiduc autrichien Carl, au cas où les Borbón retenus en

[12] The National Archive (TNA), Londres, FO 95/470 et Archivo Histórico Nacional (AHN), Madrid, Estado, 5608, Frere à Bathurst, 25/12/1809.
[13] Patrick Swoboda, *Englische Subsidien an die Habsburgermonarchie in den antifranzösischen Koalitionskriegen 1792-1815* [Les subsides britanniques à la monarchie habsbourgeoise dans les coalitions antifrançaises 1792-1815], Doctorat, Philosophie, Université de Vienne, 2014, p. 203 ; *Papers respecting Austria... presented to Parliament*, Londres, Stratham, 1808, p. 1-29.
[14] AHN, Estado, 5934, Urquijo à Campo-Alange, sd (fin 04/1809).
[15] Österreichisches Staatsarchiv (OeStA), Vienne, Notenwechsel, Polizeihofstelle, 25, Stadion à Hormayer et Hormayer à Stadion, fin 12/1808 et 24/01/1809 ; *Ibid.*, Allgemeines Verwaltungsarchiv, Polizeihofstelle, 3104/c/1809, note du 22/03/1809 ; AHN, Estado,5878, Lellis à Cevallos, 24/02/1809 et Estado, 6204, Megino à Cevallos, 28/02/1809.
[16] *Ibid.*, Preußen Diplomatische Korrespondenz, 92, Bombelles à Stadion, 20 et 27/12/1808.

France vinssent à être tués[17], et la publication d'un *Armee Befehl* (Ordre à l'armée).

Stadion se montra plus soucieux de répondre aux ouvertures anglaises à Vienne que de répondre à celles émanant de la *Junta* de Séville[18]. Il n'empêcha pas la circulation de la propagande espagnole en Autriche, et ne put empêcher qu'elle fit des émules à Vienne, jusqu'au commandant en chef de l'armée, l'archiduc Ferdinand de Modène-Este, frère de l'impératrice. Cette proximité avec le souverain permit que le dossier espagnol fût temporairement retiré à Stadion par Franz II en novembre 1808[19] et qu'un « émissaire » fût envoyé en Espagne. Le *HauptLeute* (entre capitaine et commandant) Louis de Crossard[20] devait assurer une liaison avec les Britanniques et apprendre des Espagnols les techniques de guérilla[21]. Au début du printemps 1810, Crossard était rentré à Vienne, sans que sa mission fût connue des Français avant septembre 1810[22].

Pareillement, l'opération d'influence autrichienne était déjà bien avancée lorsque, depuis Berlin, le 23 novembre 1808, le maréchal Davout annonça à Napoléon que « les grands moyens utilisés [furent] les affaires d'Espagne »[23], loin de se douter que ce mouvement d'« hispanisation » atteindrait une ampleur telle à fragiliser l'édifice impérial français De Dresde, on remarqua combien elle se diffusa « avant que la légation française elle-même ait eu connaissance de cette diffamation »[24]. Mal calibrée, la réponse française, confiée par Davout à un « partisan convaincu de Napoléon »[25] dans l'espace germanophone, l'éditeur Johann Friedrich Cotta, ne fit qu'amplifier le ressentiment contre la France. À l'été 1809, « sous les auspices du gouvernement français »[26], elle prit la forme d'une réponse adressée à un mémoire de Pedro Guerra de la Vega[27]. Pourtant, le pamphlet du dernier secrétaire d'État de Carlos IV avait été imprimé à Vienne pour être diffusé « dans toute l'Europe lors de la retraite du Roi, en 1808 ». Manquant sa cible, cette réponse fut traduite en français[28] et en allemand[29], montrant que Paris avait compris que l'objectif hispano-britannique était la plaine germano-polonaise, peut-être en liaison avec les insurrections savamment préparées par l'Autriche et la Prusse[30] (avril-mai 1809). Ce fut le sentiment de l'ambassadeur espagnol joséphiste à Berlin, Rafael de Urquijo, qui remarqua aussi que la circulation clandestine de ces brochures se ralentît dans la durée (1809-1811)[31].

[17] *Ibid.*, 87, Metternich à Cobenzl, 07/12/1805 ; *Ibid.*, Frankreich Diplomatische Korrespondenz, 203, Metternich à Stadion, 26/06/1808 ; Richard de Metternich, de Klinkowstroem, *Memoires. Documents et écrits divers laissés par le Prince de Metternich...*, 2, Paris, Plon, 1880, p. 81.

[18] *Ibid.*, Spanien Diplomatische Korrespondenz, Varia, 64, Note de la *Junta*, 27/08/1808.

[19] *Ibid.*, Vorträge, 180, Stadion à Franz, 03/11/1808 et réponse Franz écrite par Stadion, 13/11/1808.

[20] *Ibid.*, Stadion à Franz, 10, 12 et 26/12/1808.

[21] *Ibid.*, Vorträge, 182, Metternich à Franz, 06/08/1809.

[22] Alexandre Wassiltchikow, *op. cit.*, 3, *1806-1839*, 1894, p. 117 ; Nicole Gotteri, *op. cit.*, 1, 1997, p. 328.

[23] Service historique de la Défense (SHD), Vincennes, 2 C 81.

[24] *Ibid.*, 2 C 84.

[25] Bernhard Fischer, *Johann Friedrich Cotta: Verleger-Entrepreneur-Politiker*, Göttingen, Wallstein Verlag, 2014, p. 327.

[26] AD, CP Espagne, 683, La Forest à Champagny, 30/08/1809.

[27] *Observaciones sobre las causas inmediatas que han provocado el cambio de Dinastía y la Insurreccion en la España, dirigido á Pedro Cevallos*, Paris, 1809. Remedios Solano Rodríguez, *La influencia de la Guerra de la Independencia en Prusia a través de la prensa y la propaganda: la forjadura de una imagen sobre España (1808-1815)*, Doctorat, Sciences de l'Information, Madrid, 2014, p. 296-297.

[28] *Observations sur les causes immédiates du changement de dynastie et de l'insurrection de l'Espagne. Adressées à don Pedro Cevallos*, Tubingen, Cotta, 1810.

[29] „Observaciones fue Bemerkungen über die unmittelbaren Ursachen der Dynastie-Veränderung und der Insurrektion in Spanien, gerichtet an Pedro Cevallos", *Europäische Annalen*, 01-10/1810, p. 40-66, 124-173, 90-96, 217-233, 82-93.

[30] OeStAKriegsakten, 423-1, Buol-Schauenstein à Stadion, 26/04, 28/05, 5 et 17/06/1809; *Ibid.*, Preußen Diplomatische Korrespondenz, 91, Bombelles à Stadion, 20 et 27/12/1808 ; 92, Wessenberg à Stadion, 27/04/1809. AD, CP Prusse, 244, Saint-Marsan à Champagny, 27/03/1809 ; Archives nationales, Paris, AF^{IV} 1690, 13-18/03/1809.

[31] AHN, Estado, 5935, Urquijo à Campo-Alange, sd [fin 04/1809] et 03/12/1811.

Surtout, l'audience de la propagande hispano-britannique devint un exemple pour l'organisation des revanches militaires prussienne et russe contre la France. Avant d'être exfiltré vers la Russie, le propagandiste Ernst Moritz Arndt obtint des documents d'Espagne[32]. L'exemple espagnol suscita également un intérêt en Russie. Dès février 1811, le capitaine d'état-major Paisiy Kaisarov transposa dans un rapport la *guerilla* espagnole en une théorie de « guerre des partisans »[33], qu'il mit en œuvre un an et demi plus tard à la tête des Cosaques[34], invitant à « regarde[r] (…) l'Espagne et le Portugal »[35]. Elles constituèrent même un aiguillon au soulèvement de la plaine germano-polonaise, dirigée par un *Deutsches Komitee*, constituée par la Russie[36].

Avec l'Espagne et la Russie, la « petite guerre » devint guérilla, se nimbant d'un appareil propagandiste qui appelait une réponse physique et cognitive. À partir de 1808, chaque coup porté aux troupes françaises se doublait d'un retentissement éditorial à travers toute l'Europe. Ainsi, cette réflexion établie à Cadix après la publication dans *The Times* du 17 mai 1811 de l'état des troupes françaises entrées en Espagne depuis 1807 et qui se voulut un appel en langue française aux « peuples du Continent (…) Allemands, Hollandais, Italiens[37]. » Dès octobre 1810, le chargé d'affaires à Francfort, Bacher, décrivit clairement, pour l'Allemagne[38], comment cette propagande amplifiât l'échauffement des esprits induits par les effets de la conscription, de la crise économique et de la lutte contre la contrebande. Ces derniers expliquaient à eux-seuls le succès des sociétés secrètes d'émanation prussienne, comme le *Deutschen Bund*. Et la réponse uniquement répressive (fusillant des libraires et des directeurs des postes), sans le soutien de relais peu francisées comme la gendarmerie et la douane, recrutées localement, ne permit évidemment pas de rétablir la paix civile. En 1813, lorsque les contingents retraités de Russie traversèrent l'espace allemand, il n'était plus temps de réformer des élites administratives adhérant à la propagande hispano-britannique, sinon austro-prussiennes, en tout cas séduites par des discours façonnés à leur intention dans les universités prussiennes. L'effondrement du système français avait commencé cinq ans auparavant !

[32] Arndt à Reimer, 11/06/1811, *in* Heinrich Meisner, Robert Geerds (éds.), *Ernst Moritz Arndt. Ein Lebensbild in Briefen. Nach ungedruckten und gedruckten Originalen*, Berlin, Georg Reimer, 1898, p. 65, et à Kathen, 19/06/1811, *in* Albrecht Dühr (éd.), *Ernst Moritz Arndt Briefe*, Darmstadt, Wissenschaftliche Buchgesellschaft, 1972, 1, p. 181-182.

[33] Центральный государственный архив литературы и искусства (Archives centrales d'État de la littérature et de l'art), Saint-Pétersbourg, fond 79, opis 1, delo 56.

[34] Alexander Mikaberidze, *Russian Officer Corps of the Revolutionary and Napoleonic Wars*, New York, Savas Beatie, 2005, p. 174-175.

[35] Richard Stites, *The Four Horsemen. Riding to Liberty in Post-Napoleonic Europe*, Oxford, Oxford University Press, 2014, p. cxliv.

[36] Aleksandr à Stein, 20/06/1812 et mémoires de Stein, 16 et 27/06/1812, *in* Georg Heinrich Pertz (ed.), *op. cit.*, 3, p. 74-75 et 68, 87-91.

[37] *Pertes des franzois en Espagne, et coup d'oeil sur les principaux evenements de la guerre dans la Peninsule jusqu'à la fin d'aout 1811*, Cadix, Impr. royale, s.d. [1811], p. 37.

[38] AD, CP Allemagne, 740.

LE RÔLE DES SERVICES DE RENSEIGNEMENT FRANÇAIS DANS LA LUTTE CONTRE LES GROUPES TERRORISTES

Louise MASSON
Analyste à l'Institut d'études de géopolitique appliquée.

La Stratégie nationale du renseignement (SNR) établie en 2019 définit la lutte contre le terrorisme comme la priorité des services de renseignement[39], le renseignement étant une composante essentielle dans la stratégie globale de lutte anti-terroriste. Cette menace terroriste est particulièrement portée par les groupes jihadistes, principalement l'État islamique et d'Al-Qaïda. Le renforcement capacitaire de ces groupes, le maintien de leurs capacités financières et la force de leurs outils de propagande constituent une menace pour la France, ses intérêts à l'étranger et sur les théâtres d'opérations où ses forces sont engagées. D'après Bernard Émié, directeur général de la sécurité extérieure, la menace jihadiste s'inscrit aujourd'hui dans un « *continuum* transfrontalier et relationnel » entre les terroristes présents sur les terres de jihad et les individus radicalisés sur le territoire national[40]. Les menaces « projetée »[41] et « inspirée »[42] étant des conséquences de ce *continuum*. Ainsi, cette notion de *continuum* intérieur et extérieur est fondamentale afin de comprendre la lutte anti-terroriste et impose une coopération forte et quotidienne entre les services intérieurs et extérieurs.

Cet article a pour objectif de se concentrer sur la dimension extérieure de la lutte contre le terrorisme, cette menace exogène se situant dans des régions souvent instables, telles que la bande sahélo-saharienne, le Levant, la Péninsule arabique, la Somalie, la zone afghano-pakistanaise et l'Asie du Sud-Est. Dans ces régions, les groupes terroristes constituent une menace pour les militaires français qui y sont positionnés[43], les ressortissants et intérêts français[44], ainsi que pour le territoire national[45]. La sécurité de la France se joue ainsi à l'extérieur de ses frontières[46]. Ainsi, comment les services de renseignement luttent-ils contre les groupes terroristes se développant sur les terres de jihad ?

Les principaux acteurs

La Direction générale de la sécurité extérieure (DGSE) et la Direction du renseignement militaire (DRM) sont les deux services principaux en charge de la lutte contre le terrorisme à l'extérieur des frontières nationales.

D'une part, la DRM, service de renseignement des armées, œuvre à accompagner les forces armées sur le plan opérationnel ainsi qu'à éclairer la prise de

[39] *CNRLT*. (2017). Élysée. https://www.elysee.fr/cnrlt.
[40] Emié, B. (2017). Le rôle de la DGSE dans la lutte contre le terrorisme. L'ENA hors les murs, 472.
[41] La menace jihadiste projetée correspond à une attaque en France, planifiée et projetée depuis une zone de jihad.
[42] La menace inspirée correspond à une attaque non-planifiée, peu sophistiquée, commis dans le pays de résidence de l'assaillant, en réponse à un appel de passage à l'action par des groupes jihadistes. Emié, B. (2017). Le rôle de la DGSE dans la lutte contre le terrorisme. *L'ENA hors les murs*, *472*.
[43] Depuis 2013, 58 soldats français ont perdu la vie au Sahel dans le cadre des opérations Serval et Barkhane.
[44] Depuis 2010, 19 ressortissants français ont été pris en otage par des organisations jihadistes au Sahel.
[45] Les attentats de Bataclan sont une conséquence directe de l'établissement du Califat de l'État Islamique en zone syro-irakienne.
[46] Emié, B. (2017). Le rôle de la DGSE dans la lutte contre le terrorisme. L'ENA hors les murs, 472.

décisions des autorités politiques et militaires. Ainsi, elle fournit le renseignement nécessaire à « la planification et à la conduite de la manœuvre militaire » et assure « une veille stratégique permanente »[47]. La DRM oriente ses capteurs sur les cibles jihadistes identifiées, principalement les filiales de l'État islamique et d'Al-Qaïda, tels que le RVIM et l'EIGS au Sahel, afin de connaître leurs positions, leurs moyens et effectifs, leurs activités et plans. Ces renseignements sont essentiels aux forces armées, sans qui elles seraient vulnérables aux attaques jihadistes. D'autre part, la DGSE a pour but de recueillir et d'exploiter le renseignement afin de détecter les acteurs agissant sur les théâtres de jihad et de détecter la menace en dehors des frontières de la France[48]. Pour cela, son rôle est d'identifier et suivre les groupes, en cartographiant leurs relations et d'entraver les projets terroristes[49].

Les moyens et méthodes des services de renseignement

Afin de remplir leur mission de lutte anti-terroriste, les services de renseignement utilisent des capteurs, qu'ils orientent en fonction des besoins des autorités politiques et militaires. Ces capteurs peuvent être d'origine image (fournies à la fois par des moyens aériens et des satellites), d'origine électromagnétique (écoutes téléphoniques, surveillance de communications permettant d'identifier des cibles terroristes à haute valeur ajoutée[50]), d'origine humaine ou de source ouverte. Au terme de la collecte effectuée grâce aux sources, les analystes traitent l'information en la recoupant et la comparant pour obtenir un renseignement.

Enrichies par les renseignements obtenus, les services ont recours aux méthodes de ciblage et d'entrave afin de combattre les groupes terroristes. D'après Philippe Hayez, le ciblage s'est imposé comme essentiel dans les services de renseignement afin de se concentrer sur « les personnes, leur identité, leur position, leur comportement, leurs contacts, leurs finances »[51]. La connaissance des services de l'État islamique et d'Al-Qaïda est indispensable afin de prévenir leurs mutations, alliances et projets. Notamment, la DGSE a pu identifier une réunion des chefs d'Al-Qaïda au Sahel en février 2020, au cours de laquelle ils auraient « conçu leur projet d'expansion vers les pays du Golfe de Guinée »[52]. Par ailleurs, l'entrave représente la capacité des services à empêcher la concrétisation d'une menace en y mettant fin[53]. L'entrave est indissociable des services de renseignement car elle est mise en œuvre soit par les renseignements eux-mêmes, soit par les autorités politiques ou forces militaires en s'appuyant sur les renseignements fournis. La DGSE aurait ainsi éliminé directement ou indirectement près de quatre-vingts jihadistes au Sahel entre 2012 et 2014[54].

Les coopérations internationales en matière de renseignement : l'exemple du Sahel

[47] Nos missions. (s. d.). Ministère des Armées, Direction du Renseignement Militaire. https://www.defense.gouv.fr/drm/nos-missions.
[48] Émié, B. (2017). Le rôle de la DGSE dans la lutte contre le terrorisme. L'ENA hors les murs, 472.
[49] *Ibid*.
[50] Mauborgne, S., & Serre, N. (2021). Rapport d'information par la commission de la défense nationale et des forces armées sur l'Opération Barkhane.
[51] Hayez, P. (s. d.). Les services de renseignement français : Quel dispositif contre le terrorisme ? République française : Vie publique. https://www.vie-publique.fr/parole-dexpert/268362-renseignement-francais-quel-dispositif-contre-le-terrorisme.
[52] Crebessegues, F. (2021). Les services de renseignement français lèvent (un peu) le voile sur leur activité au Sahel. TV5MONDE. Consulté 12 avril 2022, à l'adresse https://information.tv5monde.com/video/les-services-de-renseignement-francais-levent-un-peu-le-voile-sur-leur-activite-au-sahel.
[53] La stratégie nationale du renseignement. (2019). Présidence de la République. https://www.economie.gouv.fr/files/20190703-cnrlt-np-strategie-nationale-renseignement.pdf.
[54] Notin J.-C. (2014), La Guerre de la France au Mali, Paris, Tallandier.

La coopération internationale est un moyen fréquemment utilisé en tant que moyen d'influence et en tant que ressource stratégique vitale pour compléter le cycle du renseignement français[55]. Cette coopération peut être effectuée sous la forme de « partage d'informations, la coopération opérationnelle clandestine, le partage d'équipement et de sites d'installation, la formation et la coopération technologique »[56]. La coopération en matière de renseignement est structurée par des accords formels ou des réunions occasionnelles ou régulières, qui restent très souvent bilatérales, en raison de la sensibilité de la matière. La France dispose de l'ensemble des capacités de renseignement disponibles : militaires et civils, intérieurs et extérieurs, humains et techniques. Elle représente donc un partenaire stratégique de choix pour des États n'ayant pas des capacités aussi développées. C'est ainsi que les forces conjointes du G5 Sahel s'appuient massivement sur la coopération en matière de renseignement avec la France. Cependant, bien que ses capacités soient complètes, la France fait également appel à des partenaires dans ce domaine, tels que les États-Unis, afin de renforcer ses opérations et réduire l'incertitude.

L'appui aux forces du G5 Sahel

Le G5 Sahel est une initiative régionale ayant pour but d'endiguer le terrorisme dans la région, en coordonnant les politiques de sécurité et de développement. La force conjointe en constitue le volet militaire. La force Barkhane appuie la force conjointe dans le domaine du renseignement principalement par appui aérien, en matière d'intelligence, de surveillance et de reconnaissance (ISR). En effet, ce soutien est indispensable tant le volet renseignement des pays du Sahel constitue un défi et une faiblesse pour ces pays, leurs seules sources de renseignement étant humaines[57]. Ainsi, au Sommet de Pau de 2020, le Mécanisme de commandement conjoint (MCC) a été déployé à Niamey, au sein duquel se trouve une nouvelle cellule de renseignement — la *Intelligence Fusion Cell* (IFC), qui est composée de personnels de renseignements sahéliens, français et américains[58]. La IFC est opérationnelle depuis mars 2020[59]. Cette cellule a permis de fluidifier le partage du renseignement et de faire face aux besoins des États du Sahel qui restent dépendants des renseignements étrangers. Il serait cependant bénéfique d'accroître le nombre de personnels au sein de l'IFC, ainsi que d'augmenter le volume de données qui lui sont transmises[60].

Ainsi, l'accroissement des capacités de renseignement des forces sahéliennes est indispensable afin d'assurer une continuité dans le futur. De même, les partenaires sahéliens sont souvent plus à même de comprendre les dynamiques internes à leurs pays et d'alimenter des réseaux de collecte de renseignement humain plus riches que les forces extérieures. Ainsi, le soutien apporté par la France est en outre opéré à travers la

[55] Oudet, B. (2018). Les coopérations internationales françaises de renseignement face aux nouvelles menaces. Les Champs de Mars, 27-35. https://doi.org/10.3917/lcdm.030.0158.

[56] *Ibid*.

[57] Compte rendu Commission de la défense nationale et des forces armées—Audition, à huis clos, du général Oumarou Namata Gazama, commandant de la force conjointe du G5 Sahel. (2020). Assemblée Nationale. https://www.assemblee-nationale.fr/dyn/15/comptes-rendus/cion_def/l15cion_def2021024_compte-rendu.pdf.

[58] Ollivier, B. (2021). Les implications de la mise en place de la Force-Conjointe du G5 Sahel sur la MINUSMA et les contributeurs régionaux. Observatoire Boutros-Ghali du maintien de la paix. https://www.observatoire-boutros-ghali.org/sites/default/files/Note%20OBG%20MINUSMA-FC_Bertrand.Ollivier.pdf.

[59] MAUBORGNE, S., & SERRE, N. (2021). Rapport d'information par la commission de la défense nationale et des forces armées sur l'Opération Barkhane.

[60] Compte rendu Commission de la défense nationale et des forces armées—Audition, à huis clos, du général Oumarou Namata Gazama, commandant de la force conjointe du G5 Sahel. (2020). Assemblée Nationale.

formation d'officiers des forces locales au renseignement. En effet, dans le cadre de partenariats bilatéraux la DRM a instauré des actions de mentorat et de formation.

Les États-Unis : un acteur primordial pour la coopération au Sahel

Au Sahel, les États-Unis misent sur le concept « d'empreinte légère », pariant sur le renseignement et la logistique. Afin de soutenir la France plus lourdement engagée au Sahel, les États-Unis offrent une aide significative et essentielle dans le domaine du renseignement. Sans le soutien de l'armée de l'air américaine, les forces de Barkhane rencontreraient des difficultés dans la conduite des opérations[61]. En effet, d'après le Général Trinquand, l'étendue de la zone rend impossible la permanence du renseignement au Sahel[62].

Ainsi, les moyens américains sont cruciaux pour frapper les jihadistes au Sahel, notamment les drones reaper américains qui sont basés au Niger à Agadez et à Niamey. En effet, en 2016 les États-Unis annonçaient la création d'une base militaire à Agadez de 100 millions de dollars. Cette base est le siège des programmes de drones et de surveillance opérant au Niger, au Mali, en Libye et au-delà[63]. Au-delà des capteurs d'imagerie, les États-Unis ont déployé des moyens d'écoute électromagnétique, avec des bimoteurs capables de capter toutes les communications radio sur leur passage[64].

À titre d'exemple de la coopération franco-américaine, l'opération ayant menée à la mort d'Abou Walid al-Sahraoui, ancien chef de l'EIGS, a été menée par les forces françaises, mais appuyée par des renseignements américains qui ont aidé à l'identification de la cible et de sa localisation.

En définitive, les services de renseignement représentent un appui indispensable aux forces armées françaises dans la lutte contre le terrorisme jihadiste. Tel que le décrit Bernard Émié, « le renseignement s'inscrit dans une stratégie globale de sécurité et de défense »[65]. Au sein de la communauté française du renseignement, la DRM et la DGSE sont les acteurs principaux du renseignement extérieur, à travers leurs capacités de collecte par des sources d'origine électromagnétique, image et humaine, capable d'entraver les actions des groupes jihadistes. En ce sens, la coopération internationale en matière de renseignement est déterminante pour capitaliser les moyens techniques et humains afin de neutraliser des cibles terroristes.

[61] Oudet, B. (2018). Les coopérations internationales françaises de renseignement face aux nouvelles menaces. Les Champs de Mars, 27-35.

[62] Boisbouvier, C. (2021, septembre 21). Invité Afrique - Général Trinquand : « Le combat au Sahel est stratégique pour la France et très utile pour les Américains ». RFI. https://www.rfi.fr/fr/podcasts/invit%C3%A9-afrique/20210921-g%C3%A9n%C3%A9ral-trinquand-le-combat-au-sahel-est-strat%C3%A9gique-pour-la-france-et-tr%C3%A8s-utile-pour-les-am%C3%A9ricains.

[63] Mohanty, A. (2020, avril 7). Why Is the US Military Fighting in Niger? Geopolitical Monitor. https://www.geopoliticalmonitor.com/why-is-the-us-military-fighting-in-niger/.

[64] Sahel : Les États-Unis s'engagent à renforcer la coopération antiterroriste. (2021, septembre 23). RFI. https://www.rfi.fr/fr/afrique/20210923-sahel-les-%C3%A9tats-unis-s-engagent-%C3%A0-renforcer-la-coop%C3%A9ration-antiterroriste.

[65] Emié, B. (2017). Le rôle de la DGSE dans la lutte contre le terrorisme. L'ENA hors les murs, 472.

LE RENSEIGNEMENT INTERNATIONAL DANS LA LUTTE CONTRE LE TRAFIC ILLICITE DES BIENS CULTURELS

Emerancia NTUMBA
Analyste au sein du département diplomatie culturelle et interculturalité de l'Institut d'études de géopolitique appliquée.

Dans une enquête[66] réalisée en 2020, *l'Organisation internationale de police criminelle* (ci-après « INTERPOL ») a évalué les chiffres de la criminalité internationale visant le trafic illicite des biens culturels. Est considéré comme un bien culturel, un bien qui « présente une grande importance pour le patrimoine culturel des peuples »[67] : il alors question de monuments d'architectures, d'œuvres d'art, de manuscrits, livres ou autres objets d'intérêt artistique, historique ou archéologique etc. À partir d'informations transmises par 72 pays membres d'INTERPOL sur les atteintes aux biens culturels, les fouilles, les arrestations et les itinéraires de trafic, l'enquête a révélé que 854 742 objets culturels avaient été saisis et plus de la moitié ont été saisis en Europe. Sur les autres continents (Afrique, Amériques, Asie et Pacifique Sud), un net accroissement du nombre de fouilles illicites a également été observé par rapport à 2019.

Dans sa lutte contre la criminalité, le renseignement international cible également le trafic illicite des biens culturels. Il s'intéresse alors au recueil d'informations qualitatives, à leur analyse, à l'indentification de leur facteurs (lieux, acteurs, causes) ou encore à la définition des priorités d'actions pour adopter une réponse policière à la menace[68]. Ces informations sont opérationnelles lorsqu'elles permettent aux autorités compétentes de développer, d'ajuster et appliquer leurs stratégies contre les menaces de sécurité. Plus largement, on peut associer le renseignement à d'autres domaines d'expertise policière tels que les investigations, la recherche, la formation ou encore la prévention. En d'autres termes, le renseignement peut désigner « *l'ensemble des informations et faits révélés et analysés par le travail des services dans le but de prévenir les atteintes aux intérêts (d'une) Nation, de protéger les personnes, les biens et les institutions et de défendre et promouvoir les intérêts d'un État* »[69]. Depuis les années 1990, le modèle de police est guidé par le renseignement ou *intelligence-led policing* (ILP) favorisant une démarche policière « *proactive, tournées vers la recherche et l'anticipation des facteurs d'insécurité* »[70]. Ce récent modèle vise à s'adapter à la modernité et à la complexité de la criminalité organisée notamment dans le cadre du trafic illicite des biens culturels.

En 2023, à l'ère de l'économie numérique et dans un contexte de pandémie et de conflits terroristes, le trafic des biens culturels s'intensifie et se complexifie. En effet, il se caractérise par « *son aspect protéiforme et un large spectre infractionnel* »[71]. Ce trafic inclut la commercialisation des biens d'origine frauduleuse (vols, pillages), la fouille illicite des sites culturels, le trafic des biens culturels contrefaits ou encore le trafic des biens

[66] Évaluation de la criminalité visant les biens culturels en 2020, Enquête auprès des pays membres d'INTERPOL, INTERPOL, Septembre 2021.
[67] Article Premier, Convention de La Haye pour la protection des biens culturels en cas de conflit armé, UNESCO, 14 mai 1954, La Haye, Pays-Bas.
[68] La France et le renseignement criminel : entre volonté et réalité, une ambition à écrire, C. de MAILLARD, Sécurité et Stratégie, 2014/2 (17), pp. 49-59.
[69] La stratégie nationale du renseignement, Coordination Nationale du Renseignement et de la lutte contre le terrorisme, Présidence de la République, Juillet 2019, p. 1.
[70] *Ibid*.
[71] Plaquette Office Central de lutte contre le trafic des biens culturels, ministère de l'Intérieur.

archéologiques en provenance des zones de conflit, populairement appelés les « *antiquités du sang* »[72].

Instrument de souveraineté des États[73], le renseignement intervient pour constituer les informations opérationnelles dans l'optique de préserver et de protéger le patrimoine culturel des États. Dans la défense de ces principes nécessitant la mise en place de stratégies de coopération internationale, se forme un réseau d'acteurs opérationnels et polyvalents.

Une lutte au cœur des préoccupations internationales

Une lutte portée par les traités internationaux

De nombreux accords internationaux portent sur la lutte contre le trafic illicite des biens culturels. La Convention de La Haye[74] de l'Unesco de 1954 (complétée par deux protocoles de 1954 et 1999) est le premier texte consacré exclusivement à la protection du patrimoine culturel. Les Hautes Parties contractantes s'engagent dans « la sauvegarde des biens culturels situés sur leur propre territoire contre les effets prévisibles d'un conflit armé » (art 3). Les États sont amenés à communiquer des données techniques, des rapports et faire des signalements auprès de la Commission générale aux biens culturels. Elle précède la Convention de 1970[75] : ratifiée par 141 États, cette dernière les exhorte à adopter des mesures de protection des biens culturels sur leur territoire (art.5), de contrôler la circulation des biens culturels (art.6-9) et contribuer à la restitution des biens culturels obtenus illicitement (art.7). Une coopération internationale est requise puisque les États parties s'engagent à participer à toute « opération internationale concertée » pour venir en aide aux États dont le patrimoine culturel est mis en danger (art.9). La Convention de 1970 est devenue le pilier d'un « ordre culturel international »[76]. De cet ordre, naît aussi un « droit à la souveraineté culturelle »[77]. L'influence de la Convention de 1970 est telle qu'en 2019, l'UNESCO a consacré le 14 novembre comme *Journée internationale de lutte contre le trafic illicite des biens culturels*[78]. Par ailleurs, la Convention d'Unidroit de 1995[79] s'affirme également comme un texte indispensable. Adoptée par des États désireux de collaborer afin d'établir des règles juridiques communes dans la défense des restitutions et des retours des biens culturels, elle vise à « maintenir une juste place au commerce licite et aux accords interétatiques dans les échanges culturels ». Cet objectif passe notamment par une coopération judiciaire internationale (art.5).

Dès lors, le domaine du renseignement s'imprègne de cet environnement juridique propice à la collaboration internationale et donc à l'échange d'informations opérationnelles sur le trafic illicite des biens culturels.

Une lutte liée aux enjeux contemporains

Le trafic illicite des biens culturels est lié à d'autres activités criminelles telles que la contrebande de drogues et d'armes, la violence, la corruption et le blanchiment d'argent[80]. À ce propos, les Nations

[72] Trafiquants d'art, trafiquants d'âme, Le Courrier de l'UNESCO, 2020-4.
[73] La France et le renseignement criminel : entre volonté et réalité, une ambition à écrire, C. de MAILLARD, Sécurité et Stratégie, 2014/2 (17), pp. 49-59.
[74] Convention de La Haye pour la protection des biens culturels en cas de conflit armé avec règlement d'exécution, UNESCO, 14 mai 1954, La Haye, Pays-Bas.
[75] Convention concernant les mesures à prendre pour interdire et empêcher l'importation, l'exportation et le transfert de propriété illicites de biens culturels, UNESCO, Conférence générale à sa seizième chambre, 14 novembre 1970, Paris, France.
[76] « Convention de 1970 : la diversité culturelle avant la lettre », Vincent Negri, « *Trafic illicite des biens culturels, 50 ans de lutte* », Le Courrier de l'UNESCO, UNESCO, 2020, p. 10.
[77] *Ibid*.
[78] Actes de la Conférence générale, 40e session, Unesco, Paris, 12 novembre-27 novembre 2019, volume 1 : Résolutions.
[79] Convention d'Unidroit sur les biens culturels volés ou illicitement exports, 24 juin 1995, Rome, Italie.
[80] « Application de la Convention des Nations Unies contre la criminalité transnationale organisée pour la protection contre le trafic de biens culturels »,

unies ont essayé d'appliquer la *Convention des Nations unies contre la criminalité transnationale organisée* (CNUCTO) à la protection des biens culturels et se sont déclarées préoccupées par les liens entre la criminalité organisée et le trafic illicite de biens culturels. Nous nous intéresserons ici plus particulièrement aux liens entretenus avec la cybercriminalité et le terrorisme.

En 2006, le Groupe d'experts INTERPOL (GEI) sur les biens culturels volés a pour la première fois soulevé une discussion sur le trafic illicite d'objets culturels sur internet[81]. Par la suite, l'UNESCO, INTERPOL et le Conseil international des musées (ci-après « ICOM ») ont coopéré pour diffuser des *Mesures élémentaires concernant les objets culturels mis en vente sur Internet* permettant de prévenir le trafic et d'accroître la « surveillance d'internet » en insistant notamment sur la tenue de statistiques, l'enregistrement d'informations et la mobilisation des plateformes numériques. Près de vingt ans plus tard, on constate que le trafic de biens culturels continue d'exploser sur internet[82] (notamment dans un contexte de pandémie). En 2019, un rapport[83] de l'Athar Projet recensait 95 groupes Facebook consacrés au commerce de biens culturels. L'absence de mécanisme interne de contrôle rend Facebook favorable à l'expansion du trafic illicite des biens culturels, sachant que les biens culturels ne figurent pas dans la liste des échanges interdits par les normes communautaires du réseau social. Cette étude ne représente qu'une infime partie de l'étendue du trafic sur internet. Un trafic accru et visant notamment les biens culturels originaires des pays du Proche et Moyen-Orient en conflit où des groupes terroristes sévissent et en profitent pour se financer.

En effet, on constate une prolifération de destructions et pillages occasionnés par des groupes terroristes en Syrie, en Irak, au Yémen, etc. Ils sont occasionnés à la fois pour des raisons idéologiques (dans le but d'« effacer le passé historique »[84] de ces pays) et pour des raisons économiques pour tirer des revenus et se financer. Selon le Centre d'analyse du terrorisme, l'État islamique aurait par exemple généré environ 30 millions de dollars grâce à ce trafic[85] en 2015. Les « antiquités de sang » auraient donc représenté « jusqu'à 15 à 20% des sources de revenu de Daech » en 2015[86]. L'Europe a réagi en 2017 avec l'adoption de la *Convention sur les infractions visant des biens culturels* pour prévenir et combattre la destruction et le trafic des biens culturels notamment dans un contexte de terrorisme.

La lutte contre le trafic des biens culturels est donc transversale et se joint à d'autres priorités du renseignement comme la lutte contre le terrorisme. Pour y répondre de manière efficace, le renseignement international se constitue en un réseau d'acteurs opérationnels et polyvalents.

---

cinquième session de la Conférence des États parties à la CNUCTO. Disponible à l'adresse suivante : http://undocs.org/fr/CTOC/COP/2010/12.

[81] Edouard PLANCHE, « La lutte contre le trafic illicite de biens culturels sur Internet : L'UNESCO et la réponse de ses partenaires », https://cites.org/sites/default/files/fra/news/world/19/05-UNESCO-Traffic%20on%20internet_F.pdf

[82] « Pourquoi le trafic de trésors culturels explose sur internet à l'heure du Covid-19 », GEO, 09/11/2020 https://www.geo.fr/histoire/pourquoi-le-trafic-de-tresors-culturels-explose-sur-internet-a-lheure-du-covid-19-202744

[83] « Facebook's Black Market in Antiquities", Athar Project (Antiquities Trafficking and Heritage Anthropology), 2019 http://atharproject.org/report2019/

[84] Mohammed DJAFOUR, « Pillage des sites archéologiques et trafic des biens culturels : un mode de financement du terrorisme », Centre Français de Recherche sur le Renseignement, Note de réflexion n°34, Décembre 2020 https://cf2r.org/reflexion/pillage-des-sites-archeologiques-et-trafic-des-biens-culturels-un-mode-de-financement-du-terrorisme/

[85] Rapport du Secrétaire général sur la menace que représente l'État islamique d'Iraq et du Levant (Daech) pour la paix et la sécurité internationales sur l'action menée par l'Organisation des Nations Unies pour aider les États membres à contrer cette menace, Conseil de sécurité, Nations Unies, 29/01/2016 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N16/023/54/PDF/N1602354.pdf?OpenElement

[86] « Les biens culturels, enjeu des conflits armés », Le Courrier de l'UNESCO, 12/10/2020 https://fr.unesco.org/news/biens-culturels-enjeu-conflits-armes

La nécessite d'une coopération internationale et interinstitutionnelle

L'efficacité du renseignement international dans la lutte contre le trafic illicite des biens culturels requiert la transmission d'informations. Cela s'inscrit dans une démarche de coopération internationale et interinstitutionnelle entre différentes autorités compétentes (États, forces de police, organisations internationales, société civile) exerçant dans différents domaines (juridique, douanier, diplomatique, policier) et à différentes échelles (locale, nationale, régionale, internationale).

D'une part, le renseignement international bénéficie d'abord de l'ancrage territorial des unités de police nationale ou de renseignement chargées de la lutte contre le trafic illicite des biens culturels sur leur territoire respectif. D'ailleurs, la Convention de l'UNESCO de 1970 encourage les États à créer des services de protection du patrimoine culturel (article 5). L'Europe est un leader en la matière puisque de nombreux pays européens ont développé des services compétents. Par exemple, depuis 1975 la France s'est dotée d'un Office central de lutte contre le trafic des biens culturels (ci-après « OCBC ») rattaché à la Direction centrale de la Police Judiciaire (DCPJ) et dont les actions se déclinent en cinq axes principaux[87] : l'investigation, le renseignement criminel, la coopération internationale, la formation et la prévention. Membre du groupe SIRASCO (Service d'information de renseignement et d'analyse sur la criminalité organisée), l'OCBC par exemple a pour mission de traiter des renseignements émanant des services territoriaux et des partenaires internationaux (dont INTERPOL) pour analyser les activités des groupes criminels organisés en matière de trafic de biens culturels.

D'autre part, il émane une nécessité de coopérer pour contrôler la circulation des biens culturels. Des opérations mondiales et spéciales sont mises en place pour permettre à différents acteurs de coopérer et d'échanger des informations décisionnelles. En 2021, l'opération « Pandora VI » dirigée par les services de police espagnols en coordination avec EUROPOL, INTERPOL et l'Organisation mondiale des douanes (ci-après « WCO ») entre le 1er juin et le 3 septembre 2021, a permis la saisie de 9 408 biens culturels et 52 arrestations dans 28 pays différents[88]. L'un des objectifs de cette opération étant de soutenir l'échange d'informations, diffuser des alertes et des avertissements et d'effectuer des vérifications croisées. EUROPOL, agence européenne spécialisée dans la répression de la criminalité, a eu pour mission de faciliter cet échange d'informations et de fournir un soutien analytique et opérationnel. INTERPOL et la WCO ont dû respectivement assurer la mise à disposition de leur système de communication (« *I-24/7* » pour l'un et « *CENcomm* » pour l'autre) pour faciliter les échanges d'informations entre les différents acteurs mobilisés.

Par ailleurs, la combinaison entre le renseignement international et la collaboration internationale se manifeste également dans la création d'organisations consacrée à la lutte contre le trafic illicite telle que l'Observatoire international du trafic illicite des biens culturels (ci-après « l'Observatoire ». Créé en 2013 à l'initiative de l'ICOM et soutenu financièrement par le programme « Prévenir et combattre la criminalité » de la Direction générale des affaires intérieures de la Commission européenne, l'Observatoire est le fruit d'un effort de coopération internationale entre chercheurs, universitaires, professionnels des musées et du patrimoine, conseillers juridiques et journalistes. En 2015, un ouvrage commandé par l'Observatoire a été publié sur le sujet intitulé "*Countering Illicit Traffic in Cultural Goods: The Global Challenge of Protecting the World's Heritage*"[89].

[87] Plaquette Office Central de lutte contre le trafic des biens culturels, ministère de l'Intérieur.

[88] « 52 arrestations à l'occasion d'une opération ciblant le trafic de biens culturels menée dans 28 pays », INTERPOL, 9 mars 2022, Lyon, France https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2022/52-arrests-in-operation-across-28-countries-targeting-trafficking-in-cultural-goods

[89] "*Countering Illicit Traffic in Cultural Goods, The*

D'autres instances plus gouvernementales ont également vu le jour tel que le Comité intergouvernemental de l'UNESCO pour la promotion du retour des biens culturels à leur pays d'origine ou de leur restitution en cas d'approbation illégale (ICPRCP) créé en 1978.

La constitution d'informations opérationnelles

L'efficacité d'un système de renseignement repose également sur la constitution d'informations qualitatives. Une information est une donnée brute ou un fait révélé tel qu'il est tandis que le renseignement est une « information finalisée, destinée à l'action »[90]. Par conséquent, le renseignement ne vaut que pour sa finalité[91].

En matière de lutte contre le trafic illicite des biens culturels, une information est opérationnelle lorsqu'elle permet d'avoir une traçabilité sur la circulation des biens culturels, d'analyser la portée des réseaux criminels et de mettre en place les outils de police adéquats (investigation, arrestation des criminels). La collecte, l'évaluation, le classement, l'analyse puis la diffusion[92] de ces informations sont des étapes essentielles. D'où l'intérêt de constituer des bases de données solides et un circuit d'informations rapide et efficace. Ces bases de données statistiques sont constituées à partir des informations obtenues à la suite d'enquêtes policières opérées par des unités nationales de police puis transmises, assemblées et comparées au sein de bases de données et registres gérés par des organisations internationales.

Un rapport de 2011[93] a analysé les structures de ces bases de données et révèle les principaux obstacles méthodologiques, juridiques et techniques. La constitution de bases de données exploitables à l'international est compliquée puisque la quantité et qualité des informations varient d'un État à un autre. Certains pays ont encore un besoin de formation du personnel dédié à cette lutte sur leur territoire. Dès lors, les disparités méthodologiques sont importantes et il est parfois difficile d'identifier certains biens. D'où la nécessite de créer des standards communs en constituant des « normes et de niveaux d'exigence »[94] et des « usages de référence » communs.

Une première solution à ce problème avait été apportée avec « Object ID »[95], une norme internationale de documentation et de description d'objets d'art et d'antiquités servant à faciliter l'identification et l'enregistrement des biens culturels. Chaque description inclut neuf catégories d'informations : type d'objet, les mesures, les matériaux et techniques utilisés, le fabricant ou l'artiste, les marques et inscriptions distinctives, les signes particuliers, le titre, le sujet et la date. Le

Global Challenge of Protecting the World's Heritage, F. DESMARAIS, ICOM International Observatory on Illicit Traffic in Cultural Goods, 2015.

[90] Renseignement et information : le point de vue de la DRM par Ch Malis (Bureau Études - Prospective DRM), École de Guerre économique : https://www.ege.fr/infoguerre/1999/07/concept-militaire-renseignement-et-information-le-point-de-vue-de-la-drm

[91] F. BEAU, Culture du renseignement et théories de la connaissance, dans Revue internationale d'intelligence économique 2010/1 (Vol 2), pp. 161-190.

[92] Systèmes d'information et de renseignement de la police, Compilation d'outils d'évaluation de la justice pénale, Nations Unies, Office de lutte contre la drogue et le crime, 2008, New York https://www.unodc.org/documents/justice-and-prison-reform/cjat/Systemes_information_renseignement_police.pdf

[93] « Étude sur la prévention et la lutte contre le trafic illicite des biens culturels dans l'Union européenne », par le Centre d'Étude sur la Coopération Juridique Internationale, CECOJI-CNRS, Octobre 2011, France file:///Users/emegrace/Downloads/Pr%C3%A9vention%20et%20la%20lutte%20contre%20le%20trafic%20illicite%20des%20biens%20culturels.pdf

[94] *Ibid* p. 188.

[95] La norme Object ID a créé en 1993 sur l'initiative du Getty Information Institute et lancé officiellement en 1997. Depuis 2004, l'ICOM détient des droits de licence et s'engage à promouvoir la norme partout dans le monde.

système « Object ID » intègre quatre étapes[96] : photographier l'objet, informer les catégories susmentionnées, rédiger les descriptions et assurer la conservation sécurisée de la documentation. Traduite en dix-sept langues, c'est la norme utilisée par INTERPOL pour enregistrer les biens culturels dans sa base de données[97].

D'autre part, des obstacles juridiques sont également comptés. Il existe différentes sources juridiques et déontologiques sur le trafic illicite des biens culturels mais elles souffrent d'une absence d'harmonisation entre elles. Ainsi, des différences d'appréciation sur des notions peuvent émerger. C'est notamment le cas pour la notion de bonne foi de l'acquéreur d'un bien culturel. Or, cette notion est déterminante pour connaître la licéité de l'origine de l'œuvre. Même si la Convention d'Unidroit de 1995[98] apporte une précision sur la notion, son impact est restreint puisqu'elle n'a été ratifiée que par 53 États contractants. Dès lors, même si le droit international essaye de construire un cadre juridique commun, on retrouve tout de même un éparpillement des normes.

Par ailleurs, des obstacles techniques sont également soulevés. L'étude de 2011, citée ci-dessus, constate une hétérogénéité des bases de données quant à leur contenu, alimentation, accès, critères de description des biens, etc. Par exemple, deux types de bases de données[99] ont été identifiés. D'une part, les bases dites « passives » pour lesquelles le requérant envoie une description du bien culturel sur lequel il souhaiterait obtenir des informations. Par la suite, la description est vérifiée et analysée par des experts. C'est sur ce modèle qu'a été développée, depuis 1995, la base de données « TREIMA II » de l'OBCB en France. Elle est la principale photothèque d'objets volés. Conçue, alimentée et limitée aux policiers et aux agents de la Direction nationale du renseignement, elle sert également aux enquêtes douanières. Autre exemple, la base de données non gouvernementale « Art Loss Register »[100], utilisée par des entreprises du milieux des assurances, des collectionneurs d'art et unités de police, est également un modèle de base de données dite « passives ». D'autre part, il existe des bases dites « actives » qui incitent le requérant à rechercher et vérifier lui-même les informations disponibles sur un bien qu'il souhaite détenir. On peut citer la base de données d'INTERPOL.

INTERPOL met à disposition une base de données de plus de 52 000 objets culturels[101] provenant de 134 pays. Considérée comme « la seule base de données internationales contenant des informations de police certifiées sur les œuvres et objets d'art volés et disparus »[102], elle permet l'identification des objets volés et pillés à travers les descriptions faites, les informations données et les photographies partagées. De plus, elle est le fruit d'une coopération internationale entre plusieurs entités (INTERPOL, UNESCO, ICOM, ICRROM). L'efficacité de son utilisation nécessite une mise à jour régulière des moyens technologiques employés. L'innovation est donc indispensable pour mieux exploiter la base de données. C'est pourquoi INTERPOL a lancé en 2021 l'application mobile « ID-Art[103] », gratuite et accessible au grand public. L'application permet la vérification des enregistrements, la création de catalogues de collections artistiques privées, le

[96] Object ID, Conseil international des musées https://icom.museum/fr/ressources/normes-et-lignes-directrices/object-id/

[97] Object ID, INTERPOL, https://www.interpol.int/fr/Infractions/Atteintes-au-patrimoine-culturel/Object-ID

[98] Convention d'Unidroit sur les biens culturels volés ou illicitement exports, 24 juin 1995, Rome, Italie

[99] Sic « Étude sur la prévention et la lutte contre le trafic illicite des biens culturels dans l'Union européenne », par le Centre d'Étude sur la Coopération Juridique Internationale, CECOJI-CNRS, Octobre 2011, France, p. 194 file:///Users/emegrace/Downloads/Pr%C3%A9vention%20et%20la%20lutte%20contre%20le%20trafic%20illicite%20des%20biens%20culturels.pdf

[100] La base de données non gouvernementales « Art Loss Register" a été créée en 1991 par des entreprises des milieux de l'assurance et de l'art.

[101] Base de données sur les œuvres d'arts volées, INTERPOL, https://www.interpol.int/fr/Infractions/Atteintes-au-patrimoine-culturel/Base-de-donnees-sur-les-aeuvres-d-art-volees

[102] ID-Art, Saisir les objets d'art – Se saisir des malfaiteurs, INTERPOL

[103] *Ibid*.

signalement des objets volés ou des sites culturels menacés et le signalement des fouilles illicites. En matière de renseignement, l'innovation participe ainsi à la sensibilisation et la prévention contre la criminalité relative aux biens culturels et plus encore, elle vient renforcer « l'action collective en faveur de la sauvegarde »[104] du patrimoine culturel international. C'est ainsi que récemment, à la suite d'un signalement communiqué par un amateur d'art Britannique, la police nationale espagnole a retrouvé des pièces d'or datant de l'Empire romain qui avaient été volées en Suisse en 2012. Suite à ce signalement, deux personnes ont été arrêtés[105]. Au marché noir, la valeur de ces pièces était estimée à 200 000 euros.

Malgré les efforts constatés, la dispersion des informations, le manque d'harmonisation des normes ou d'actualisation de certaines informations créent une carence. Or, selon les chercheurs du CNRS, une « interconnexion » entre l'ensemble de ces bases de données serait nécessaire pour leur donner une plus-value certaine[106].

De sorte que l'on peut considérer qu'en matière de lutte contre le trafic illicite des biens culturels, le renseignement international n'est qu'au commencement et tend encore à se développer pour mettre au point des outils encore plus efficaces et opérationnels permettant de capter les informations toujours autant nécessaires pour la lutte contre le trafic illicite des biens culturels.

[104] *Ibid*.
[105] Évaluation de la criminalité visant les biens culturels en 2020, Enquête auprès des pays membres d'INTERPOL, INTERPOL, septembre 2021.
[106] « Étude sur la prévention et la lutte contre le trafic illicite des biens culturels dans l'Union européenne », par le Centre d'Étude sur la Coopération Juridique Internationale, CECOJI-CNRS, Octobre 2011, France, p. 196.

QUAND LE RECUEIL DE RENSEIGNEMENT À PARTIR D'INFORMATIONS DE SOURCES OUVERTES IMPACTE LA CONDUITE DES CONFLITS MODERNES

Franck DECLOQUEMENT
Expert en intelligence économique et stratégique, chercheur associé à l'Institut d'études de géopolitique appliquée.

Pour bien comprendre ce qu'est l'OSINT et ce que cette terminologie recoupe, posons ici quelques propos liminaires. L'OSINT doit être entendu comme l'exploitation de toutes les données publiques à des fins de renseignement. C'est une nuance subtile qui a son importance, puisque le grand public a tendance à limiter l'acception du renseignement de source ouvertes aux seules traces numériques. Tandis que dans une approche axée sur le renseignement, il est bien entendu nécessaire de prendre en considération d'autres sources ouvertes, le plus souvent non numérisées. Ce qui représente en définitive un retour aux sources historiques initiales de l'OSINT. Très concrètement, le renseignement de source ouverte (« OSINT » est l'abréviation de « Open Source Intelligence » en anglais) ou « ROSO » en français (« Renseignement d'Origine Source Ouverte »), est une pratique d'investigation reposant sur la recherche, la collecte et l'analyse de toute information non classifiée. L'acquisition de ces données n'est pas assimilable à un vol de données confidentielles ou publiques. Les sources exploitées vont être les médias, le web, les journaux, forums, réseaux, et plus généralement, toute source pouvant être vecteur de diffusion d'informations. L'Open Source Intelligence est un élément fondamental pour les opérations de renseignement, car elle peut par ailleurs contribuer à la discipline émergente de mesures et signatures (MASINT), au contre-renseignement (CI) ou à des opérations de sécurité (OPSEC). Pour mieux comprendre la définition de l'OSINT axée renseignement, il faut savoir que le renseignement sur Internet se découpe très schématiquement en quatre grandes familles.

L'Open Source Data (OSD)

L'OSD correspond aux données de première impression : la diffusion et le compte rendu oral d'informations à partir d'une source primaire. Il peut s'agir d'une photographie, d'un enregistrement ou encore d'une lettre personnelle d'un individu.

L'Open Source Information (OSIF)

L'OSIF se compose en définitive de données pouvant être assemblées, généralement par un processus éditorial qui assure le filtrage, la validation et la gestion de la présentation. Cette information générique est souvent largement diffusée dans les journaux, les livres ou des rapports quotidiens. L'OSIF est en réalité ce que produit en définitive la plupart des acteurs de l'OSINT actuellement.

L'Open Source Intelligence (OSINT)

Comme indiqué précédemment, l'OSINT est une information qui a été délibérément ouverte, diffusée à un public choisi pour répondre à une question spécifique. Finalement, l'OpenSource Intelligence applique le processus éprouvé du renseignement aux multiples sources d'informations ouvertes.

Validated OSINT (OSINT-V)

L'OSINT-V correspond à une information à laquelle un haut degré de sécurité peut être attribué. Celui-ci peut être produit par un professionnel du renseignement ou une source ouverte.

Il existe plusieurs branches à l'OSINT :

- **Le SOCMINT** (Social Media Intelligence) : autrement dit, l'utilisation des réseaux sociaux pour obtenir des informations.

- **L'IMINT** (Imagery Intelligence) : il s'agit de l'analyse de tout type d'images comme les photographies classiques. On peut aussi citer l'utilisation d'images de satellites, infrarouges, radar, etc. Selon la doctrine américaine, il s'agit de l'analyse des informations géolocalisées provenant d'imageries (photographies traditionnelles, images infrarouges, radar, etc.) obtenues par des satellites, avions, drones, etc. La France restreint le renseignement d'origine image (**ROIM**) aux seules activités de recherche et développement concernant les techniques d'acquisition et d'analyse d'images.

- **Le GEOINT** (Geospatial Intelligence) : c'est l'analyse combinée des informations de géolocalisation, géologiques et météorologiques tout en faisant appel à l'IMINT. Selon la doctrine américaine, le GEOINT cumule les techniques d'acquisition d'imagerie géolocalisées, l'analyse liée à ces informations (IMINT), l'ajout de données géodésiques, géologiques et météorologiques. La France désigne par renseignement géospatial toutes les activités opérationnelles de GEOINT.

- **Le SIGINT** (Signals Intelligence) : le SIGINT est décrite comme « l'analyse des signaux électromagnétiques et communications radio ». En français « ROEM » (Renseignement d'origine électromagnétique).

- **Le MASINT** (Measurement and signature intelligence) : désigne l'utilisation et l'analyse des informations issues de tout type de capteur (ondes radio, nucléaire, acoustique, etc), afin de déterminer son origine.

- **Le RECON** : extraction d'informations techniques liées à des sites Web, ou d'autres entités accessibles sur le Web.

De nombreux autres termes peuvent être employés dans le cadre des conversations entre spécialistes de l'OSINT, tels que COMINT, ELINT, FISINT. Bien que le but même de l'OSINT soit de consulter légalement des sources en accès libre, certaines informations référencées peuvent toutefois ne pas être libre d'accès (référencement public non consenti par leur propriétaire par exemple), et tout accès à ces dernières peut donc être considéré comme « illicite ». Par nature transverse, l'OSINT peut être utilisé par différents acteurs, dans de multiples domaines et contextes : dans le journalisme, à des fins de vérification des faits. En matière judiciaire, par les forces de l'ordre, dans le cadre d'analyses de données. Dans le domaine de la sécurité informatique, lors d'une phase de reconnaissance avant un pentest, ou un audit de sécurité. En intelligence économique également. Les OSINT peuvent être classés en fonction de l'endroit où se trouvent les données publiques - dans les catégories suivantes à titre d'exemple : l'Internet (blogs, sites Web de médias sociaux, fichiers numériques (photographies, vidéos, sons) et leurs métadonnées, les empreintes techniques des sites Web, webcams, Web profond (dossiers gouvernementaux, dossiers météorologiques, dossiers d'état-civil, dossiers criminels, dossiers fiscaux et de propriété), ressources du Darknet, sites Web de fuite de données, adresses IP et tout ce qui est publié publiquement accessible en ligne). Les médias traditionnels tels que la télévision, la radio, les journaux et les magazines. Les publications universitaires telles que les mémoires de master ou de thèses, les documents de recherche, les revues spécialisées et les livres. Les documents d'entreprise tels que les profils d'entreprises, les comptes rendus de conférences, les rapports annuels, les actualités internes, les profils d'employés et les curriculums vitae. Les informations géospatiales telles que les cartes en ligne, les images satellites commerciales, les informations de géolocalisation associées aux messages sur les médias sociaux, le suivi des transports (aérien, maritime, véhicules et ferroviaire), etc.

Expliquer et démocratiser la pratique de l'OSINT peut aussi permettre d'amener plus d'utilisateurs à se rendre compte de la quantité exceptionnelle d'informations tout à fait exploitables que chacun laisse en libre accès derrière lui. En contexte de guerre, on saisit immédiatement le danger potentiel, mais aussi les opportunités pour les différentes parties prenantes au conflit.

Les renseignements recueillis à partir d'informations en Open Source ont d'ores et déjà un impact notable sur les menées de la guerre traditionnelle. Très schématiquement, l'agrégation commerciale

massive de mégadonnées durant les deux dernières décennies (issues en droite ligne des systèmes d'information déployés à l'échelle mondiale, dans le cadre des infrastructures civiles nécessaires au bon fonctionnement de la téléphonie mobile), puis l'extension exponentielle à tous les domaines de nos existences des appareils « intelligents » de réception et de captation, mais aussi des plate-formes géantes dites « sociales », a drastiquement remodelé la façon dont les renseignements peuvent aujourd'hui être collectés, triés, puis analysés par de très nombreux opérateurs : brokers, organisations civiles ou mercantiles mais aussi régaliennes. Et dans le cadre des opérations de guerre conduites par les États, l'usage de l'OSINT n'est pas récent, puisque déjà utilisé et mis en œuvre à maintes reprises, et ceci bien avant l'émergence de l'Internet. Parallèlement en cela aux informations obtenues de manière coercitive et clandestine (ce que l'on nomme communément « l'espionnage ») par les centrales du renseignement. Ceci posé, l'une des conséquences directes des informations recueillies et exploitées en open source est que l'anonymat s'érode drastiquement partout. Non seulement pour les civils ordinaires, mais aussi pour les membres des forces armées et de la communauté du renseignement. Par exemple, même des informations manquantes peuvent alerter un service de renseignement adverse : l'identité des agents travaillant sous couverture dans les ambassades pouvant être ainsi facilement déduite parce qu'ils ne disposent pas de profils Facebook ou Linkedin.

La guerre en Ukraine restera indéniablement comme le premier conflit entièrement « couvert » par les osinteurs du monde entier, qui se sont d'ailleurs très vite imposés, y compris sur les plateaux de télévision. À l'image des journalistes ayant aidé par leurs efforts de documentation sur les exactions russes (identification de l'officier russe Azatbek Omurbekov, dit aussi le « boucher », en charge du secteur de Boutcha par un collectif d'OSINT ukrainien). De surcroît, les opérations de désinformation et de propagande noire étant indifféremment utilisées par tous les belligérants en lice, les médias internationaux ont aussi été contraints de vérifier davantage la fiabilité de leurs sources. Nourrissant aujourd'hui beaucoup plus de méfiance vis-à-vis des flots de photographies, de récits et de vidéos publiées sur la toile. Car seules des preuves irréfutables peuvent permettre de qualifier certains faits.

Les technologies de l'information, par leur nature hybride, désintègrent et transcendent en définitive les frontières distinctives et les repères spatiaux habituels que nous connaissions. Elles érodent indubitablement les barrières conventionnelles. *« Le renseignement n'est pas seulement de l'information raffinée »*, expliquait Jeff Rogg, un historien du renseignement américain dans les colonnes de WIRED. L'objectif du renseignement, par rapport à la simple information, est d'obtenir et de conserver un avantage concurrentiel déterminant sur ses adversaires. Que ce renseignement soit obtenu de manière clandestine, illicite et secrète, ou par le truchement de l'open source. C'est par exemple ce principe qui est en jeu lorsque l'administration Biden déclassifie et partage étonnamment avec ses homologues et leurs populations, les renseignements de la CIA sur les intentions russes, afin de contrer très en amont les manigances du Kremlin aux yeux de tous. Cette manière d'opérer sans précédent a d'ailleurs beaucoup surpris les observateurs.

Compte tenu de l'accent mis sur l'apport des sources ouvertes dans la guerre en Ukraine, il est malgré tout assez facile d'oublier à quel point les résultats du renseignement peuvent également dépendre du secret, voire d'un peu de tromperie (« deception » en anglais)... *« Attribuer les succès en Ukraine aux seules sources ouvertes peut également offrir une sorte de couverture pour des sources et des méthodes plus étroitement détenues »* nous indique à ce titre Jeff Rogg dans WIRED, dont les travaux portent d'ailleurs principalement sur les relations civil-renseignement.

L'open source et les technologies grand public devraient à l'avenir avoir un effet durable sur le calcul de la parité des forces, entre les acteurs étatiques et non étatiques en conflit. La guerre en Ukraine à son corps défendant jouant en la circonstance le rôle de révélateur sur ce point. Et à ce titre, c'est ce que semble également percevoir le chercheur britannique Matthew Ford, coauteur avec Andrew Hoskins d'un ouvrage sur l'impact que les infrastructures d'information et les appareils connectés ont sur les conflits militaires conventionnels. Il nomme d'ailleurs le phénomène *« guerre radicale »*. Ford examine en outre l'explosion et la prégnance du numérique qui s'est rapidement propagée sur le champ de bataille, militarisant nos attentions collectives, et faisant de chacun de nous – peu ou prou – une extension ou un participant *« malgré lui »* au conflit. Face à la Russie, les plate-

formes sociales et les téléphones mobiles apparaissent comme des démultiplicateurs de force déterminants pour une puissance militaire jugée plus faible comme l'Ukraine. En particulier lorsqu'il s'agit de coordonner la collecte de renseignements pour les activités de ciblage des blindés adverses et des soldats Russes. *« Ces informations de ciblage sont désormais échangées en ligne »*, nous explique Ford. Les éliminations et les entraves réussies sont célébrées sur Telegram. Des chatbots ont été mis en place, aidant les Ukrainiens à partager les coordonnées des cibles avec leurs smartphones.

L'identification des cibles n'implique pas pour autant de systèmes militaires très complexes. Ils fonctionnent d'ailleurs à partir d'infrastructures d'informations civiles : *« Le problème avec le renseignement participatif dans une guerre comme l'Ukraine est la standardisation des rapports »*, déclarait Ford dans WIRED. Par exemple : *« Vous voulez être en mesure d'identifier le véhicule, de le géolocaliser, puis de le cartographier par rapport à tous les signaux ou images satellite disponibles, ou à d'autres disciplines de collecte, en le fusionnant en informations cibles exploitables. »* Ford affirme par ailleurs que le haut niveau de connectivité mobile parmi les Ukrainiens et l'absence notable de séquences de combat provenant de smartphones et de caméras frontales, en particulier dans les premières phases de la guerre, suggère qu'une opération d'information efficace pourrait être en cours. *« Nul doute que les Ukrainiens craignent que de telles images ne révèlent leurs tactiques, leurs techniques et leurs procédures »*, nous explique-t-il.

À cet effet, les Ukrainiens s'autocensurent fort logiquement pour ne pas être défaits. En définitive, cette invasion par la Russie de l'Ukraine est la guerre conventionnelle la *« plus numériquement connectée de l'histoire »*, conclut Ford. *« Si les Ukrainiens peuvent rendre ces renseignements exploitables plus rapidement que les Russes, ils peuvent aussi utiliser plus efficacement leurs tirs à distance limités, leur artillerie, leurs drones et peut-être même leurs missiles ou leur puissance aérienne. L'objectif est donc de trouver, de repérer et d'achever les forces russes plus rapidement que les Russes ne peuvent le faire eux-mêmes ».* On le perçoit bien désormais, la collecte d'informations et de renseignement de source ouverte est à bien des égards un élément-clé dans les guerres conventionnelles. Mais n'oublions pas cependant que l'utilisation par des civils « non combattants de plates-formes open source, ou d'appareils grand public, à l'appui d'actions militaires hostiles, soulève aussi de très sérieuses questions sur les frontières floues entre civils et combattants. Ceci pouvant inéluctablement conduire à ce que les mêmes individus deviennent illico des cibles légitimes – ou jugés comme telles par l'adversité. En vertu du droit de la guerre, les civils sont légalement protégés par le droit international, tant qu'ils ne sont pas des parties prenantes aux conflits. Et tout cela change indéniablement la donne.

MENACES CYBER ET RENSEIGNEMENT

Lucien CHAYA PODEUR
Analyste cyber – renseignement et investigation.

Le rythme et l'impact des évolutions technologiques se sont drastiquement intensifiés depuis la prolifération des technologies de l'information. La convergence croissante de domaines scientifiques initialement étrangers a provoqué et provoquera l'émergence de nouvelles technologies aux utilisations multiples, qui elles-mêmes seront la cause de révolutions qui leur succèderont. Internet est l'un de ces exemples, à l'origine d'une transformation des capacités humaines et de la création d'un espace de partage immense. Cet espace est aujourd'hui le théâtre d'un affrontement interétatique constant, sorte de guerre qui n'en porte pas le nom. Les belligérants y sont déguisés par nature, compliquant d'autant les investigations forensiques et renforçant l'impunité des acteurs. Cette concurrence globale s'intensifie à mesure que le numérique s'insère au sein des domaines régaliens, produisant de nouveaux enjeux devenus centraux. La pandémie de Covid-19 a joué un rôle de catalyseur, les activités cybercriminelles ayant augmenté drastiquement au cours de cette période. Les données de santé ont soudain acquis une criticité toute nouvelle, les laboratoires travaillant à l'élaboration de vaccins devenant des cibles prioritaires de campagne d'espionnage. Ces nouveaux enjeux n'ont cependant pas changé la nature du renseignement, les missions historiquement attribuées aux services étatiques se reflétant au sein du cyberespace : fournir des informations qualifiées aux responsables politiques, déstabiliser, saboter, le tout au moyen de prérogatives exceptionnelles. À contrario, le cyberespace inverse les rapports de force en vigueur lors d'agressions, la défense étant grandement désavantagée. On considère qu'il est cinquante fois plus coûteux pour une entité de protéger l'ensemble de son périmètre que pour un attaquant de tenter d'en percer les défenses en un point précis. Cet état de fait permet ainsi à certains États considérés comme comparativement faibles de profiter de l'espace numérique pour mener des campagnes efficaces, à l'image de la Corée du Nord qui finance une partie significative de ses activités au moyen d'une « caisse noire » composée des recettes accumulées lors d'opérations cybermalveillantes. En outre, les conflits se déroulant au sein du cyberespace sont déguisés par nature, et qui ne montre pas son visage peut se permettre d'agresser sans avoir à en subir les conséquences.

La maîtrise du cyberespace et par extension la domination des autres États au sein de ce dernier a été initiée par les États-Unis. Leur statut de « créateur du Web » conférait au pays une avance certaine, avantage exploité dès le potentiel du cyberespace définitivement entériné. La stratégie appliquée afin d'y parvenir fut celle qui primait déjà lors de la guerre froide : les États-Unis visent une écrasante supériorité technologique et quantitative qui leur permettra de submerger leurs adversaires ; les capacités cyber-offensives des États-Unis demeurent cependant largement non documentées, bien que ces dernières soient largement démontrées. À titre d'exemple, si le gouvernement des États-Unis se garde bien de revendiquer les succès de ses agences de renseignement en Ukraine afin de ne pas s'impliquer outre-mesure dans le conflit, les informations fournies permettraient de diriger les assauts contre des cibles stratégiques russes. Le renseignement cyber, au même titre que le renseignement classique, est aujourd'hui massivement partagé afin de défendre ses intérêts par procuration. Réunis au sein des « *Five Eyes* », l'Australie, le Canada, la Nouvelle Zélande, le Royaume-Uni et les États-Unis représentent aujourd'hui la plus importante communauté de renseignement du monde. Formidable instrument de reconnaissance, cette organisation est régulièrement décrite comme supranationale, s'affranchissant des lois domestiques de ses membres. Cette « domination »

occidentale inquiète. Si aujourd'hui la conception du cyberespace ne permet pas de considérer qu'une domination étatique absolue est envisageable, certains acteurs ont néanmoins entrepris d'en obtenir la maîtrise domestique. La Chine est à l'origine du concept de « Great FireWall of China », qui se définit comme la tentative du gouvernement de préserver son peuple de toute influence étrangère au sein du cyberespace, en bloquant la quasi-totalité des contenus disponibles sur la toile. La Russie a pour sa part déjà déconnecté la totalité de son territoire d'Internet, ultime solution de repli face à une cyberattaque massive dirigée contre ses intérêts.

Les cultures stratégiques française et européenne considèrent l'attribution d'une attaque à une entité étatique comme un acte politique, aussi l'État français se garde-t-il généralement de rendre publiques les conclusions des rapports par l'Agence Nationale de Sécurité des Systèmes d'Information. Le 10 mai 2022, l'Union européenne a néanmoins accusé pour la première fois de son existence la Russie d'être à l'origine de la cyberattaque menée contre le satellite européen KA-SAT utilisé par l'armée ukrainienne, au commencement de l'invasion de l'Ukraine le soir du 24 février 2022. Action de sabotage utilisée afin de déstabiliser l'armée régulière ukrainienne, cette cyberattaque a accompagné les premiers assauts menés par la Russie sans pour autant les remplacer. Le cyberespace, si souvent théorisé comme un substitut au théâtre de guerre classique entre grandes puissances, apparaît aujourd'hui plutôt comme une évolution technologique s'inscrivant dans la lignée des découvertes scientifiques ayant révolutionné le champ de bataille. Cet espace, non contraint par les limites géographiques classiques, représente également un moyen pour les acteurs non étatiques d'influencer le conflit, les activités de renseignement et de déstabilisation ne possédant plus l'attribut de domaine réservé des États. L'élan de solidarité numérique connu sous le nom d' « *IT Army of Ukraine* », organisation créée à la suite de l'appel citoyen lancé par le ministre de la transformation digitale Ukrainien, implique des civils situés aux quatre coins du globe. Ces derniers submergent les sites russes de fausses requêtes, protègent les systèmes d'information ukrainiens, le tout bénévolement et de manière coordonnée via le site de messagerie Télégram. L'initiative française de renseignement en sources ouvertes menée par OpenFacto, collectif composé d'experts civils exerçant au sein de domaines divers liés aux activités de renseignement, permet de suivre de manière quotidienne et extrêmement précise l'avancée du front. Ce travail collectif documente également les pertes humaines et matérielles provoquées par le conflit, de manière gratuite et accessible par tous sur le site Web de l'association. Le média BellingCat, considéré comme le premier collectif à l'origine de l'utilisation de la recherche en sources ouvertes, s'est fait connaître grâce à son enquête approfondie sur le crash du MH17 ayant révélé l'implication des services de renseignement militaire russes dans la tragédie. Là est la véritable révolution : la guerre et sa documentation en temps réel ne sont plus des affaires réservées aux professionnels et aux institutions étatiques, pour peu que son théâtre soit accessible au sein du cyberespace et que les informations nécessaires à son étude soient disponibles. Si ce constat est particulièrement probant lors d'un conflit « reconnu », il l'est également au quotidien, au sein de ce conflit silencieux qui oppose cybercriminels, entreprises et agences de renseignement classiques.

La frontière séparant groupes cybercriminels et Advanced Persistent Threats (APT) affiliés à des États est souvent fine. Actuellement, les menaces principales pour les entités au sein du cyberespace sont les opérateurs de *ransomware*. Le *ransomware*, ou rançongiciel, est un logiciel malveillant qui a pour but de chiffrer les fichiers du système d'information qui en est la victime. Les opérateurs de *ransomware* fondent leur modèle économique sur la rançon potentiellement obtenue en échange d'un retour des données subtilisées et de la reprise de l'activité de l'entreprise ; à ce titre, ces derniers visent dorénavant principalement les entreprises au capital élevé. Si cette menace est principalement dirigée à l'encontre d'entreprises privées, certains exemples démontrent que ces acteurs malveillants possèdent la capacité d'influencer la politique quotidienne des

États les plus puissants. En avril 2021, SolarWinds, une importante société américaine de technologies de l'information largement utilisée dans le pays a fait l'objet d'une cyberattaque qui s'est propagée à ses clients de manière dissimulée pendant des mois. Des APTs affiliés à la Russie auraient par ce biais espionné des entreprises privées à l'image de la société de cybersécurité FireEye ainsi que certains échelons supérieurs du gouvernement américain, notamment le ministère de la sécurité intérieure et le département du Trésor. Action attribuée au gouvernement russe, cette attaque représente à ce jour l'un des compromissions connues les plus importantes subies par les États-Unis. Si cette attaque a été attribuée aux services officiels russes, les intérêts vitaux étatiques peuvent également être la cible d'entités cybercriminelles privées. Le Colonial Pipeline, l'un des oléoducs les plus importants des États-Unis, a été victime d'une attaque par *ransomware* en mai 2021. Cette attaque a infecté certains des systèmes numériques du pipeline, le mettant hors service pendant plusieurs jours. Le piratage a été considéré comme une menace pour la sécurité nationale, contraignant le président Joe Biden à déclarer l'état d'urgence. Une semaine après avoir reçu l'argent de la rançon payée par l'entreprise, l'opérateur à l'origine de l'attaque Darkside a annoncé mettre fin à ses opérations à la suite d'une pression « sans précédent » reçue par le gouvernement des États-Unis. Cet événement est à l'origine d'un paradigme encore appliqué par la plupart des groupes cybercriminels privés : les secteurs considérés comme vitaux sont désormais épargnés, sous peine de recevoir une attention bien malvenue de la part des agences de renseignement. Le cyberespace s'affranchit des frontières et des règles régissant les théâtres de guerres cinétiques. Les affrontements qui se déroulent en son sein impliquent des belligérants bien plus nombreux et variés, qu'ils soient criminels, étatiques ou seulement patriotes ; seule les compétences et la compréhension de son environnement comptent. Ces nouvelles règles sont à l'origine de menaces inédites et de capacités de renseignement décuplées qui façonnent les enjeux géopolitiques contemporains. Les événements ukrainiens apportent une nouvelle grille d'analyse, celle de l'utilisation de l'arme cyber au sein d'un conflit opposant des puissances militaires majeures ; l'étude de ce conflit *a posteriori* révèlera certainement que la nature même de la guerre a changé, sous la pression de ces nouveaux codes régissant la chose guerrière contemporaine.

RENSEIGNEMENT PÉNITENTIAIRE ET LUTTE CONTRE LE TERRORISME

Bruno CLEMENT-PETREMANN
Directeur du centre pénitentiaire de Paris-la-Santé.

La façon dont le renseignement pénitentiaire a longtemps été perçu par les « services partenaires » selon le terme consacré, est assez symbolique de la façon dont l'administration pénitentiaire était elle-même considérée. Alors que les revendications des organisations syndicales des personnels de surveillance portaient depuis la fin des années 80 sur l'alignement de leur statut sur celui des policiers, il aura fallu attendre 2009 et la promulgation de la fameuse « loi pénitentiaire » pour affirmer le principe que l'administration pénitentiaire est la « troisième force de sécurité du pays ».

À cette évolution des textes s'est ajoutée quelques années plus tard un fait à la fois sociétal et politique : le développement du terrorisme islamiste et la question de la radicalisation en milieu carcéral.

C'est sous l'effet conjugué de ces deux éléments que le renseignement pénitentiaire est passé de l'âge de pierre à l'âge d'or.

L'âge de pierre du renseignement pénitentiaire

Le terme n'apparaît officiellement qu'en 2002 à l'issue de la réorganisation de la direction de l'administration pénitentiaire (DAP). En effet, une série d'atteintes graves à la sécurité dont le point d'orgue est l'évasion d'Antonio FERRARA depuis le quartier disciplinaire du centre pénitentiaire de Fresnes impose une réorganisation de la fonction sécuritaire de la DAP. Une sous-direction de l'état-major de sécurité (EMS) est alors créée. Son troisième bureau (EMS3) est nommé le bureau du renseignement pénitentiaire (BRP) et c'est la première fois dans l'histoire de la DAP que le terme est employé et consacré dans un texte réglementaire.

Il existait jusqu'à cette date clé une vague entité baptisée « bureau de liaison police-pénitentiaire », chargé de faire le lien entre les services. Alors même que l'un des fondements de la mission pénitentiaire est bien l'observation que le surveillant pratique au quotidien sur la coursive et qui permet d'anticiper d'éventuels incidents en détention, cette fonction n'avait jamais réellement été conceptualisée.

La naissance du BRP vient donc consacrer cette évolution. Mais que l'on ne s'y trompe pas : le bureau n'est à l'époque pas considéré comme un partenaire par les autres services avec lequel on peut partager des informations. Il n'est ni plus moins qu'une simple source et l'utilisation des éléments des données communiquées ne fait que très rarement l'objet d'un échange quelconque.

Il faut dire que les moyens mis en œuvre demeurent très faibles : 12 personnes, chef de bureau inclus, au niveau central et à peine un délégué en région pour traiter l'ensemble des remontées. La structuration du renseignement en établissement est encore plus faible puisqu'à l'exception de quelques grands établissements, aucun site n'est doté d'agent en charge sur le terrain du renseignement. Elle est même inexistante en milieu ouvert alors que le nombre de suivis est deux fois et demi supérieur au nombre de personnes incarcérées.

Néanmoins, les prémices de ce qui fera la fortune du renseignement pénitentiaire sont déjà en germe en ce milieu des années 2000. Le BRP est ainsi divisé en deux sections : l'une en charge du grand banditisme et de la criminalité organisée, l'autre du terrorisme et de l'islam radical. De manière empirique, le BRP crée en 2008 une grille d'évaluation et de détection du risque de radicalisation. Le bureau se dote également d'un

logiciel permettant la mise en relation et la collecte des données concernant l'ensemble de ses suivis.

La lutte contre la radicalisation et le développement du renseignement pénitentiaire

La trajectoire sanglante de Mohamed MERAH au printemps 2012 représente un premier tournant dans la montée en puissance du renseignement pénitentiaire. Dans les minutes qui suivent la neutralisation du terroriste, François MOLINS, procureur de la république de Paris, déclare devant les caméras de télévision que « Mohamed MERAH s'est radicalisé en prison ». Bien que ne résistant pas à un examen attentif de la situation (internet et l'influence familiale ont joué un rôle bien plus important dans la radicalisation de l'intéressé que son parcours carcéral de petit délinquant), cette affirmation marque le début de la réflexion sur la lutte anti-terroriste en détention et la place prépondérante que doit y prendre le renseignement pénitentiaire.

Les trois années qui suivent ouvrent une période de transition liée à deux phénomènes : la centralisation des poursuites par le parquet de Paris en matière de terrorisme et le nombre croissant de personnes revenant des zones de combat, les « revenants ». Si la France a jusqu'alors privilégié la dispersion, la DAP s'interroge sur la nécessité du regroupement pour favoriser une prise en charge plus efficace.

L'année 2015 impulse une avancée majeure dans la réflexion sur la lutte contre la radicalisation et le développement du renseignement pénitentiaire. Entre les attentats de janvier et ceux de novembre, toute une réflexion sur l'évolution de la doctrine en la matière va en effet se développer.

Les auteurs des attentats de janvier 2015, les frères KOUACHI et Amedy COULIBALY, ont ainsi fréquenté la prison de Fleury-Mérogis. Ils ont à un moment ou à un autre de leur parcours croisé Djamel BEGHAL, pourtant placé au quartier d'isolement. Incarcéré pour un projet d'attentat contre l'ambassade des États-Unis à Paris, ce dernier est un terroriste haut placé dans la hiérarchie d'Al-Qaïda.

Le choix est donc fait de privilégier définitivement le regroupement des radicalisés, tout d'abord au sein de quartiers d'évaluation puis ensuite dans des quartiers de prise en charge ayant vocation à développer un contre-discours et à mettre en œuvre une politique de désengagement. Cette politique sera déclinée après la tentative d'assassinat d'un surveillant par un détenu de l'unité de radicalisés de la maison d'arrêt d'Osny dans le Val d'Oise en 2016.

Un autre élément va contribuer au développement du renseignement pénitentiaire qui consiste dans le nécessaire suivi devant être mis en place à la libération : l'information des services partenaires lors de l'élargissement d'un détenu incarcéré pour des faits de terrorisme est une impérieuse nécessité pour la sécurité de l'État. On se souvient par exemple que la presse avait abondamment commenté le fait que rien n'avait été prévu lors du suivi de Medhi NEMOUCHE malgré les alertes données par le délégué au renseignement pénitentiaire de la prison de Toulon et transmises par courriels au service partenaire, en l'espèce l'unité locale de la DGSI. Quelques semaines plus tard, l'intéressé se rendra coupable de la tuerie du musée juif de Bruxelles.

L'âge d'or du renseignement pénitentiaire : la création du service national du renseignement pénitentiaire (SNRP)

La loi du 3 juin 2016 renforçant notamment la lutte contre le crime organisé, le terrorisme et leur financement, a consacré l'intégration du renseignement pénitentiaire dans le second cercle de la communauté nationale du renseignement. De cette consécration découle une organisation qui n'a plus rien à voir avec le BRP de 2002.

En haut de la pyramide se dresse le SNRP qui anime et coordonne les activités de toute la filière. Il exerce à ce titre une autorité hiérarchique exclusive sur l'ensemble des agents du renseignement (qui sont près de 500 aujourd'hui, ce chiffre devant être comparé avec la petite vingtaine d'agents composant la filière il y a une dizaine d'année). Le SNRP définit la doctrine et la déontologie. Il est surtout le point de contact unique des services centraux partenaires et

des autorités judiciaires à compétence exclusive. C'est le SNRP qui est le guichet unique pour les demandes de mises en œuvre des techniques de recueil de renseignement et à ce titre l'interlocuteur du groupement interministériel de contrôle et de la commission nationale de contrôle des techniques de renseignement.

Le SNRP est piloté directement et rapporte exclusivement au directeur de l'administration pénitentiaire.

Nous retrouvons ensuite au sein de chacune des directions inter-régionales des services pénitentiaires (on en compte neuf en métropole auxquelles s'ajoute la mission outre-mer) une cellule inter-régionale du renseignement pénitentiaire (CIRP) qui est responsable de l'animation du réseau dans sa circonscription géographique.

La CIRP décline le plan annuel de renseignement rédigé par le SNRP et exploite et synthétise les données concernant les objectifs. Elle informe le directeur de la circonscription de l'état de la menace et représente l'interlocuteur des chefs d'établissement et des directeurs de SPIP dont les services assurent les suivis en milieu ouvert. La CIRP est également le point de contact avec les échelons déconcentrés des services partenaires et l'un de ses représentants participe au groupe d'évaluation départementale réuni sous l'égide des préfets.

Mais la nouveauté majeure et l'avancée la plus spectaculaire tient sans doute dans la reconnaissance du rôle essentiel tenu dans chaque établissement par les délégués locaux au renseignement pénitentiaire (DLRP). Ces postes sont aujourd'hui fléchés et attribués à des agents faisant l'objet d'une sélection spécifique qui précède leur habilitation.

Dans la définition des objectifs et dans la mise en place des techniques, ils relèvent de l'autorité hiérarchique de la CIRP et pas du chef d'établissement dans lequel ils sont affectés (ce dernier conservant toutefois une autorité fonctionnelle sur les DLRP).

Les moyens d'investigation de la filière sont quant à eux régis de la même façon que ceux utilisés par des services comparables, notamment tous ceux appartenant au second cercle de la communauté. Les sources humaines obéissent à un « code de traitement des sources » qui garantit par exemple l'anonymisation des sources et des agents traitants. Quant aux moyens techniques, ils obéissent aux principes du code de la sécurité intérieure qui définit les techniques de recueil de renseignement (TRR). Les demandes sont collectées par les CIRP et validées par le SNRP qui les centralisent.

Les CIRP ont notamment été fortement renforcées sur le plan qualitatif par des personnels spécialisés, le plus souvent contractuels, tels que les experts en investigation numérique ou les analystes-veilleurs.

En une décennie, le visage du renseignement pénitentiaire a été profondément remanié. Il est devenu une service puissant, doté de moyens et reconnu par ses pairs (le directeur de la DGSE s'est par exemple loué récemment de la qualité des informations et du partenariat noués avec le SNRP).

Il n'en demeure pas moins que cette croissance rapide occasionne de nouveaux défis auxquels il est impératif de répondre : le premier est celui de la bonne coordination sur le plan local qui doit régner entre les DLRP et les responsables locaux qui sont au premier chef concernés par ce qui se passe dans leur établissement. Autant les DLRP doivent se consacrer entièrement à leur mission, autant ils doivent collaborer avec les directions des établissements. Leurs seuls interlocuteurs ne sauraient être les services partenaires ou les CIRP. Pour garantir la nécessaire cohérence des inter-actions, chaque CIRP a été amenée à proposer la signature d'un protocole de fonctionnement à chaque direction d'établissement.

Le second chantier en cours mais qui reste à investir plus massivement est celui du lien avec la filière insertion et probation. Si de plus en plus de

personnels de cette filière s'intéressent à la question du renseignement et au suivi des personnes radicalisées, ce qui n'était pas à l'origine culturellement évident, le défi demeure de taille parce que les personnes incarcérées aujourd'hui sont les futurs suivis à l'extérieur de demain. Et il est toujours plus simple de suivre et d'anticiper des événements dans le cadre contraint de la prison qu'en milieu ouvert où par définition les personnes restent libres de leurs faits et gestes.

LES VECTEURS AÉRIENS ET SPATIAUX DU RENSEIGNEMENT MILITAIRE FRANÇAIS : COMPOSITION ET ENJEUX

Romain BERTOLINO
Ancien directeur général de l'Institut d'études de géopolitique appliquée, analyste indépendant en relations internationales.

Il est difficile voire impossible d'évoluer dans un environnement sans en avoir une connaissance fine. Face à tout brouillard de guerre, la collecte et l'analyse de signaux électromagnétiques (ROEM) et d'informations visuelles (ROIM) sont alors primordiaux. Les milieux aérien et spatial semblent être les plus disposés à cela : la « 3e dimension » permet en effet par définition de prendre de la hauteur, c'est-à-dire d'avoir une vision globale (donc complète), ainsi que d'atteindre des endroits naturellement inaccessibles à l'Homme. D'où son importance pour identifier un trafic illicite (entre autres par transbordement en haute mer), un rassemblement d'individus à l'attitude hostile, etc.
Ils impactent tant le milieu terrestre que maritime. Si l'armée de l'Air et de l'Espace (AAE) est particulièrement concernée, la Marine nationale dispose également de vecteurs[107] aériens propres pour son renseignement (ne se contentant donc pas de navires de surface et de sous-marins), tout comme l'armée de Terre.

Des vecteurs aériens lourds pour une récolte « directe »

De quels aéronefs parle-t-on ?

De nombreux aéronefs lourds ont leurs structures directement équipées de capteurs destinés au renseignement.

L'AAE dispose ainsi de ce qui suit :

- le Mirage 2000D, équipé d'une nacelle[108] ASTAC (un capteur de ROEM),
- l'E-3F SDCA *Awacs*, véritable avion radar, équipé d'un ensemble d'antennes d'écoute électronique[109] (ROEM),
- les Rafales B et C, équipés de nacelles Reco-NG (ROIM). Elles prennent des photographies en haute et très basse altitude, de jour comme de nuit, grâce à un capteur optique pouvant tourner à 180° et pointer un objectif sous différents angles. Leurs radar RBE2 AESA et système SPECTRA peuvent alimenter le ROEM,
- le drone MQ-9 *Reaper*, à voilure fixe (idéale pour une projection longue distance), disposant d'une boule optronique opérant un capteur de ROIM : vidéos et images (qui peuvent être « habillées » d'éléments complémentaires) en haute définition sont ainsi récoltées. Depuis peu, les *Reapers* sont aussi équipés de capteurs de ROEM,
- l'ALSR Vador, un *Beechcraft* équipé de capteurs de ROIM et de ROEM,
- le C-130 Hercules à disposition du COS, équipé de capteurs de ROIM dans le cadre de la capacité C3ISTAR.

La Marine détient l'Atlantique 2 pour du ROIM, et du ROEM dans une moindre mesure, au départ d'une BAN[110]. Les Flacon 50 M et 200 – *Gardian* peuvent également être utilisés pour cela. De plus le porte-avions Charles de Gaulle embarque l'*Hawkeye* comme équivalant à l'E-3F SDCA (ROEM), et le Rafale M, lui aussi équipé d'un pod Reco-NG (ROIM). Elle se dote aussi de drones à voilure tournante (fonctionnant comme des hélicoptères, plus adaptés à ses porte-hélicoptères amphibies que ceux à voilure fixe) : le Serval (ROIM).

[107] Un porteur de capteur(s).
[108] Aussi appelé « pods ».
[109] Mesure de soutien électronique (MSE).
[110] Base d'aéronautique navale.

L'artillerie de l'armée de Terre est quant à elle équipée du drone *Patroller* (ROIM), à voilure fixe.

Enfin, notons que des hélicoptères (concernant chaque armée) peuvent être équipés de capteurs, particulièrement des caméras thermiques (ROIM), à l'image des Caracals (AAE et armée de Terre).

Quelles logiques de complémentarité ?

Les complémentarités entre les options précédentes s'expliquent par :

- les différents types de capteurs qu'elles utilisent (ROIM et/ou ROEM),
- la performance individuelle des différents capteurs d'un même type. Par exemple chez l'AAE, bien que les Rafales et MQ-9 *Reapers* fassent tous deux du ROIM, l'écran de ce dernier est plus grand et dispose d'une meilleure résolution. Il est donc privilégié pour les tâches de *battle damage assessment* (BDA) qui exigent de déceler des détails dans la complexité des débris, l'obstruction de fumées, etc.,
- les spécificités techniques de chaque aéronef qui porte son ou ses capteurs, influençant la qualité et la quantité des informations récoltées par lesdits capteurs, ainsi que les conditions possibles de capture. En guise d'exemple, l'autonomie et la portée d'un aéronef sont des variables importantes. Ainsi, le *Reaper* permet une « permanence » contrairement au Rafale, car il dispose d'une bien plus grande durée de vol et est bien moins repérable car moins bruyant. En guise de second exemple, notons que dans la Marine le Rafale peut voler plus bas et plus rapidement que l'Atlantique 2,
- les différentes raisons d'être d'un porteur : ainsi, le Rafale est omnirôle et ne peut être employé exclusivement pour du renseignement.

Des vecteurs aériens lourds pour une récolte « indirecte »

Il existe plusieurs aéronefs lourds qui participent aux activités de renseignement de manière indirecte, dans le sens où ils transportent des Hommes équipés de vecteurs portatifs ou de capteurs mobiles[111], utilisables en l'air ou au sol une fois projetés. À titre d'exemple le Caracal est utilisé par le Service action de la DGSE et les Forces spéciales air. Nous constatons en outre avec cet exemple qu'un aéronef peut être un acteur direct et indirect. De plus contrairement à la plupart des exemples précédents, ces moyens permettent d'acquérir du ROHUM. L'ensemble des hélicoptères (concernant chaque armée), mais aussi des avions de transport tactiques (AAE & Marine) peuvent ainsi jouer des rôles (variables) dans cette tâche.

Les vecteurs aériens portatifs, pour du renseignement de proximité

De quoi parle-t-on ?

Nous évoquons ici des drones. Selon la taille, trois catégories émergent : les nanodrones (pouvant tenir dans une main), les microdrones (de la dimension d'un casque) et les minidrones (pouvant être aussi grands qu'un Homme). La taille d'un drone dépend des besoins opérationnels. En effet plus il est petit, alors :

- moins il est encombrant, et donc plus il est valorisé lors des missions longues ou encore qui nécessitent une agilité de mouvement,
- plus il permet d'accéder à des lieux étroits,
- moins il est repérable (vision et son),
- plus il est fragile, et donc sensible au vent et aux aléas des combats,
- moins il durera en vol.

Il existe également une seconde catégorisation, partagée avec les modèles lourds, se focalisant sur la voilure. Un drone à voilure tournante permet des vols stationnaires : il est donc plus maniable dans ses déplacements et réussit à cibler un objectif plus aisément que s'il était en mouvement. Le second type, à voilure fixe, au fonctionnement proche de celui d'un planeur, a l'avantage de pouvoir parcourir de plus longues distances et de voler plus longtemps.

[111] Exemple : des jumelles infrarouges.

Au profit des commandos…

Les soldats au sol ou sur embarcation légère en mer bénéficient de la multiplication des drones de petites tailles. Les drones portatifs permettent en effet d'acquérir des informations tactiques en temps réel, à moindres perte (car permettent aux troupes de voir sans être vues), coût et énergie (car évitent l'usage de moyens lourds), qui seraient difficiles sinon dangereux d'obtenir habituellement. Il est question de vérification d'une position ennemie dans un fossé, derrière un bâtiment, etc. Ils répondent ainsi avant tout à un besoin militaire tactique, là où les vecteurs lourds sont autant utiles aux militaires qu'aux décideurs politiques, tant pour des décisions tactiques que stratégiques. Ces drones sont également appréciés pour leur capacité à faire du renseignement de type BDA.

Les commandos parachutistes de l'air sont équipés des drones correspondant à leurs raisons d'être :

- le CPA 10, spécialisé entre autres choses dans les opérations de libération d'otages, d'évacuation de ressortissants et de neutralisation, bénéficie ainsi de l'agilité des drones à voilure tournante *Black Hornets* (nano, ROIM) et *Anafi USA* (micro, ROIM),
- le CPA 30, spécialisé notamment dans la recherche et le sauvetage au combat, a besoin d'une projection de son champ de vision. Il bénéficie ainsi du « planeur » *Skylark Lex NG* (mini, ROIM).

Faute de poids et de taille suffisants, ces modèles ne sont pas équipés de capteurs additionnels de ROEM. L'*Anafi* équipe également la Marine.

Les « terriens » en sont également équipés, tout comme ils le sont de *Black hornets* à l'instar de l'AAE, mais utilisent additionnellement un troisième drone à voilure tournante : le *NX70* (micro, ROIM).

…mais pas uniquement

Le SMDM[112], minidrones à voilure fixe catapultés pour du ROIM, intègre progressivement les navires lourds de la Marine. Ils sont très utiles pour du renseignement de proximité, pour lequel l'emploi de moyens lourds semble moins pertinent.

L'artillerie de l'armée de Terre dispose des SMDR[113], également des minidrones à voilure fixe pour une grande projection de capacité de ROIM, en complément du *Patroller* (qui n'est pas portatif).

Quels moyens spatiaux ?

Les satellites partagent la logique de la 3e dimension. Le système d'observation MUSIS-CSO est ainsi dédié au ROIM. Mentionnons aussi la récente constellation CERES, unique en Europe : selon le ministère des Armées, elle assure « une couverture géographique mondiale, […] des zones inaccessibles aux capteurs actuels de ROEM, et ce par tout temps, de jour comme de nuit […] dans toutes les zones d'intérêt et de conflits ».

Les coûts de manœuvrabilité des satellites sont tels qu'ils sont surtout employés lorsque les moyens aériens précédemment mentionnés montrent leurs limites.

L'armée dispose également du soutien d'autres moyens publics (avec les satellites Pléiades du CNES par exemple) et de moyens issus du secteur privé (comme des logiciels de Preligens).

Même s'il est sous l'autorité de l'AAE, le commandement de l'espace répond aux besoins de chaque armée et agence de renseignement.

Un avenir tracé, mais pavé de difficultés

Les capacités futures sont déjà planifiées. Ainsi, l'armée projette d'acquérir d'ici deux ans des drones portatifs plus grands que les minidrones, des « petits drones », pour qu'ils soient enfin équipés à la fois de capteurs ROEM et ROIM. Les commandos marine (mais aussi fusiliers marins) tentent également d'intégrer des minidrones à voilure fixe qui auraient

[112] Système de mini-drones aériens embarqués pour la Marine.

[113] Système de mini-drones de reconnaissance.

cette bicéphalité, grâce au projet *Sköll*. Le nouveau « planeur » Puma devrait également intégrer diverses forces spéciales : contrairement au *Skylark Lex NG*, il pourra être envoyé par les mains uniquement et non plus avec l'assistance d'un élastique agissant comme une catapulte (ce qui diminuera l'encombrement). Il sera également plus rapide à monter.

Concernant les vecteurs lourds, les futurs SDAM[114] (des drones à voilure tournante pour du ROIM et ROEM) sont également à l'étude pour la Marine. Mais l'expression du plein potentiel d'autres aéronefs lourds, voire leur mise en service, sont mis au défi. À titre d'exemple, si les capacités de ROEM des *Reapers* se mettent en place, il aura fallu sept ans de négociation avec les Américains pour en bénéficier. D'autres mésaventures peuvent ainsi voir le jour.

Il convient également de noter l'arrivée en 2025 du système Archange (AAE), un ensemble de *Falcon* 8X équipés du système de CUGE[115] permettant du ROEM : ce sont des « antennes multipolarisation » couplés à une intelligence artificielle pour le traitement de données. Il doit pouvoir, simultanément, détecter et analyser les émissions de radio et les signaux radars. Ce projet est évidemment positif, mais certains observateurs commencent à craindre des retards de livraison.

Les ALSR, eux, subissent le handicap d'un capteur de ROIM[116] qui ne répond pas aux attentes. Sa sélection était justifiée par des impératifs budgétaires.

De plus, notons que l'Eurodrone d'Airbus équipé du nouveau capteur *Euroflair 610* de Safran devrait également intégrer l'arsenal français d'ici 2030. Si la souveraineté de ce programme est à louer, certains observateurs craignent qu'à cette date le drone ne soit dépassé, notamment vis-à-vis de la concurrence américaine. De manière générale, la souveraineté des industries française et européenne est un enjeu tant pour les porteurs que les capteurs.

Notons également que le départ du C160 *Transall* (AAE) en 2022 a apporté son lot de défis. Après près de 60 ans de service, et essentiel aux forces françaises jusqu'à l'opération Barkhane, son retrait crée un risque de rupture capacitaire ROEM aérienne. De manière générale, des observateurs craignent que notre capacité future de ROEM aérienne soit incomplète. Notons malgré tout la diversité des moyens prémentionnés et que l'équipage du *Transall* a été rattaché aux ALSR, de sorte que le savoir-faire en matière de ROEM se conserve.

De plus, notons que les hélicoptères Fennecs (AAE) pourront bientôt transmettre des vidéos en temps réel au CNOA[117] et que les Guépards du programme Hélicoptère interarmées léger (HIL) qui les remplaceront d'ici la fin de la décennie, et dont bénéficieront aussi la Marine et l'armée de Terre[118], devraient être également équipés de moyens de renseignement.

Enfin, gardons à l'esprit que nous sommes dans un domaine en constante évolution et que des innovations peuvent intéresser à l'avenir les armées françaises. En guise d'exemple, la *Luftwaffe* a réussi à lancer un drone par la soute d'un A400M en plein vol.

[114] Système de drone aérien pour la Marine.
[115] « Capacité universelle de guerre électronique » de Thales.
[116] *Star Safire 380*, de conception américaine.
[117] Centre national des opérations aériennes.
[118] Via le COM ALAT.

RENSEIGNEMENT ET GÉOPOLITIQUE : LES ENJEUX CONTEMPORAINS

Laurane RAIMONDO
Chercheure, entrepreneure et auteure dans les domaines de la cybersécurité, du spatial et de la protection des données, chargée de cours magistral à l'Université Jean Moulin Lyon 3.

Lorsque l'on demande à Louis Pouzin s'il avait imaginé qu'un jour Internet deviendrait ce qu'il est, il répond mi-amusé mi-dépité que non, pas un instant. Un nouvel « espace », purement artificiel et purement technique a été édifié en deux décennies : le « cyberespace ». Les États le considèrent comme une fraction de leur territoire (le « territoire numérique »), une fraction de l'espace international (en mer ou dans l'exo-atmosphère), une matrice d'opportunités mais aussi de risques et de menaces. Le renseignement, lui, est aussi ancien que les États, les armées, les guerres. Il s'agit toujours de percer le secret de l'Autre, notamment l'Ennemi. Recueillir et collecter des informations, les trier, les vérifier, les recouper, les exploiter, telle est l'activité des professionnels du renseignement. Cette activité doit bien sûr s'adapter à la révolution du numérique, qui lui confère en même temps une dimension sans précédent. On rappellera la distinction des risques et des menaces, puis on passera aux différents services compétents en France, aux fonctions du renseignement et aux cibles du renseignement, c'est-à-dire les adversaires identifiés.

La distinction des risques et des menaces

Le cyberespace a autant de définitions que de milieux intéressés : académique, militaire, scientifique, littéraire. On ne reviendra pas sur les différentes couches perçues et analysées par le général Kempf, physique, logicielle, sémantique, corrigées, nuancées ou révisées depuis la parution de son ouvrage il y a dix ans[119], ni sur celles identifiées par GEODE, le centre de recherche et de formation en sciences humaines et sociales à l'Université Paris 8 dédié à l'étude des effets de la transformation numérique sur l'environnement stratégique. Un constat fait cependant consensus : le cyberespace est le champ des données. Et qui détient la donnée - l'information - détient le pouvoir. Les méthodes numériques de captation, transmission, conservation, analyse des données engendrent inévitablement de nouveaux risques et de nouvelles menaces. Les sciences sociales et le droit positif clarifient les termes : il y a menace lorsqu'il y a intention et capacité de nuisance d'un sujet conscient et agissant, autrement dit, d'une personne physique ou morale, État, collectivité non étatique, individu ; il y a risque lorsqu'il y a dangerosité objective d'un bien ou de l'environnement, qu'une intention hostile ou criminelle pourrait exploiter. Parler de menace cyber implique ainsi un individu, un groupe d'individus ou une instance ayant la volonté et le pouvoir de nuire, pour des motifs politiques ou crapuleux, à d'autres individus, collectivités ou institutions par le biais des systèmes informatiques. Pour parer aux risques et aux menaces, les pouvoirs publics mènent des politiques publiques.

Selon le code de la défense et le code de la sécurité intérieure français, l'ensemble des politiques publiques concourent, ou sont censées concourir, à la sécurité nationale. Mais elles comportent deux principaux piliers : la politique de défense (plutôt militaire, incluant la dissuasion nucléaire) et la politique de sécurité intérieure (plutôt civile, incluant la fonction hospitalière). Cette dernière inclut la sécurité publique (les mesures de police, administratives et judiciaires, face aux troubles à l'ordre public et aux infractions ou aux menaces de

[119] O. Kempf : *Introduction à la cyberstratégie*, Paris, Economica, 2012.

troubles à l'ordre public et d'infractions), la sécurité civile (les mesures de police administrative pour limiter les risques d'accidents, épidémies, calamités, catastrophes ou de dommages intentionnels, et l'organisation des secours en cas d'accidents, épidémies, calamités, catastrophes ou de dommages intentionnels), la sécurité économique (les mesures de protection des infrastructures d'importance vitale, notamment les installations nucléaires, les transports et les hydrocarbures, les communications électroniques). Puisque que le cyberespace, ou les moyens cybernétiques, englobent et articulent la plus grande partie des activités dans notre monde numérisé, la cybersécurité et la cyberdéfense sont devenues cruciales, en liaison avec les câbles sous-marins d'une part, les satellites orbitaux d'autre part (de « l'espace virtuel » est connecté à de l'espace réel).

Les services de renseignement en France

Les services de renseignement en France s'organisent principalement - mais pas exclusivement - autour de la distinction entre l'intérieur et l'extérieur du territoire. On mentionne la Direction générale de la sécurité intérieure (DGSI), rattachée au ministère de l'Intérieur ; la Direction générale de la sécurité extérieure (DGSE), rattachée au ministère de la Défense, à l'instar de la Direction du renseignement militaire (DRM) et de la Direction du renseignement et de la sécurité de la défense (DRSD)[120] ; la Direction nationale du renseignement douanier et des enquêtes douanières (DNRED) et le Traitement du renseignement et action contre les circuits financiers clandestins (TRACFIN), tous deux rattachés au ministère de l'Économie et des Finances. La DGSE, donc la défense, garde la primauté, puisque c'est à elle qu'est dévolue la mise en place des capacités techniques mutualisées au profit de l'ensemble de la « communauté du renseignement », interministérielle, supervisée par le Conseil national du renseignement (CNR) et par le Coordonnateur national du renseignement (CoNR)[121]. Parmi ces capacités techniques, figure la Plateforme nationale de cryptage et de décryptement (PNCD), créée en 2002, base de données personnelles commune aux services de renseignement. Existe aussi la CNRCT (Coordination nationale du renseignement et de la lutte contre le terrorisme). Tel est le « premier cercle » du renseignement, énoncé dans le décret du 28 septembre 2015 portant désignation des services spécialisés de renseignement[122]. Le « second cercle » correspond à différents services (23) de la Police nationale et de la Gendarmerie nationale[123], principalement sous l'autorité du ministère de l'Intérieur, secondairement, du ministère des Armées[124].

La loi sur le renseignement du 24 juillet 2015, insérant un livre VIII dans le code de la sécurité intérieure (CSI), a défini le renseignement comme *« la recherche, la collecte, l'exploitation et la mise à disposition du gouvernement des renseignements relatifs aux enjeux géopolitiques et stratégiques ainsi qu'aux menaces et... risques susceptibles d'affecter la vie de la nation »* ; *« ils contribuent à la connaissance et à l'anticipation de ces enjeux ainsi qu'à la prévention et à l'entrave de ces risques et menaces »* (art.L.811-2). On retrouve bien la grande distinction des risques et des menaces. Connaître et anticiper les risques donc les dangers, les menaces donc les adversaires : tel est le rôle clef des services de renseignement. Cela les amène fondamentalement à interroger le « cyberespace », à l'explorer et à le maîtriser, ou du moins à tenter de l'explorer et de le maîtriser. À l'instar de la « communauté du renseignement, la « communauté cyber » française comprend plusieurs services : TRACFIN et sa division d'enquête spécialisée sur la cybercriminalité financière ; la DNRED et son service spécialisé de cyber-douane ; la DGSI, dont le rôle de prévention, surveillance et répression des actes d'ingérence portant atteinte au potentiel économique, industriel et scientifique de la France en fait l'unique service de cybersécurité combinant

[120] Plus le Commandement des opérations spéciales (COS).
[121] Créés par un décret du 24 décembre 2009.
[122] Article L.811-2 CSI.
[123] Décret du 11 décembre 2015 portant désignation des services autres que les services spécialisés de renseignement (art.L.811-4 CSI).
[124] Loi du 24 juillet 2015 relative au renseignement.

cadre judiciaire et cadre de renseignement ; la DRM et la DRSD, dont les centres de recherche et d'analyse cyber concourent à informer, éclairer, renseigner les autorités dans leurs décisions, principalement relatives aux opérations extérieures ; la DGSE et sa PNCD. Les services de renseignement du « premier cercle » entretiennent des relations spécifiques avec les autres organes de la « communauté cyber » française, tels l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et le Commandement de cyberdéfense (COMCYBER). La première a un rôle d'anticipation des risques ou menaces, de détection et de réponse aux incidents ou attaques. Le second assure la protection des systèmes d'information placés sous la responsabilité du ministère des Armées (MINARM) et du chef d'état-major des armées (CEMA). Spécialement, l'ANSSI pilote le Centre de coordination des crises cyber (C4), une instance interministérielle qui traite de l'analyse de la menace et vient s'assurer de l'indispensable échange d'informations entre l'ANSSI, le COMCYBER, la DGSE et la DGSI. Elle veille également à la diffusion des informations techniques entre les experts des différents services compétents concernés. Ainsi est-elle chargée du pilotage des opérations et de l'organisation de la réponse en cas d'attaque informatique majeure contre le pays.

On ne peut connaître et anticiper la menace cyber sans tenir compte d'une particularité intrinsèque : la transversalité du cyber. On mesure la différence entre la perception occidentale du « cyberespace », vu comme un espace à part entière, le cinquième après la terre, la mer, l'air et l'exo-atmosphère, espaces naturels, et la perception russe ou chinoise. Le « cyberespace » n'existe pas pour les Russes ou les Chinois, qui préfèrent parler de « moyens cybernétiques » traversant et articulant les quatre autres espaces, terre, mer, air et exo-atmosphère. Mais la transversalité demeure. Celle-ci se corrèle à l'internationalité. Risques et menaces, étatiques ou subétatiques, hostiles ou criminelles, transcendent les frontières. C'est aussi pourquoi la coopération doit être internationale, européenne, atlantique ou avec tout autre partenaire.

Les fonctions du renseignement

Selon les documents officiels français, le *Livre blanc de la défense et de la sécurité nationale* 2013 (*LBDSN*), la *Revue stratégique de défense et de sécurité nationale* 2017 (*RSDSN*) actualisée en 2021 (*Actualisation stratégique*) et la *Revue nationale stratégique* 2022 (*RNS*), le renseignement fait partie des fonctions stratégiques. Il y en avait cinq : connaissance-anticipation, dissuasion, protection-résilience, prévention, intervention ; une sixième a été ajoutée en 2022 : l'influence. Toutes doivent être articulées afin de répondre au *continuum* de risques ou de menaces et à l'évolution du *continuum* de risques ou de menaces qui pèsent sur la France, ses intérêts et ses valeurs, ainsi que sur les intérêts et les valeurs des alliés et partenaires de la France. Concentrons-nous sur la première fonction, appelée « connaissance-compréhension-anticipation » dans la *RNS* 2022.

Elle comprend cinq domaines : renseignement, connaissance des théâtres d'opérations, diplomatie, prospective et anticipation, maîtrise de l'information. Elle vise à préserver une capacité d'appréciation autonome et à faciliter la réactivité de la décision découlant de l'appréciation. Il s'agit de connaître tout compétiteur, ses intentions et ses capacités. Cela suppose de vérifier, trier et hiérarchiser l'information, mais aussi de pouvoir compter sur l'information et l'appréciation partenariales. Depuis 2022, la fonction renseignement se confond également avec un objectif stratégique. Dix ont été énoncés : la dissuasion nucléaire, la résilience nationale, l'économie de défense, la cyberdéfense, la France comme allié exemplaire, la défense européenne, la France comme partenaire de souveraineté et pourvoyeur de sécurité, l'autonomie de renseignement et de décision, la capacité de défense dans les champs hybrides, la libre capacité opérationnelle en tous domaines (tous milieux et tous champs).

On remarque l'importance accordée à la cyberdéfense. La résilience n'est pas que morale et économique, mais cyber. La *RNS* constate qu'il ne saurait y avoir de logique dissuasive dans le

cyberespace (*« l'application d'une logique dissuasive dans le cyberespace qui forcerait tout attaquant à la retenue contre la France est illusoire »*). Mais adopter des stratégies de réponse nationale et interalliée efficaces permet de rendre les cyberattaques très coûteuses pour les assaillants. La résilience cyber consiste à disposer de capacités adaptées et organisées aux fins de prévenir ou, le cas échéant, de réduire les conséquences et la durée des cyberattaques menées contre la France, *a minima* pour les fonctions les plus critiques. Il s'agit donc d'améliorer la résilience cyber des secteurs publics et privés, de consolider les acquis du modèle français (depuis 2008), d'investir dans la durée pour atteindre le plus haut niveau de résilience dans l'ensemble des services publics, ou du moins les plus essentiels. Cela implique de s'appuyer sur un écosystème cyber public et privé dynamique et compétitif, de former et de sensibiliser au risque cyber le grand public, de renforcer l'attractivité des métiers de la filière, la responsabilité des fournisseurs de services et la sécurisation des chaînes d'approvisionnement. La résilience cyber de la France dépend aussi de celle de ses partenaires européens et internationaux, ainsi que de la sécurité et de la stabilité du cyberespace dans son ensemble. D'où l'effort nécessaire pour encadrer le commerce, lutter contre la prolifération des armes cyber en utilisant des outils de contrôle de l'export des biens et technologies, établir un référentiel commun de gestion de crise cyber et des mécanismes de coopération ou d'entraide internationale.

Du côté de l'autonomie de renseignement et de décision, soit le huitième objectif stratégique, il s'agit d'accroître et d'améliorer les capacités de connaissance, compréhension, anticipation, renseignement, veille et coordination, aux fins d'identifier toute menace conventionnelle ou non conventionnelle et d'y parer, y compris en coopération européenne ou atlantique. On sait que le renseignement s'abreuve à six types de sources : le renseignement d'origine humaine (ROHUM), le renseignement d'origine électromagnétique (ROEM), le renseignement d'origine image (ROIM), le renseignement d'origine géospatial (ROG), le renseignement d'origine cyber (ROC), le renseignement d'origines sources ouvertes (ROSO). À son tour, le renforcement du renseignement, en ses six sources, sert au dernier objectif stratégique de la *RNS*, à savoir la libre capacité opérationnelle en tous domaines. Ce dernier objectif couronne l'ensemble, en étant probablement le plus important. Or, il implique la capacité à anticiper, détecter, connaître et comprendre les intentions et les capacités des adversaires, soit la fonction renseignement.

Les cibles du renseignement (les adversaires des services)

Depuis le *LBDSN* 2013, la France est le « pays des deux angles » : Est et Sud, avec deux types de menaces : celles de la force, celles de la faiblesse. La *RSDSN* actualisée et la *RNS* ne l'ont pas répété mais ne l'ont pas infirmé ; la considération reste opératoire, sous-jacente. La France fait partie de l'Alliance atlantique et de l'Union européenne (UE) ; elle fait même partie des États membres fondateurs. Étant une puissance occidentale (se voulant telle), sa défense n'est pas tournée vers l'Ouest ou le Nord, mais vers l'Est et le Sud.

Les « menaces de la force », à savoir les grands États ou l'émergence de grands États, se trouvent surtout à l'Est ; les « menaces de la faiblesse », à savoir les effondrements d'États, dont profiteraient les organisations jihadistes, remplaçant les États faillis, se trouvent notamment au Sud. Probablement, la « menace de l'Est », de l'ancien *rideau de fer* à l'actuel arc de tension russo-occidental, est dissuadable, à la frontière de l'UE et de l'OTAN (comme l'a montré l'invasion de l'Ukraine en 2022). Pas l'autre, *transnationale*. La grande menace serait la relance de la prolifération nucléaire, et la menace suprême, l'acquisition d'une ou plusieurs bombes atomiques par des jihadistes - soit une fusion des « menaces de la force » et des « menaces de la faiblesse ». L'Est et le Sud, ainsi que les menaces de la force et de la faiblesse, convergent au Proche-Orient avec, d'une part, le partenariat russo-iranien, la double alliance des États-Unis avec Israël et l'Arabie saoudite, deux États qui n'entretiennent pas de relations diplomatiques, d'autre part, les enjeux

pétro-gaziers et financiers du Golfe, la montée d'une Turquie « néo-ottomane » et « néo-eurasiste » se réislamisant et se désoccidentalisant, le double antagonisme du Proche-Orient, à savoir le conflit irano-saoudien et le conflit irano-israélien, le carré nucléaire du Proche-Orient, à savoir les ambitions de l'Iran, l'arsenal israélien notoire mais non déclaré, les missiles américains en Turquie, le lien étroit entre l'Arabie saoudite et le Pakistan, soit un Royaume (fragile) qui a les moyens de s'acheter la Bombe et une République (instable) qui la possède.

Mais la montée de la Chine populaire (RPC), le partenariat sino-russe, la poussée russe et chinoise au Proche-Orient et en Afrique, le glissement du jihadisme vers l'Afrique subsaharienne ont approfondi ou déplacé les « deux angles » français, d'un Est proche (Russie) à un Est lointain (RPC) et d'un Sud proche (Méditerranée) à un Sud lointain (Sahel). C'est ainsi que la RPC, à l'autre bout du monde, a fait irruption dans les « deux angles » français. Tel est le champ géopolitique du renseignement français.

La dimension numérique du renseignement adverse

La Fédération de Russie s'est engagée dans une restructuration de son architecture numérique depuis le début des années 2010, au lendemain des « printemps arabes » et des manifestations hostiles à la volonté de Poutine de briguer un troisième mandat présidentiel. La Douma a adopté en 2019 la loi FZ90 dite du « Runet souverain », avec pour objectif de se doter de la capacité de se déconnecter du reste du monde si nécessaire et de contrôler les flux de données. Une attitude partagée par la Chine populaire qui, dès la construction de son système, a mis en place un fonctionnement en mesure de contrôler les flux de données entrants et sortants. Depuis le début du conflit russo-ukrainien, les démonstrations de force cyber de Moscou surprennent par une faible intensité au regard des capacités préalablement estimées par ses adversaires. Cela est dû, d'une part, à la perception de la Russie du « cyberespace » qui, pour elle, n'existe pas, d'autre part, à son utilisation transversale des moyens cybernétiques notamment dans la sphère de l'influence, soit la sixième fonction stratégique énoncée par la *RNS* 2022. Rien d'innovant, mais une continuité de la politique russe de déconnexion de son espace informationnel par rapport à celui des pays occidentaux. Le Service du renseignement extérieur (SVR) russe, la Direction principale du renseignement (GRU), organe de renseignement militaire extérieur, et le Service fédéral de sécurité (FSB), chargé de la sécurité intérieure et de la contre-ingérence, travaillent de concert et se livrent à une politique agressive contre leurs équivalents occidentaux, notamment dans la sphère numérique. Il en va de même côté chinois.

L'espace numérique de la République populaire de Chine (RPC) s'est formé dans le souci de maintenir les prérogatives de l'État, donc du Parti[125], en matière de contrôle des informations. L'aspect défensif a vite fait place à un aspect offensif, même si l'ensemble est en *continuum*. Xi Jinping a édifié depuis une dizaine d'années une architecture fonctionnant en vase clos, tout en déployant une cyber-diplomatie visant à façonner un espace numérique mondial plus favorable aux intérêts chinois. Il s'agit de battre en brèche la suprématie américaine, par l'élaboration de nouvelles normes internationales en matière numérique et par l'export vers les pays occidentaux de biens ou services numériques : stockages de données, câbles, capteurs de sons et d'images, logiciels de connectivité, etc. Sachant qu'un Occidental moyen possède environ cinq outils numériques personnels, incluant l'Internet des objets, la Chine s'est assurée une place de choix dans la collecte et le traitement des données qui en sont issues. Il est clair que vendre des biens ou services signifie acquérir et contrôler de l'information. Les relations sino-russes étant de plus en plus étroites et de plus en plus déséquilibrées au bénéfice de Pékin et au détriment de Moscou, le défi chinois est bien le plus massif vu des États-Unis ou d'Europe.

[125] Puisque la Chine communiste est un Parti-État.

Il n'y a pas que l'Est, proche ou lointain, mais aussi le Sud, proche ou lointain. Le « cyber-jihadisme » est une réalité prise en compte depuis 2015, y compris le spectre du « cyber-terrorisme ». L'état de la menace est analysé selon trois axes : le recrutement de spécialistes ; l'utilisation des moyens et la désignation puis la frappe des cibles ; les effets physiques et psychologiques des attaques, notamment leur impact social et politique. On sait que *Daesh* rémunérait sept fois plus un combattant détenant des compétences informatiques qu'un combattant « ordinaire ». L'espace numérique fait partie aussi bien des « fronts » du jihadisme que de la « guerre au terrorisme ». Ainsi, à l'automne 2017, « l'État islamique » irako-syrien ne perdit pas seulement son assise territoriale, il recula considérablement au plan numérique : le « Califat virtuel » subit la même érosion que le « Califat territorial ». La « bataille en ligne » s'articula autour de trois axes : l'interdiction, c'est-à-dire la pénétration par le *Cyber Command* américain du système d'information des jihadistes et la destruction de la totalité de leurs serveurs au terme de trois mois de cyberattaques ; la régulation, c'est-à-dire les mesures suspensives adoptées par les grandes plateformes numériques qui se refusaient jusqu'alors à supprimer nombre de contenus diffusés par les jihadistes au nom de la « neutralité du Net » et qui s'y trouvèrent contraintes par la pression politique des autorités ; l'utilisation d'algorithmes, qui permit de repérer les comptes suspects et de les effacer, à raison de 18000 par mois à l'été 2015 puis de 40000 à l'été 2016.

L'extension exponentielle du cyberespace, la furtivité des attaques, le potentiel de destructivité avec peu de moyens, les dynamiques de lutte du fort au fort comme du faible au fort, entraînent des périls incessamment renouvelés que seule une action coordonnée des services de renseignement nationaux et alliés permettront d'identifier pour parer les risques et menaces inhérents au nouvel « espace ».

LE MÉTAVERS : QUELS ENJEUX, QUELS DÉFIS POUR LE RENSEIGNEMENT FRANÇAIS ?

Karine ROUSSEAUX
Professeur agrégé histoire-géographie, chercheur associé à l'Institut d'études de géopolitique appliquée.

En 1992, Neal Stephenson publiait son roman de science-fiction, *Snow Crash* (*Le Samouraï virtuel*), dans lequel, pour la première fois, apparaît le mot « métavers », un monde virtuel dans lequel les individus se réfugient. Mais ce mot ne rencontre un succès qu'avec l'annonce, en octobre 2021, de la création de « Meta » par Marc Zuckerberg, un monde virtuel et immersif en 3D. Fantasme pour certains, simple évolution de technologies virtuelles déjà existantes pour d'autres, il est aussi un objet d'étude anthropologique pour les possibles ruptures qu'il représenterait dans le domaine cognitif ou comportemental. À cet égard, il présente potentiellement des enjeux et défis multiples pour les services de renseignement, dans ce nouveau champ de conflictualité qu'est le Web.3. Futur lieu de divertissement, de travail, de commerce, d'apprentissage, il sera ainsi, comme l'exprime le général Pierre-Joseph Givre, directeur du CDEC (Centre de doctrine et d'enseignement du commandement), lors du colloque « Métavers, un nouveau champ de bataille ? », en décembre 2022, « un lac de données », un lieu de convergence massive d'informations[126]. Les services de renseignement ont pour objectif de récolter des informations permettant d'assurer la stratégie française de défense et sécurité nationale[127]. Cette récolte, depuis quelques décennies, s'extrait de l'espace numérique avec les réseaux sociaux. Le Métavers, par les nombreuses données open source qu'il pourrait générer, ses capacités plus immersives et le développement de nouvelles formes de menaces touche aux missions des services de renseignement. Ce réseau spatial présente-t-il des singularités, nouvelles problématiques pour les services de renseignement français? Avec, en arrière-plan, la loi d'Amara : « Nous avons tendance à surestimer l'incidence d'une nouvelle technologie à court terme et à la sous-estimer à long terme ».

Illustration de François Schuiten pour le scénario de science-fiction « Chronique d'une mort culturelle annoncée » de la Red Team, avec ses bulles numériques personnalisées (« safe sphères »), janvier 2022[128]

Un enjeu d'abord lié à la lutte contre le cyberterrorisme et la cybercriminalité dans le cadre de la sécurité et sûreté de l'État

La menace terroriste figure dans la dernière feuille de route de la Stratégie nationale du renseignement (SNR), en juillet 2019, comme le premier enjeu prioritaire cité[129]. Les cyberdjihadistes sont déjà très présents sur les réseaux sociaux depuis les années 2010[130]. Le Métavers est une courroie de transmission supplémentaire pour la diffusion de leur propagande et donc de la

126 https://www.youtube.com/watch?v=AdXtp51TJ8E

127 http://www.academie-renseignement.gouv.fr/communaute.html

128 https://redteamdefense.org/saison-1/chronique-dune-mort-culturelle-annoncee

129 http://www.sgdsn.gouv.fr/uploads/2019/07/20190703-cnrlt-np-strategie-nationale-renseignement.pdf

130 https://www.cairn.info/revue-defense-nationale-2015-9-page-32.htm

radicalisation et recrutement de nouvelles recrues, pour améliorer leur préparation et organisation d'attentats, grâce à des camps d'entraînement virtuels reproduisant de manière très précise la réalité. Le dernier rapport d'Europol, l'agence européenne de police criminelle, en octobre 2022, imagine même la création d'un « Califat virtuel ou un État suprémaciste blanc »[131]. La quête du renseignement y est donc cruciale afin de protéger populations et institutions. De plus, la capacité à attirer et « retourner » des individus est décuplée par l'immersion du corps dans cet espace virtuel et les possibilités de personnalisation. Un rapport du Centre d'analyse, de prévision et de stratégie montre que l'avatar, mis en relation avec des individus dont le visage, la voix, la gestuelle s'adaptent aux nôtres, accorde davantage sa confiance car il y a ressemblance. Cette technique est connue en neurolinguistique comme l'« effet miroir », bien étudié dans le cadre des élections notamment, et décuplé par l'immersion dans le Métavers[132]. La présence du renseignement y est donc cruciale.

Quant aux autres formes de cybercriminalité, une étude récente avance l'hypothèse de crimes, déjà présents sur le Net, plus nombreux, plus difficilement détectables au sein du Métavers : blanchiment d'argent, escroquerie financière, fraude, agression et harcèlement sexuels et pédo-criminalité[133]. Les services de renseignement transmettent déjà des informations sur ces sujets dans le cadre de la mutualisation du renseignement cyber. Et concernant l'enjeu en matière d'intelligence économique, il fait aussi parti des enjeux prioritaires du renseignement décrits dans la SNR : « La défense et la promotion de notre Économie » et donc la protection de nos secteurs sensibles et stratégiques. Or, certaines grandes entreprises françaises se tournent déjà vers le Métavers comme Airbus, non seulement pour ses employés (« collaboratif immersif ») mais aussi pour ses clients (« support augmenté »)[134]. Le Métavers pourrait aussi faciliter la « contre-ingérence », c'est-à-dire la transmission d'informations ou la vente de services d'anciens diplomates ou cadres d'entreprises à des pays étrangers et donc nécessiter une présence de la Direction du renseignement et de la sécurité de la défense.

Un enjeu ensuite informationnel et d'influence dans le cadre de la protection des intérêts et de l'intégrité de la nation

La récolte et l'analyse d'informations par les renseignements dans le domaine de la guerre informationnelle revêt de même une importance accrue dans le Métavers, avec l'utilisation plus poussée d'outils de manipulation déjà existants comme les deepfake. Les contre-récits, narratifs alternatifs seront plus persuasifs grâce aux technologies immersives, à l'engagement du corps de l'individu et à l'effet miroir. Ainsi, ce que certains nomment le *Sharp power*, détournement du *soft power*, manière plus agressive de manipuler l'opinion publique, souvent appliqué à la Chine et la Russie, y trouverait là un « terrain de jeu » exceptionnel[135]. Les services de renseignement y sont déjà habitués mais le Métavers rendrait cette stratégie plus efficace dans le projet de déstabilisation d'un pays. La situation de certains pays d'Afrique de la zone sahélienne en témoigne : si les campagnes de désinformation et de dénigrement de la France, par le biais des réseaux sociaux et d'acteurs locaux et étrangers ne constituent qu'un élément d'explication du rejet de la France et de la dégradation de son image, on y perçoit le potentiel que représenterait le Métavers pour des puissances hostiles à un pays pour y

131 https://www.europol.europa.eu/publications-events/publications/policing-in-metaverse-what-law-enforcement-needs-to-know

132 https://www.diplomatie.gouv.fr/IMG/pdf/les_manipulations_de_l_information_2__cle04b2b6.pdf

133 https://documents.trendmicro.com/assets/white_papers/wp-metaverse-or-metaworse-cybersecurity-threats-against-the-internet-of-experiences.pdf

134 https://www.lemagit.fr/etude/Airbus-fait-decoller-sa-realite-mixte-vers-le-metavers

135 https://www.radiofrance.fr/franceculture/podcasts/le-tour-du-monde-des-idees/le-sharp-power-usage-d-informations-trompeuses-a-des-fins-hostiles-3975410

générer des émeutes, révoltes ou mouvements de contestation dans l'opinion publique du pays visé. Les recherches faites sur des mouvements comme « Occupy Wall Street », « Los Indignados » ou les « Gilets Jaunes » montrent le poids des réseaux sociaux dans l'amplification de leurs actions, organisation et durée (« connectives actions ») et leur plus grande perméabilité aux fausses informations ou « récits alternatifs »[136]. Le Métavers pourrait décupler ces possibilités de manipulation et de déstabilisation d'un pays par un autre, avec des armées d'avatars engagés et entraînés pour s'infiltrer dans les sphères du Métavers et rejoindre des mouvements locaux contestataires. Cet enjeu de parer tout risque de « subversion violente », remettant en cause l'État de droit et ses fondements démocratiques est intégré dans la SNR. La question du « cognitive warfare » est de même réinterrogée à l'aune du Métavers : une étude en partenariat avec l'OTAN en 2020 en témoigne : « Le cerveau sera le champ de bataille du XXe siècle. Les conflits futurs se produiront probablement d'abord numériquement puis physiquement, à proximité des centres de pouvoir politique et économique. » Agir sur le cerveau pour faire plier l'adversaire n'est pas nouveau en terme stratégique mais le Métavers offre là encore des opportunités et capacités accrues, que le renseignement doit parer par l'intrusion dans ces bulles informationnelles virtuelles[137].

Un enjeu enfin d'ordre militaire dans le cadre de la protection des opérations militaires et de la sécurité de l'État

Trois services de renseignement dépendent du ministère des Armées. La Direction générale de la sécurité extérieure (DGSE) gère les activités d'espionnage et de contre-espionnage à l'extérieur de la France. La DRSD assure la sécurité des employés, des informations collectées et des installations sensibles. La Direction du renseignement militaire (DRM) est engagée sur les théâtres d'opération militaires tant sur le plan du renseignement stratégique que tactique. Le Métavers est évidemment un possible espace d'entraînement virtuel des soldats. Cela existe déjà comme pour l'exercice de l'opération Orion, programmé pour février-mai 2023, conçu comme un « théâtre opérationnel hybride partagé » (TOHP)[138]. Mais le Métavers ira plus loin dans l'immersion, avec, de plus, des données militaires qui pourront être laissées par les soldats et donc être captées par le renseignement, en protégeant à contrario les nôtres : le programme Scorpion, par exemple, qui vise à numériser le champ de bataille pour nos futurs soldats l'impose. Le renseignement peut jouer aussi un rôle pour transformer un capital informationnel en capital opérationnel, comme le résume le colonel Samir Yaker, chef de bureau « Champs immatériels » au CDEC. Car la récolte de données, d'informations du renseignement pour les armées est cruciale pour accentuer le « dilemme tactique chez l'ennemi » : « Celui qui décide plus vite dans une confrontation militaire a des chances de l'emporter ». Cela repose en partie sur la bonne information captée, transmise au bon moment et bien exploitée dans ce « lac de données » du Métavers et primordiale dans le cadre de l'OSINT, recherche en ressource ouverte, comme en témoigne, par exemple, la possibilité déjà de tracer un membre de la DGSE avec une application de footing (STRAVA)[139]. Le Métavers risque donc d'être une source de menaces supplémentaires par la masse de données ouvertes qu'il pourrait contenir à l'avenir.

***

Face à ces nouveaux défis du Métavers, les services de renseignement disposent déjà de quelques outils : la formation et l'anticipation. Le CDEC en est un exemple avec son dernier colloque. Les récits de science-fiction de la Red Team, soutenus par le

136 https://theconversation.com/gilets-jaunes-medias-et-internet-les-premiers-enseignements-108517

137 https://lerubicon.org/publication/la-guerre-cognitive/

138 https://incyber.org/combattre-metavers-virtuel-existe-deja-pour-experts-notre-armee-terre/

139 https://www.lefigaro.fr/secteur/high-tech/2018/07/09/32001-20180709ARTFIG00286-des-milliers-d-agents-du-renseignement-identifies-a-cause-d-une-appli-de-fitness.php

ministère des Armées et l'Agence de l'Innovation de Défense (AID), sont un autre exemple avec notamment « Chronique d'une mort culturelle annoncée », imaginant des populations européennes enfermées dans des univers de réalité virtuelle (les « safe sphères »), soumises aux fake news et méfiantes face aux consignes de l'armée organisant l'évacuation. Le rôle joué par l'IRSEM par ses recherches dans le « Domaine Renseignement, anticipation et menaces hybrides »[140] permet, de même, une remontée de méthodes, d'apport de connaissances utiles aux différents services de renseignement. Le renseignement pourra aussi s'appuyer sur de nouvelles probables législations européennes : le Digital Services Act s'y penche désormais et l'actuel Règlement général de protection des données devrait s'y adapter.

140 https://www.irsem.fr/la-recherche-a-l-irsem/renseignement-anticipation-et-menaces-hybrides.html

LA « CYBERCRATURE » CHINOISE : UNE MENACE INTERNE ET EXTÉRIEURE ?[141]

Emmanuel VÉRON
Docteur en géographie et spécialiste de la Chine contemporaine.

Indéniablement, la Chine est un acteur étatique majeur du cyberespace, de la cyberguerre, de la cybercriminalité et d'autres formes de cyber-offensives et de cyberdéfense. En parallèle de l'ouverture de la Chine à l'économie globale dès les années 1980, et surtout avec l'accélération de son développement dans les années 1990 et 2000, le régime a progressivement pris en compte Internet. Il est important de bien comprendre le développement d'Internet en Chine pour prendre la mesure de l'usage du cyber dans la stratégie de puissance de Pékin aujourd'hui et les projections futures du régime. Tout au long de l'urbanisation, de l'industrialisation et du développement intérieur de la Chine, le nombre d'internautes chinois n'a cessé d'augmenter. De plus de 200 millions d'usagers au milieu des années 2000[142], on compte plus d'un milliard d'internautes chinois aujourd'hui.

Le régime chinois va trouver en Internet un outil précieux pour soutenir son développement pour surveiller sa population[143] et l'utiliser dans une logique de cyber offensive pour acquérir des informations économiques, sécuritaires et diplomatiques. En somme, le Parti verra dans l'Internet la possibilité de se maintenir au pouvoir et un outil d'espionnage formidable. Cet article rappelle dans un premier temps la reprise en main de l'Internet au service de sa puissance, puis, l'usage offensif majeur en matière d'espionnage, ce qui induira une riposte américaine et une cristallisation de la rivalité systémique.

Le cyber à la croisée des chemins nationalistes et d'administrations centrales de l'État

Balbutiant dans les années 1990, Internet en Chine va rapidement devenir un Intranet. Pour les autorités chinoises, Internet est un outil privilégié à la fois de surveillance et d'espionnage. Le cyber chinois va commencer à être offensif dès la fin des années 1990, en particulier à l'endroit des États-Unis. En 1999, le bombardement par erreur de l'ambassade chinoise à Belgrade et la collision de deux avions militaires, l'un chinois, l'autre américain, vont induire les premières cyber-attaques en direction des États-Unis. Ces premières attaques ont des fins politiques et sont signées par deux groupes : *China Eagle Union* et *Honker Union of China*[144]. Ces deux groupes sont composés de jeunes chinois agissant de leur propre chef, motivés par un nationalisme exacerbé. Rapidement, en parallèle de la fin des négociations sur l'entrée de la Chine à l'OMC en 2001, le Parti va reprendre le contrôle de ces groupes. La volonté de contrôle des *hackers* par le Parti sera rapide et efficace afin de mieux contrôler les capacités, mais aussi pour enrichir les savoir-faire en matière cyber dans les services de police, militaire une perspective de politique intérieure et de politique extérieure.

Dès lors, Internet est vu comme une formidable plate-forme de contrôle de la population chinoise (en cela la collaboration du régime avec les BATX – Baidu, Alibaba, Tencent et Xiaomi - est décisive) d'une part et à l'étranger d'autre part, un vecteur de

[141] Une partie de ce texte est issu d'un entretien pour le site Diploweb, publié en 2021. Aussi, plusieurs mises à jour tout au long de l'année 2022 nourrissent cet article.
[142] https://larevuedesmedias.ina.fr/le-prodigieux-developpement-dinternet-en-chine
[143] https://hal.archives-ouvertes.fr/hal-02166585/document
[144] https://www.youtube.com/watch?v=JeAQHnkJXik&ab_channel=ARTE

puissance et d'offensive cyber, plus précisément de cyber-espionnage et d'actions clandestines. Tout au long des années 2000, Internet en Chine a permis de cibler des cibles molles, des serveurs du monde entier pour littéralement piller des contenus, des savoirs, des brevets etc. Puis les cibles (souvent les sociétés occidentales) se sont renforcées et ont augmenté les niveaux de protection.

Que ce soit les unités cyber comme la plus célèbre, militaire, l'unité 61398[145], basée à Pudong (Shanghai) ou les « cyber-nationalistes » appelés *wumao dang*, du nom des 5 centimes gagnés par dénonciation ou signalement de contenus contraires à la doxa du régime, Pékin compte sur la masse démographique d'une part et les savoir-faire technique d'autre part. Le domaine cyber fait écho aux stratégies militaires passées (Sun Zi et *L'art de la guerre* ou le *36 Stratagèmes* par exemple) en raison de la nature des attaques, de l'espionnage et autres modalités. En effet, le cyber privilégie l'indirect, les voies détournées et les attaques à distance sans exposer une armée, un État, etc.

L'usage du cyber offensif au service de Parti et de la puissance chinoise

L'arrivée au pouvoir de Xi Jinping va être marquée par le renforcement du contrôle du Parti sur l'ensembles de l'État. L'outil cyber se retrouvera recomposé et renforcé. L'intégration du champs cyber global se fera au travers du 13e Plan quinquennal (2016-2020). En amont, dès 2015, Xi Jinping formule ce qui sera la base en pleine expansion d'une administration centrale pour le cyber. L'Administration du cyberespace de Chine (CAC) est conçue comme l'organisme central de réglementation, de censure, de surveillance et de contrôle de l'Internet pour la Chine. Le bureau détient également le titre administratif du Bureau du parti de la Commission centrale des affaires du cyberespace. Cette administration centrale est le propriétaire majoritaire du *China Internet Investment Fund*, qui détient des participations dans des entreprises technologiques telles que ByteDance (*TikTok*), Weibo Corporation, SenseTime et Kuaishou. Ces opérateurs sont tous mobilisés pour la surveillance de masse des individus et alimenter le programme dit de « Système de Crédit Social ».

L'article 7 de la loi chinoise sur le renseignement national de juin 2017 dispose que toutes les sociétés et les individus chinois doivent coopérer avec les services de renseignement chinois afin de protéger la « sécurité nationale ». Les termes sont à la fois clairs dans les structures (ou organes) désignées mais restent évolutifs et non définitifs. Au contraire ceci est très mouvant, inclusif et large. Ceci apparaît au grand public en 2017, période du début des tensions accélérées entre la Chine et les États-Unis, notamment sur le débat des technologies Huawei, des réseaux 5G et de la compétition technologique et des marchés entre Chinois et Américains. Ce fameux article 7 n'est que le prolongement, la montée en puissance et la mobilisation des forces démographiques chinoises de Chine ou des diasporas dans une logique de puissance et d'intimidation[146]. Un tel article permet de galvaniser les troupes tout en désignant l'étranger comme potentiel agent de subversion et d'ordonner un glissement stratégique sur le sentiment d'une Chine menacée pour justifier l'expansion de la puissance et de ses moyens. C'est enfin un message des autorités envoyé aux populations chinoises de mobilisation générale pour opérer à la poursuite du rattrapage technologique dans tous les domaines et dans toutes les directions.

De telles ambitions existaient à travers le programme 863 ou de développement de haute technologie dans les années 1980 ou le programme 973 à la fin des années 1990. Ces programmes avaient comme

[145] Unité cyber de l'APL, basée à Shanghai a été fondée en 2004 et regroupe plusieurs milliers d'agents. Il difficile d'avoir un chiffre précis sur l'ensemble des opérateurs. Cette unité est rattachée au 3e département de l'état-major général de l'APL. Il existe d'autres unités cyber, dans d'autres territoires chinois.

[146] https://www.csis.org/programs/strategic-technologies-program/technology-and-innovation/cybersecurity-and-governance/china

objectif à l'instar du plan Made in China 2025[147], un rattrapage technologique et sont basés sur le recueil d'informations via des universités (coopérations, échanges etc.), l'espionnage, la compromission et « l'achat » de savoir-faire. Il fallait recueillir des informations sensibles, protégées et non protégées. En cela la Chine a une longue histoire du renseignement, de l'espionnage. Ce dernier est bien ancré dans la culture chinoise. Le PCC a institutionnalisé cela d'abord pour chasser les ennemis du Parti, puis pour le développement militaire, technologique et aujourd'hui massivement sur des questions économiques et technologies à la fois dans le monde civil comme militaire, où le passage d'une technologie de l'un à l'autre sert la puissance chinoise[148].

L'importance du Cyber en Chine et la rivalité avec les États-Unis

En 2021, l'ampleur du marché chinois de la cybersécurité a atteint 62,7 milliards de RMB (8,64 milliards de dollars), soit une augmentation de 9,5 milliards de RMB (1,3 milliard de dollars), soit 17 %, par rapport à 2020. En effet, le marché de la cybersécurité du pays est entré dans une période de développement rapide, principalement motivé par deux facteurs : la conformité aux politiques et la modernisation industrielle. Notamment, les services de sécurité réseau sont devenus la piste à la croissance la plus rapide du marché, les entreprises allouant un budget plus élevé de leurs dépenses de sécurité aux services de cybersécurité. Cette année, les revenus du marché chinois de la cybersécurité atteindront 14,05 milliards de dollars américains, les solutions cybernétiques représentant le plus grand segment de marché avec un volume total de 9,42 milliards de dollars américains.
Dans une ébauche de 2021 de son plan politique le plus complet pour l'industrie de la cybersécurité en Chine, le ministère de l'Industrie et des Technologies de l'information (MIIT) avait exigé que des industries importantes comme les télécommunications allouent 10% de leur budget de mise à niveau informatique à la cybersécurité d'ici 2023[149].

Face à ce développement rapide et ces efforts financiers majeurs, l'administration américaine réagit. Dès 2014-2015, l'administration Obama, marquée par d'importantes et récurrentes affaires d'espionnage va mettre en lumière l'unit 61398 par une conférence de presse du DOJ américain donnant les détails sur les cibles américaines et les auteurs chinois de cette unité cyber. Lors d'une visite d'État de Xi Jinping à Washington en 2015, la Chine et les États-Unis s'engagent à ne plus recourir au cyber pour voler des secrets technologiques et économiques. Mais les révélations de Snowden embarrassent l'administration Obama…

Puis, les services de sécurité américains, dans la continuité de l'arrivée au pouvoir de Trump vont faire monter en puissance l'ensemble des dispositifs de cybersécurité. Par exemple, la *Cybersecurity and Infrastructure Security Agency* (CISA)[150] publie des rapports sur la « cyber-activité malveillante chinoise ». Les États-Unis organisent également des séances de témoignages diffusées publiquement, explorant les cyber-activités et les menaces de la Chine.

Les dirigeants chinois sont en train de mettre en place le régime de gouvernance le plus étendu pour le cyberespace et les technologies de l'information et des communications de tous les pays du monde[151]. Reconnaissant que la technologie a progressé plus rapidement que la capacité du gouvernement à la contrôler, Pékin a rapidement élaboré un cadre politique et réglementaire couvrant la cybersécurité, l'économie numérique et le contenu des médias en

[147] Elle se poursuit aujourd'hui avec le 14e Plan quinquennal et la « Vision 2035 » afin de recueillir les besoins nécessaires pour nourrir l'écosystème d'innovation chinois.
[148] https://www.aspi.org.au/report/mapping-chinas-tech-giants
[149] https://www.china-briefing.com/news/chinas-cybersecurity-industry-a-market-analysis/
[150] https://www.cisa.gov/uscert/china
[151] https://www.csis.org/programs/strategic-technologies-program/other-projects-cybersecurity/chinas-emerging-cyber

ligne, le tout sous un même ensemble[152]. Ces éléments couvrent les règles de protection des données, les infrastructures critiques, le cryptage, le contenu Internet, ainsi que le renforcement de l'industrie chinoise des TIC. La loi chinoise sur la cybersécurité - qui a peut-être reçu le plus d'attention - est au centre d'une vision beaucoup plus large[153]. La plupart des lois et stratégies actuelles sont définitives, mais bon nombre des mesures et normes correspondantes sont encore à l'état de projet[154].

L'effort de Pékin est déjà plus complet que celui des États-Unis et de l'Europe. La dégradation des relations entre la Chine et le reste du monde, en priorité l'occident verra une progression forte des problématiques de cybersécurité, marquant un seuil de basse intensité. Les interdépendances économiques et commerciales importantes entre ces deux pôles hétérogènes suffiront-elles à ne pas franchir le seuil de la haute intensité ?

[152] https://www.boozallen.com/insights/cyber/chinas-cyberattack-strategy-explained.html

[153] Un véritable écosystème chinois cyber est en voie rapide de maturation, notamment avec les sociétés : Antiy Labs, Bangcle, Beijing Zhizhangyi Science & Technology Co., Ltd, Bluedon, BUGBANK, DBAPP Security, Ltd, H3C ou encore Threatbook.

[154] https://thediplomat.com/2022/04/chinas-new-focus-on-us-cyber-activities/

POLITIQUE ET GÉOPOLITIQUE DES SERVICES DE RENSEIGNEMENT AU MOYEN-ORIENT

Julien DREVETON
Analyste à l'Institut d'études de géopolitique appliquée.

Des « services de renseignement » aux « services de sécurité »

Si l'on regroupe dans notre analyse les services de renseignement d'une si complexe région du monde, on ne saurait en un seul article en expliquer toutes les subtilités. Il est cependant possible de tirer des clés de compréhension des services de renseignement (*moukhabarat*) au Moyen-Orient à travers deux axes. Politique, d'abord. Géopolitique, ensuite. Nous examinerons en ce sens les services turcs, iraniens, saoudiens, israéliens et syriens.

D'un point de vue politique, dans le sens de lutte pour le pouvoir au niveau national, ces services ont pour rôle la pérennité du régime politique voire du clan ou de la famille au pouvoir. Ils diffèrent en cela des services occidentaux. Jérôme Poirot, ancien adjoint du coordinateur national du renseignement en France, décrit dans son *Dictionnaire du renseignement*, trois critères pour qualifier un service de renseignement (SR)[155]. Le fait d'être une administration menant la politique du gouvernement, la poursuite de l'intérêt national (contrairement à la police qui produit du renseignement dans le cadre judiciaire) et enfin la reconnaissance par les services étrangers[156]. Cependant, il faudrait, pour comprendre les SR du Moyen-Orient, ajouter un quatrième critère : le rôle politique de maintien au pouvoir du régime en place. C'est pour cela qu'Agnès Levallois, chercheuse et consultante, les qualifie plutôt de « services de sécurité »[157]. Ici, « sécurité » ne signifie pas « sécurité des citoyens » ou « lutte contre le terrorisme » mais bien « sécurisation du pouvoir en place » ou « lutte contre la contestation politique interne ». Nous tenterons de décrire en quoi la place qu'occupe les services dans l'appareil d'État éclaire ou non leur rôle politique.

De plus, ces « services de sécurité » du régime prennent place dans la politique étrangère. Turquie, Iran, Arabie saoudite, Israël et Syrie utilisent leurs services pour influencer la géopolitique de la région. Les opérations clandestines sont alors le prolongement de la sécurisation du régime politique, par d'autres moyens. C'est le cas de la manipulation du terrorisme et des groupes armés « jihadistes ». Nous chercherons à voir si des actions de l'ombre peuvent être menées en contradiction avec les discours officiels pour servir des intérêts stratégiques. Surtout, il sera intéressant de voir quel État choisit quelle action de l'ombre et pourquoi. L'objet de ce questionnement, que l'on verra par le terrain de la guerre en Syrie, pourra montrer en quoi les SR sont de véritables révélateurs géopolitiques des positionnements réels des États.

Un rôle politique : la pérennisation des régimes

Pour expliquer le rôle des services dans la pérennité des régimes, on peut élaborer une échelle de leur intégration politique dans l'appareil d'État. Agnès Levallois distingue les services saoudiens, relativement intégrés, qu'elle appelle « outils du pouvoir » des services syriens, très intégrés, qu'elle nomme « centre de pouvoir »[158]. Nous tenterons d'approfondir et d'élargir cette théorie en proposant une analyse des SR israéliens, saoudiens, turcs,

[155] Poirot Jérôme, Dictionnaire du renseignement. Perrin, « Hors collection », 2018.
[156] *Ibid*.
[157] Levallois, Agnès. Espionnage et renseignement au Moyen-Orient. Conférence du 24 octobre 2017.
[158] Levallois, Agnès. Espionnage et renseignement au Moyen-Orient. Conférence du 24 octobre 2017.

iraniens et également syriens. Nous irons alors du moins au plus intégré politiquement. Dans le même temps, chacun a pour mission la survie de l'État.

À commencer par les israéliens. On remarque les priorités données pour la survie de l'État hébreu jusque dans le découpage institutionnel des services. En effet, le « *Shabak* », service de sécurité intérieur, est divisé en trois pôles : affaires arabes, affaires non-arabes et sécurité intérieure[159]. Avoir une branche entière consacrée aux affaires arabes montre bien la volonté d'assurer la sécurité du pays contre le groupe *Hamas* et ses attentats récurrents. Le très connu Mossad est également un exemple de l'intégration politique des SR israéliens. Il est en effet directement placé sous la tutelle du Premier ministre. C'est ce dernier qui décide les opérations clandestines, prérogatives du Mossad.

Plus encore intégrés politiquement sont les SR saoudiens. Le *General Intelligence Presidency* (GIP) est placé en lien direct avec le roi[160]. La pérennité de l'État et du régime passe pour le GIP par le contrôle de la population, mais surtout par une focalisation sur les mouvement islamistes, considérés comme principaux mouvements d'opposition. Cela est dû au traumatisme de la prise de la Grande Mosquée de La Mecque en 1979, par des extrémistes wahhabites[161], qui voulaient le départ de la famille Saoud. Cet événement a précipité les nominations de spécialistes anti-terroriste au sein des SR. Parce que la famille régnante détenait, et détient toujours, une légitimité du fait du régime monarchique, il lui a été possible de placer des experts et non pas des membres de la famille à ces postes[162]. Un mécanisme qui, nous le verrons, serait impossible en Syrie par exemple.

La Turquie peut se placer sur une même échelle d'intégration politique des SR dans l'État. Le MIT (Millî İstihbarat Teşkilatı ou Organisation Nationale du Renseignement) a pour chef depuis 2010 Hakan Fidan, un proche du pouvoir. Il fut nommé par R. T. Erdogan lui-même. Plus tard, alors qu'il voulait s'engager en politique, Hakan Fidan fut immédiatement repris par le président et maintenu en poste[163]. Erdogan voulait ainsi garder un de ses proches à ce poste stratégique. Le chef d'État semble depuis 2016 avoir accéléré la stratégie de pérennisation de son propre pouvoir autocratique[164], passant, nous venons de le voir, par la sécurisation du soutien des services.

Entrons désormais dans les services qui ne sont pas seulement liés au pouvoir mais *sont* le pouvoir. Les SR iraniens et syriens. Il faut d'abord rappeler que la République islamique d'Iran compte deux armées : l'armée régulière et les *pasadaran* (« gardiens de la révolutions ») qui sont garants du maintien de l'État révolutionnaire[165]. Au sein des *pasadaran*, on remarque une force d'opération clandestine : *Al-Qods*[166]. Cette force parallèle est plus qu'intégrée au pouvoir, elle représente le pouvoir. *Al Qods* est ainsi placé sous la tutelle directe du Guide Suprême. Il s'agit d'une force d'intervention, bras armé du pouvoir iranien, qui ne connaît pas d'intermédiaire institutionnel. Par ailleurs, si les gardiens de la révolution s'affairent à la stabilité du régime, ils le font afin d'assurer leur propre stabilité. On les sait par exemple particulièrement inclus dans l'économie du pays, en contrôlant les principales industries et ressources d'Iran[167].

Les *moukhabarat* syriens sont dépositaires de, et commandés par, les membres de la famille Assad pour perpétuer leur régime. Hafez al-Assad basait déjà son maintien au pouvoir sur les services[168]. Plus

[159] Elkaïm, David. Le renseignement israélien : entre processus de paix et sécurité de l'État hébreu. 2017.
[160] Bou Nader, Philippe. Le Hezbollah en Syrie et en Irak : une force au service du panchiisme iranien. 2017.
[161] *Ibid*.
[162] Levallois, Agnès. Espionnage et renseignement au Moyen-Orient. Conférence du 24 octobre 2017.
[163] Hurriyet. Turkey's former intel chief withdraws decision to run for parliament, returns to MİT. Mars 2015.
[164] Marcou, Jean. « Acteurs et enjeux du système politique turc contemporain ». 2022.
[165] Posh, Walter. Les services de sécurité d'Iran, un corps multiple au cœur du pouvoir. 2017.
[166] *Ibid*.
[167] Cibien, Laurent. L'Iran à court d'eau. Arte, 2018.
[168] Rey, Matthieu. Histoire de la Syrie (XIXe-XXIe

tard, au moment de résister aux Printemps arabes en 2011, le chercheur François Burgat parle de « construction de la guerre civile »[169] par les SR, une sorte de montée aux extrêmes créée de toute pièce. Pour la survie du régime, les services syriens ont pratiqué et semblent pratiquer encore la désinformation et la répression, notamment par la torture et les exécutions sommaires de syriens[170]. Ce déferlement de violence a ainsi accéléré la radicalisation de la rébellion, transformant la protestation politique en guerre civile et justifiant ainsi de nouvelles violences étatiques[171]. Outre cet exemple, la pérennité du régime par les SR est aussi structurelle. La communauté de renseignement syrienne est composée d'un service de sécurité générale (*al-amn al-`amm*), renseignements généraux au service du chef de l'État[172]. Ils sont réputés pour leur fort ancrage au sein de la population, donnant ainsi l'impression d'une surveillance constante. Le service de sécurité politique (*al-amn al-siyassi*)[173] surveille opposants et étrangers. Enfin, on remarque un « service de sécurité aérienne » (*al-amn al-jawwi*)[174]. Sous ce nom se cache en fait un « service action » menant les opérations clandestines. Chacun des chefs du renseignement a un lien familial avec Bachar al-Assad : les SR *sont* le régime syrien.

Un rôle géopolitique : les usages stratégiques du *jihad*

Le *jihad*, que l'on comprend ici comme le combat des groupes armés se prétendant eux-mêmes « jihadistes », peut être utilisé par les services afin de servir les intérêts de l'État. C'est particulièrement le cas dans le conflit syrien, dont la complexité sert l'Iran (allié d'Assad), la Turquie (adversaire d'Assad) et le régime syrien lui-même.

On voit la construction d'un réseau de renseignement iranien en Syrie[175]. Ce réseau passe par l'implication locale des services iraniens encadrant la population par des scouts chiites[176] et recourant à des bergers frontaliers comme informateurs[177]. Surtout, le soutien de l'Iran à Bachar al-Assad passe par des groupes armés transnationaux opérant en Syrie et en Irak, des milices formées en Iran ou au Liban et dirigées par les gardiens de la révolution via le groupe armé *Hezbollah*. La République islamique appelle ces milices au *jihad* en Syrie afin de « préserver les lieux sacrés chiites »[178]. Dans le même temps, le discours officiel persiste à nier l'implication directe de l'Iran dans le conflit. Ces milices pakistanaises, afghanes, irakiennes ou « milices chiites internationales » permettent alors de mener le *jihad* pour soutenir le régime syrien sans que des iraniens soient impliqués[179]. Le Hezbollah arbore même les insignes de ces milices pour se confondre et cacher sa présence[180].

On se rend compte d'un autre cas d'usage stratégique du *jihad* : la « manipulation du terrorisme » en Syrie[181]. En 2011, les SR ont volontairement relâché des prisons syriennes des criminels et des jihadistes, individus se retrouvant par la suite à la tête de divisions de l'État islamique[182]. Cette opération d'Assad voulait encourager le développement de mouvements djihadistes radicaux pour forcer la population à choisir son camp, tout en appelant les États

siècle), Paris, Fayard, 2018.

[169] François Burgat. Pas de printemps pour la Syrie: Les clés pour comprendre les acteurs et les défis de la crise (2011-2013). p.19.

[170] Glasman, W. Les ressources sécuritaires du régime. 2013. In Pas de printemps pour la Syrie p.33.

[171] *Ibid*.

[172] *Ibid*.

[173] *Ibid*.

[174] *Ibid*.

[175] Bou Nader, Philippe. Le Hezbollah en Syrie et en Irak : une force au service du panchiisme iranien. 2017.

[176] Posh, Walter. Les services de sécurité d'Iran, un corps multiple au coeur du pouvoir. 2017.

[177] Rodier, Alain. Entretien semi-directif réalisé le 22 avril 2021.

[178] Channel 4 News. Iran's proxy war in Syria, explained. Mai 2017.

[179] Posh, Walter. Les services de sécurité d'Iran, un corps multiple au coeur du pouvoir. 2017.

[180] *Ibid*.

[181] Glasman, W. Les ressources sécuritaires du régime. 2013. In Pas de printemps pour la Syrie. p.52.

[182] *Ibid*.

étrangers à aider le régime syrien contre l'EI. Ce mécanisme a été particulièrement efficace pour radicaliser la rébellion, légitimant ainsi la répression la plus implacable.

Il faut citer enfin « l'affaire des camions du MIT »[183]. Par ces camions, la Turquie aurait livré entre fin 2013 et début 2014 des armes aux jihadistes de l'État islamique[184]. L'objectif : servir une stratégie de tolérance et de soutien aux ennemis du régime syrien. On connaissait déjà la « mansuétude »[185] de la Turquie vis-à-vis du groupe jihadiste Hayat Tharir al-Cham (HTC) du fait de ses alliances avec des milices turques. Les ennemis de mes ennemis sont mes amis. Tous les moyens semblent avoir été bons pour contrer Assad, même une livraison d'armes à l'EI, censée rester secrète. Les journalistes turcs ayant partagé l'affaire furent arrêtés en 2015 avant d'être libérés à la suite d'une décision de la Cour Constitutionnelle[186].

Des révélateurs géopolitiques ?

On préfère parler de « services de sécurité » des régimes politiques au Moyen-Orient, dont les services tendent à pérenniser le pouvoir. Cet effort de résilience passe par une intégration profonde des services dans les appareils d'État, voire au sein du clan ou de la famille en place. Le contrôle de la population et de l'opposition politique comme la lutte antiterroriste en sont les principales prérogatives au niveau national (comme en Arabie saoudite). Au niveau international, les services menants des opérations clandestines sont enclins à l'action par procuration, voire à l'instrumentalisation de groupes armées jihadistes pour arriver à leur fins (par l'Iran, la Syrie et la Turquie). Ils le font afin de pallier une faiblesse militaire (l'Iran ne pouvant mener un affrontement direct) ou à une intégration dans la communauté internationale les empêchant une large marge de manœuvre (la Turquie s'étant engagée avec les occidentaux contre l'EI). Ceci étant, l'analyse des services en fait des révélateurs géopolitiques, dévoilant les opérations menées à l'ombre des discours.

[183] Le Monde. Un journal turc publie les images d'armes livrées par la Turquie aux djihadistes en Syrie. Mai 2015.
[184] BBC News. « MİT tırları soruşturması: Neler olmuştu? ». 27 novembre 2015.
[185] Rodier, Alain. Entretien semi-directif réalisé le 22 avril 2021.
[186] BBC News. « MİT tırları soruşturması: Neler olmuştu? ». 27 novembre 2015.

FACE AUX GUERRES PROBABLES DU XXIe SIÈCLE, L'INTELLIGENCE ÉCONOMIQUE DOIT ÊTRE SOCIÉTALE EN AFRIQUE

François Xavier NOAH EDZIMBI
Analyste en stratégie internationale, en géopolitique, géoéconomie, intelligence et sécurité économiques.

À l'heure de la réaffirmation des puissances, phénomène visible depuis le début du XXIème siècle, les nouveaux visages de la guerre menée entre les sociétés sont hybrides et mouvants. Comme conséquence, les acteurs de l'espace mondial sont confrontés à la nécessité d'intégrer la guerre économique et la guerre informationnelle dans leurs matrices stratégiques, du moment où les rivalités s'étendent désormais à l'ensemble des domaines économique, social, culturel, etc. L'âge de l'information est aujourd'hui celui d'un chaos relationnel fait de dépendances souterraines, de jeux d'influence et de fabrique des perceptions. Le cadre spatial et mental dans lequel se déploient les guerres ayant considérablement évolué, les objectifs et les moyens développés pour les atteindre ont, entre autres, également subi des mutations profondes. Ainsi, la guerre ne visant plus à tuer des individus mais à détruire une entité collective, et à n'en laisser subsister que des individus sans volonté, il est judicieux pour les Africains, dont les objectifs sont de se développer et disposer d'une place de choix en tant qu'acteur influent dans la conception et la mise en œuvre de décisions stratégiques internationales, d'explorer de nouvelles voies dans l'intelligence économique, de changer de logiciel, autrement dit leur état d'esprit, afin qu'ils s'arriment aux jeux et aux enjeux de puissance post-bipolarité.

La mondialisation a multiplié les frictions et les rivalités entre acteurs de l'espace mondial. Aussi, l'explosion des échanges a pour corollaire celui des affrontements. De fait, pour diverses raisons, la guerre n'est plus un effet de la volonté humaine. Elle est devenue un état relationnel permanent, une situation contextuelle. La guerre n'est plus livrée, mais vécue dans un état de guerre continuel. En partie discrédité, l'homicide interétatique est devenu moins fréquent. En contrepartie, les affrontements non-militaires se sont multipliés[187]. Les rivalités classiques autour des ressources primaires s'étendent désormais à l'ensemble des domaines économique, social, culturel, etc. L'âge de l'information est celui d'un chaos relationnel fait de dépendances souterraines, de jeux d'influence et de fabrique des perceptions. L'âge de l'accumulation des moyens a fait place, parallèlement, à celui de leur combinaison et du traitement transversal des données. Pour illustration, la course à la suprématie technologique, notamment dans les domaines de l'intelligence artificielle (IA), de l'informatique quantique et de la 5G, entre les États-Unis et la Chine, dessine une géopolitique de l'innovation qui laisse peu de place à une Afrique en mal d'autonomie stratégique[188]. Les approches stratégiques pluridisciplinaires sont désormais incontournables.

La guerre économique, expression d'une réaffirmation des puissances en ce début de XXIe siècle, est un mode de domination qui évite de recourir à l'usage de la puissance militaire pour imposer une suprématie durable. Il ne s'agit plus de soumettre l'autre par la force, mais de le rendre dépendant par la technologie, l'économie et la culture. À la volonté guerrière des anciens empires se substitue désormais une forme de duplicité des

[187] Bruno Racouchot, « Des guerres à venir, de la guerre économique et de la dislocation potentielle de notre monde », *Revue internationale d'intelligence économique*, 2021/1, Vol. 13, pp. 163-174.
[188] Philippe Clerc et Patrick Cappe De Baillon, « Course à la suprématie technologique et géopolitique de l'innovation. Où il est question d'autonomie stratégique et de souveraineté », *A.D.B.S, I2D, informations, données et documents*, 2020/3, N° 3, pp. 22-33.

nouveaux conquérants qui instrumentalisent la morale afin de masquer la finalité de leur stratégie[189]. Cette conception permet de comprendre le contexte stratégique de guerre globale, où l'économie constitue une part majeure mais non exclusive. Le choc des idées retrouve ici ses lettres de noblesse qui, majoritairement, opposent le modèle occidental à d'autres modèles comme celui de la Chine, de la Corée du Nord, de l'Iran ou encore de la Russie. La guerre s'étend donc au domaine des perceptions et mobilise jusqu'à la psychologie et l'ingénierie sociale. Les nouveaux visages de la guerre, menée entre les sociétés, sont hybrides et mouvants. Ils troublent le citoyen, dans la mesure où ce dernier a peur de l'inconnu. Toutefois, il est judicieux pour toute société de lutter contre la tentation de se rassurer collectivement en s'accrochant à des biais cognitifs obsolètes[190]. L'esquisse d'une géopolitique de l'innovation est envisagée à travers « la guerre des intelligences ». Plusieurs rivaux sont engagés, mais la bataille se livre entre deux « hégémons » : États-Unis et Chine. La stratégie est ici une dialectique des intelligences, dans un milieu conflictuel, fondée sur l'utilisation ou la menace d'utilisation de la force à des fins politiques. La « guerre des intelligences », qui se joue au cœur des dynamiques géopolitiques de l'innovation, s'exprime à travers la bataille pour la suprématie technologique sur trois technologies issues de la révolution numérique : intelligence artificielle, informatique quantique et 5G, ainsi que sur le nouveau modèle de création de valeur et de développement à travers « le choc des capitalismes[191] ». Cette opposition de modèles marque une rupture dans le jeu des rivalités. En effet, la compétition se déroule entre des pays et des acteurs, les nouveaux émergents, qui n'ont pas les mêmes conceptions philosophiques du monde occidental, ni les mêmes rapports au temps. Ils n'ont pas les mêmes conceptions de la place de l'individu dans la société, ni les mêmes logiques de pensée et ne respectent pas les mêmes règles du jeu.

Les Africains, pour leur part, trouvent jusqu'ici des difficultés à intégrer les ingénieries cognitives civilo-militaires qui caractérisent les relations internationales. Ils sont peu préparés au contexte de guerre systémique, qui est celui de la combinaison et des interactions. L'intégration d'une culture et d'une méthodologie de combat dans leurs approches globales est, pour eux, le principal moyen pour contrer des compétiteurs qui ne visent pas tant à les briser frontalement qu'à provoquer leur dislocation. L'Afrique se doit de réajuster ses grilles de lecture des rapports de forces politiques, culturels, technologiques et économiques mondiaux, ainsi que des stratégies sophistiquées de puissances mondiales comme les États-Unis et la Chine. Face à ces deux géants, usant des règles du jeu à géométrie variable, faisant preuve de force et de ruse (arme de l'extraterritorialité du droit américain, interventionnisme de l'État chinois, « encerclement cognitif »), « l'agir stratégique » africain se doit de restructurer ses politique, moyen et outil de renseignement. Ces déploiements et renforcements de son arsenal de sécurité économique contribueront à limiter une rénovation des sphères d'influence et l'étendue d'une sous-traitance des affaires africaines par les puissances mondiales et émergentes.

La rénovation des sphères d'influence : l'Afrique comme espace d'affirmation de la puissance technoéconomique des États-Unis et de l'influence française sur l'espace mondial

Le contexte contemporain de compétition permanente entre les puissances a ouvert de nouveaux champs d'affrontement immatériels appelés *political warfare*, la guerre par le milieu social (GMS), qui consiste à agir sur les structures sociales et cognitives de la cible[192]. La guerre de l'information et l'influence connaissent un important développement. La mesure de cette révolution dans

[189] Christian Marcon, « L'intelligence économique sera géopolitique et sociétale », *Revue internationale d'intelligence économique*, 2020/2, Vol. 12, pp.107-120.
[190] Bruno Racouchot, *op. cit.*
[191] Philippe Clerc et Patrick Cappe De Baillon, *op. cit.*
[192] Raphaël Chauvancy, « L'ingénierie cognitive, arme de guerre », *Revue internationale d'intelligence économique*, 2021/2, Vol. 13, pp. 11-22.

l'art du combat est sous-estimée/mésestimée en Afrique, lorsqu'il se constate que les *fake news* monopolisent l'attention et bornent l'innovation conceptuelle. La géopolitique a investi le champ des relations économiques et commerciales internationales, et la guerre économique procède précisément de cette évolution paradigmatique. « Au mode traditionnel de confrontation des États-nations par la guerre militaire a succédé une nouvelle géographie des rapports de force dominé par la recherche de la puissance géoéconomique, culturelle et sociétale[193] ». Il s'observe l'existence de relations commerciales plus tendues, de la multiplication des actes délictueux, facilités par la révolution de l'Internet et du développement d'une cybercriminalité, des grandes entreprises et des États qui se livrent à une féroce concurrence. Ainsi, malgré les déclarations officielles, notamment des chancelleries occidentales, sur l'existence d'un monde dans lequel « les grandes puissances ne se définiraient pas par leur sphère d'influence[194] », les sphères d'influence réinvestissent le champ des relations internationales. L'impact économique consécutif de la guerre entre Russes et Ukrainiens est, pour certains économistes, plus important que celui lié à la pandémie liée au Covid-19[195]. En effet, d'après ces experts, le conflit russo-ukrainien engendre trois évolutions structurantes pour les économies étatiques. Premièrement, il signe un nouvel âge des sanctions économiques internationales, qui va contraindre la dépendance de certains pays, ceux de l'Union européenne (UE) en particulier, aux hydrocarbures. Deuxièmement, le conflit augmente les prix des produits alimentaires à l'échelle internationale et, troisièmement, il entraîne une importante hausse des dépenses militaires tant chez les puissances mondiales que celles émergentes, conduisant à plus d'insécurité mondiale. Ces différentes incertitudes conduit certains acteurs à renforcer leurs politiques de recherche, de développement et d'industrialisation, afin de disposer d'une puissance décisive dans une guerre économique[196] qui caractérise les relations internationales post guerre froide.

La quête et la collecte d'informations est ainsi le nerf de la guerre économique pour les États-Unis. Pour ce faire, Washington a créé un système d'espionnage électronique connu sous le nom de *Echelon*, qui surveille et espionne ses alliés géopolitiques mais concurrents économiques. Dès 2013, les États-Unis consacrent d'importants moyens au renseignement : 40% de l'arsenal de renseignement est mobilisé dans l'intelligence économique[197]. La même année, et selon des informations publiées par *Le Monde*, 10 milliards de dollars ont été mobilisés pour l'agence nationale de sécurité (*NSA*) qui employait 60 000 salariés directement en plus de 40 000 sous-traitants et disposait de plus de 40 stations d'écoute électromagnétiques implantées dans douze pays[198]. Les révélations d'Edward Snowden, ancien agent de la *NSA*, dévoileront que les géants du web font de l'espionnage et du renseignement économiques : *Google*, avec *Gmail* et *Android*, équipe plusieurs centaines de millions de *Smartphones* et est un collecteur de données, comme *Facebook* qui a plus d'un milliard d'utilisateurs, de même qu'*Amazon* et ses milliards de clients[199]. Pour illustration, les portables personnels des d'anciens dirigeants

[193] Christian Harbulot, *Sabordage : « comment la France détruit sa puissance »*. Paris, Éditions François Bourin, 2014, p. 44.

[194] Pierre-Yves Hénin, « L'offensive russe en Ukraine, une guerre pour une sphère d'influence », *Revue internationale et stratégique*, 2022/2, N° 126, pp. 17-27.

[195] Pierre-Antoine Delhommais, « La guerre meurtrière du blé », *Le Point*, 17 mars, 2022, p. 14.

[196] Ali Laïdi, « L'intelligence économique russe sous Poutine », *Études internationales*, N° 40(4), 2009, pp. 631-646.

[197] Bernard Carayon, « Les définitions de l'intelligence économique », 2013, *Portail de l'IE*. Consulté le 31 mai 2022 sur http://www.portail-ie.fr/article/572/Les-definitions-de-l-intelligence-economique

[198] Ridha Loukil, « L'Usine nouvelle » publié le 11 juillet 2013. Consulté le 28 mai 2022 sur http://www.usinenouvelle.com/article/les-etats-unis-super-espions-de-lindustrie.N201146

[199] Bruno Godard, « Espionnage industriel, les affaires qui ont fait trembler l'économie », *Capital*, 2015. Consulté le 31 mai 2022 sur https://www.capital.fr/economie-politique/espionnageindustriel-les-affaires-qui-ont-fait-trembler-l-economie-1074640

européens, Angela Merkel et Nicolas Sarkozy, avaient été placés sur écoute. Les médias sociaux, qui ont pris une forte ampleur depuis 2008, ont, quant à eux, rendu en partie obsolète le modèle du média d'influence hérité de la guerre froide. Les médias traditionnels, qui font désormais face à la concurrence, sont mis à mal par l'émergence du numérique et des médias sociaux, d'où Wadah Khanfar, ancien journaliste de la chaîne arabe *Al-Jazira*, affirmait, lors d'une conférence donnée à Sydney en novembre 2012, que les « réseaux sociaux ramènent la profession sur terre. *Al-Jazira*, comme les autres doit (pour gagner les cœurs et les esprits au XXIe siècle), se réformer[200] ». Cette mise en garde a conduit les Américains à créer de nouvelles techniques d'information et de communication, à savoir les réseaux sociaux *Twitter*, *Facebook*, *WhatsApp* et *Instragram*, majoritairement utilisés par les populations africaines. Ces réseaux sociaux suivent une logique horizontale, où les émetteurs sont les récepteurs, tandis que les médias d'influence fonctionnent, par définition, selon un schéma vertical, où un émetteur tente de convaincre des populations, à l'extérieur ou à l'intérieur des frontières.

Les pays d'Afrique se caractérisent, quant à eux, par une absence de culture du renseignement[201] qui leur permet laborieusement de s'arrimer aux jeux et aux enjeux de puissance[202]. Ils se contentent d'un achat sur étagère[203] desdits instruments de renseignement pour répondre au retard et à l'inadaptation accusés dans le domaine correspondant. Dans une « guerre technologique » en cours en cette deuxième décennie du XXIe siècle, la dépendance de l'Afrique aux médias sociaux, et au renseignement américain, est une vulnérabilité pour une volonté africaine d'autonomie stratégique[204]. Ces « entrepôts de données » informatiques, devenus indispensables à tous les échanges au travers du *cloud* qui est aux mains de sociétés américaines (*Amazon* en tête, mais aussi *Microsoft* et *Google*), signifie que ces dernières stockent toutes les données stratégiques acquises sur le *cloud* américain. Les Américains disposent donc subtilement des renseignements stratégiques des pays d'Afrique (secrets industriels, militaires, espionnage, logistiques sanitaires et numériques, études de brevets, etc.) au profit de l'État étatsunien pouvant les utiliser lorsqu'une nécessité stratégique se présente, tout en réduisant les capacités/expertises intellectuelles, cognitives, réflexives, stratégiques et opérationnelles

[200] Philippe Thureau-Dangin, « Les médias d'influence sur le déclin », *Revue internationale et stratégique*, N° 89, 2013, pp. 123-129.

[201] Michel Masson, « L'avenir du renseignement », *Géoéconomie*, N° 51, 2009.

[202] Sévérin Tchetchoua Tchokonté, « La diplomatie des matières premières de l'Inde et du Brésil en Afrique », *Dialectiques des intelligences*, N° 003, 2017, p. 74.

[203] François Xavier Noah Edzimbi, « Le déficit de l'Union Africaine dans le domaine du renseignement comme frein à son projet de renaissance à l'horizon 2063 », *Dialectique des intelligences*, N° 004, 2017.

[204] Le site Internet *Wikileaks* a publié, dès 2010, 250 000 télégrammes diplomatiques américains. Ils dévoilent certains usages secrets de représentants étatsuniens en Afrique. L'une des plus révélatrice est l'instruction donnée aux agents de la *Directive National Humint Collection* (*Humint* pour *Human Intelligence*, renseignement humain), présents en Afrique, de recueillir toutes les informations possibles sur les « personnes liées à l'Afrique des Grands Lacs. […] Numéros de téléphone, de portable […], répertoires de téléphones [sur CD-Rom ou format électronique si possible] et de comptes email […] numéros de cartes de crédit, numéros de cartes de fidélité des compagnies aériennes, agendas de travail, et autres informations biographiques utiles ». Entre autres, la divulgation de pratiques de surveillance de masse de la *NSA* a été permise par Edward Snowden, informaticien consultant de la *National Security Agency* (*NSA*), ancien employé de la *Central Intelligence Agency* (*CIA*). Deux documents top-secret de la *NSA*, transmis aux quotidiens *Guardian* et au *Washington Post*, révèlent en premier que la plupart des communications mondiales transitent par les États-Unis, et mettent ensuite à jour le programme *PRISM* qui permet à la *NSA* d'accéder aux communications d'internautes étrangers se situant hors des États-Unis par le biais de différentes entreprises américaines d'Internet ou d'informatique, telles que *Microsoft*, *Apple*, *Google*, *Yahoo !*, *Facebook* ou *Skype*. Les États-Unis sont ainsi dotés d'un programme d'espionnage généralisé sur le monde entier par le biais du téléphone, d'Internet et réseaux sociaux.

d'institutions nationales[205] et privées d'Afrique. L'avantage des États-Unis est qu'ils peuvent prendre possession de ces « datas stratégiques » en raison d'une loi extraterritoriale, le *Cloud Act*, que Washington a adopté en 2018[206]. Ce dispositif législatif oblige toutes les entreprises américaines du *cloud* à transmettre à leurs autorités l'intégralité de leurs données, même si elles sont conservées sur des serveurs basés en Afrique. Aussi, les nouveaux moyens de communication ont-ils rapproché les milieux/groupes d'Afrique aux États-Unis par une représentation « globalisée et démocratique » du monde, portant critique à la perception dite « autocratique » de celle des autorités étatiques du continent. Cette puissance technologique constitue un important atout américain dans une quête de puissance décisive[207]. Ces instruments technologiques, indispensables à la fonction de renseignement, permettent ainsi aux Américains, premièrement, d'anticiper les intentions d'adversaires potentiels et de mettre en évidence des indices d'alerte dans une guerre économique en cours. Ils contribuent à dégager des modes d'action les plus probables, participent à la veille stratégique et conservent un avantage dans les processus de négociations avec des partenaires d'Afrique, au détriment de ces derniers. Enfin, ils préservent la place d'hégémon des États-Unis dans la conception, la structuration, la mise en œuvre et l'exécution des normes juridiques internationales et d'accords économiques.

Les puissances économique et technologique représentant un terreau d'affirmation de l'hégémonie mondiale pour les États-Unis, l'Afrique voit grandir l'écart entre elle et d'autres acteurs de la scène internationale dans le processus d'intégration dans la mondialisation. Entre autres, cette situation s'accentue lorsqu'on s'intéresse à la détermination française à disposer d'une forte influence dans ses anciennes colonies et territoires sous tutelle de l'ère coloniale. En effet, les Français s'interrogent sur la place qu'occupe leur pays sur la scène internationale. Si l'on s'en tient à des données chiffrées, tout en se référant à certains critères de puissance (la capacité militaire, l'assise territoriale, la géographie, les ressources naturelles, les poids économique, culturel et diplomatique, etc.), le poids de la France dans le monde diminue. Les Français représentent aujourd'hui moins de 1 % de la population mondiale, le territoire national moins de 0,5 % des terres émergées. Le produit intérieur brut (PIB) de la France classe celle-ci au 6e ou 7e rang mondial selon les années, mais avec un poids dans les équilibres mondiaux qui s'amenuise. Le PIB chinois est passé, quant à lui, de 1,6 % du PIB mondial dans les années 1990 à 16 % aujourd'hui, tandis que le PIB français passait de 5,6 % à 3 %. La part de la France dans le commerce mondial a chuté d'environ 6 % en 1995 à 3 % aujourd'hui. Toutefois, les réformes faites sous les chefs d'État François Hollande et Emmanuel Macron ont eu un effet, en termes de compétitivité, d'attractivité de l'économie nationale ou encore d'innovation et, plus récemment, de création d'emplois. Entre autres, lorsqu'on s'intéresse à d'autres critères, la France reste parmi les dix puissances militaires mondiales, mesurées par le niveau des dépenses de défense. Aussi continue-t-elle de bénéficier du statut de membre permanent du Conseil de sécurité des Nations unies et de puissance dotée de l'arme nucléaire. Sur les plans économique, militaire, politique et finalement sur le terrain de l'influence, le rapport des forces s'est progressivement déplacé au détriment de la France en Afrique. Celle-ci doit compter avec les puissances émergentes sur le plan économique (Inde, Brésil, Indonésie, Afrique du Sud, etc.) et avec des puissances ré-émergentes sur le plan géopolitique (Russie, Turquie, Iran, etc.). Partant de ces réalités, durant deux heures de temps le 2 septembre 2022 et

[205] Fabien Geledan, « Les cabinets de conseil au cœur de la RGPP », N. Matyjasik et Guenoun (dir.), *En finir avec le New Public Management*, Institut de la gestion publique et du développement économique, 2019.

[206] Cour des comptes, « Le recours aux marchés publics de consultants par les établissements publics de santé », 2018. Consulté le 91 mai 2022 sur https://www.ccomptes.fr/system/files/2018-09/20180709-refere-G6418-0152E-recours-marches-publics-consultants-par-EPS.pdf

[207] Philippe Moreau Defarges, *Introduction à la géopolitique*, Paris, Éditions Seuil, 2009.

devant les ambassadeurs français réunis à l'Élysée, le président Emmanuel Macron analysa l'émergence d'un nouveau monde et ses conséquences pour la France et pour l'Europe. D'après le chef d'État, le « retour de la guerre sur le sol européen », le « désordre climatique », certaines ressources jusque-là jugées acquises, comme l'énergie et l'alimentation, « redeviennent des sujets géopolitiques », expressions d'une « fracture de l'ordre économique mondial[208] ». De ce constat, la France doit bâtir une « indépendance géopolitique » par rapport au « duopole » sino-américain. « Nous n'avons pas à être sommés de choisir, nous devons partout pouvoir garder cette liberté d'action », car la France doit être une « puissance d'équilibres ». Étant consciente de disposer de moyens limités dans la guerre économique tant entre alliés que rivaux stratégiques, la France a donc intérêt, selon Emmanuel Macron, à « bâtir de plus en plus de partenariats équilibrés bilatéraux ou régionaux », d'où les tournées diplomatiques entreprises en Afrique en 2022, continent qui regorge d'importants gisements de matières premières estimés à 30 % des réserves mondiales, et disposant de 60 % de terres arables, d'écosystèmes favorables et d'une main d'œuvre jeune[209].

L'Afrique dans son ensemble représente 5,3 % du commerce extérieur français, et les échanges avec les pays de la zone franc, qui se sont fortement détériorés, s'établissent aujourd'hui à un niveau de 0,6 %. La Chine est désormais le premier partenaire commercial de la plupart des anciennes colonies françaises et territoires sous tutelle à l'exception du Tchad, du Niger, du Sénégal et de la Tunisie. La part de marché relative de la France sur le continent est passée de 15 % à 7,5 % entre 2000 et 2020[210]. Avec une industrie en déclin, elle ne peut pas satisfaire les besoins des pays africains en biens d'équipement quand la Chine peut, elle, y répondre. Depuis 2018, l'Allemagne est le premier fournisseur européen de l'Afrique et, en juin 2022 lors d'un sommet à Kigali au Rwanda, le Togo et le Gabon ont adhéré au *Commonwealth*, jugé commercialement plus dynamique que la zone francophone[211]. Aujourd'hui, les entreprises françaises représentent à peine 10 % de l'économie camerounaise alors qu'elles couvraient 40 % de son économie voilà une trentaine d'années. L'objectif d'Emmanuel Macron était donc, en visite au Cameroun du 25 au 26 juillet 2022, de « marquer la continuité et la constance de l'engagement de la France dans la démarche de renouvellement de la relation avec le continent africain[212] », et modifier une situation non-bénéfique aux intérêts français dans ledit pays. L'Afrique est en effet un tremplin économique pour la France dans le commerce mondial, avec 1 100 groupes et 2 109 filiales d'entreprises françaises présentent sur le continent, et stock d'investissements qui se positionne à la troisième place après le Royaume-Uni et les États-Unis[213]. Le continent renforce sa sécurité économique au moyen d'un patriotisme économique qui préserve des emplois et le savoir-faire français. Ainsi, dans un contexte de déséquilibre d'approvisionnement et de raréfaction de sources énergétiques provoqués par la guerre d'Ukraine, l'Algérie se présente, entre autres pour la France, comme un « roi du gaz naturel[214] », avec des réserves évaluées à 2 400 milliards de m^3. Accompagné d'une délégation constituée d'autorités

[208] Isabelle Lasserre, « Emmanuel Macron dresse un sombre état du monde », *Le Figaro*, 30 août 2022, p. 6.

[209] Anne Cheyvlalle, « L'Afrique peut-elle devenir autosuffisante pour son alimentation ? », *Le Figaro*, 30 août 2022, p. 13.

[210] Hervé Gaymard, « Relancer la présence économique française en Afrique », *Rapport au ministre de l'Europe et des affaires étrangères et au ministre d'économie et des finances*, 2019.

[211] Peter Fabricius, « La France est-elle en train de perdre du terrain en Afrique ? » *Institute for Security Studies Africa*, 2022.

[212] Anne-Cécile Robert, « Paris aux petits soins des régimes autoritaires. M. Macron trébuche au Cameroun », *Le Monde diplomatique*, septembre 2022, p. 21.

[213] Sandrine Berthaud-Clair, « La France en Afrique, un partenaire d'affaires de moins en moins particulier », *Le Monde Afrique*, 6 février 2020. Consulté le 20 octobre 2022 sur https://www.lemonde.fr/afrique/article/2020/02/06/la-france-en-afrique-un-partenaire-d-affaire-de-moins-en-moins-particulier_6028642_3212.html

[214] Cyrille Louis, « À Alger, Emmanuel Macron tente de renouer avec « un pays essentiel », *Le Figaro*, 26 août 2022, p. 7.

gouvernementales et militaires, le chef d'État français a souligné durant son séjour à Alger du 25 au 28 août 2022 que l'Algérie est, pour la France, « un pays essentiel par le passé commun, le présent partagé et les défis futurs ». Il a rappelé que « l'Algérie est un fournisseur de gaz pour la France » à hauteur de 8 %. Dès lors, consciente de l'importance stratégique que revêtent les partenaires africains pour son rayonnement international, la France n'est pas disposée à tolérer les empiétements d'autres puissances porteuses de projets de domination, susceptibles de contrebalancer son influence, mieux de contester les monopoles traditionnels de ses entreprises sur le continent[215]. De fait, face à ces nombreuses incursions géoéconomiques et géopolitiques de la Chine, de la Russie ou encore des États-Unis dans sa « sphère d'influence naturelle », la France s'efforce d'y préserver ses intérêts.

L'opinion publique africaine ne pouvant utiliser l'arme des fausses informations pour des raisons éthiques et de cohérence interne, la première réaction face aux projets géostratégiques des puissances mondiales et émergentes en Afrique consiste, majoritairement, à écarter les solutions offensives et à se cantonner à une défense introvertie, orientée et, ensuite, solliciter une aide/assistance extérieure. La veille et la pédagogie des contenus sur le microthéâtre des réseaux sociaux ne permettent d'agir qu'en réaction, c'est-à-dire tardivement. Les Africains entérinant leur perte d'initiative, ils se présentent comme vaincus d'avance dans les rapports établis avec d'autres acteurs, tandis que la GMS et les guerres d'influence se situent sur un tout autre plan. Les *fake news* n'en sont en effet qu'un simple vecteur dont l'efficacité ne doit pas être surestimée, car les menaces plus importantes sont furtives et structurelles. Elles ne visent pas les émotions du moment, mais les structures mentales, les grilles d'analyse, les biais culturels, les matrices psychologiques. Ainsi la réponse africaine aux guerres contemporaines ne doit être « ni politique ni militaire : elle doit être totale ![216] ». Aujourd'hui, on peut vaincre sans tuer. La GMS a pour but la dislocation de l'adversaire afin de briser sa volonté sans même se découvrir. C'est ce que le général Burkhard appelle « gagner la guerre avant la guerre ». Il est désormais nécessaire pour les Africains de se dégager du schéma classique ami-ennemi au profit d'un ciblage en termes d'influence. Il peut être plus utile d'influencer un allié qu'un adversaire. Dans un cadre de compétition globale, l'avenir appartient aux nations qui sont capables de diffuser leur modèle, d'où l'urgence pour l'Afrique de s'arrimer à cette donne. Il ne s'agit pas de diriger les actions de la cible, ce serait de la manipulation, pouvant être moralement remise en cause en cas de découverte. En revanche, l'objectif est de modéliser insensiblement et irrémédiablement ses modes de pensée. Tel est le domaine de l'ingénierie cognitive, le pivot du combat immatériel. Elle s'inscrit dans la durée et doit être conduite sur le mode de l'anticipation et non de la réaction[217]. Plutôt que de chercher vainement à « réparer » une structure sociale défaillante, il est essentiel d'en percevoir les déséquilibres en amont et d'agir si possible. La GMS conduit inéluctablement à l'ingénierie cognitive, qui ne peut être qu'offensive. Elle est une menace entre les mains des adversaires, mais plus encore, elle constitue un important outil pour diffuser les valeurs

[215] Dans une telle configuration, la riposte stratégique de la France aux incursions de la Russie en République Centrafricaine constitue un important indicateur de sa détermination à garder sa « mainmise », en dépit de la concurrence. La contre-offensive de la France aux assauts de la Russie dans ce pays s'observe par la mise à contribution de l'ensemble de son dispositif de puissance. Face à nouvelle idylle entre Moscou et Bangui, les réactions de la France ont été quasi-immédiates et épousent aussi bien les contours militaires et budgétaires. La France a en effet décidé de suspendre son aide militaire et financière aux nouvelles autorités centrafricaines, complices d'une campagne antifrançaise initiée par la Russie. L'arrestation en juin 2021 du français Juan Remy Quignolot à Bangui, accusé d' « espionnage, de complot et d'atteinte à la sureté de l'État », a fortement contribué à la dégradation des relations entre Paris et Bangui. C'est dans environnement que Paris a décidé de rompre sa coopération militaire avec Bangui.

[216] Colonel Jean Nemo, « La guerre dans le milieu social », *Revue Défense Nationale*, N° 136, mai 1956, p. 622.

[217] Raphaël Chauvancy, *op. cit.*

africaines dans un monde dont la première superpuissance serait, peut-être demain, la Chine.

LA COMMUNICATION COMME UN OUTIL EFFICACE POUR LE RENSEIGNEMENT DANS LA LUTTE CONTRE LA VIOLENCE HYBRIDE : LE CAS DU CAMEROUN

Berthe Mélika OBAMA MEWALI
Division de la communication du ministère de la Défense du Cameroun

Le renseignement fait face à une nouvelle réalité depuis la fin de la guerre froide, celle de l'émergence de nouveaux acteurs réapprovisionnés par de nouvelles techniques de combat basées sur la terreur et la recherche du gain. Cette nouvelle dimension de la menace asymétrique, appelée violence hybride, brouille toutes les pistes d'accès à la collecte, la diffusion et la réception d'une information pertinente en temps de crise grâce à l'apparition du numérique. Pendant que le renseignement utilise les drones et les satellites pour une opération militaire, les médias et les réseaux sociaux s'accaparent de l'information pour la transformer. De ce fait, les technologies de l'information et de la communication ne cessent de gagner du terrain dans la mise en récit des informations en temps de crise et la perception de la crise. L'enjeu de l'information devient donc primordial dans la construction du renseignement en temps de crise ou de conflit. À cet effet, la question de la fiabilité de l'information dans la lutte contre la violence hybride au Cameroun, par exemple, interroge sur la place de la communication dans la construction du renseignement. Comment la communication peut-elle permettre au renseignement d'accéder à une information pertinente et fiable pour lutter contre la violence hybride ? Par quelles voies les individus ont-ils accès aux informations et comment la perçoivent-ils ?

La dimension communicationnelle du renseignement

La nature du renseignement amène souvent les différents acteurs à travailler sur des stratégies d'influence impliquant des actions d'intoxication, de désinformation et de manipulation des individus stratégiques, tant en période de paix qu'en période de crise. Cette stratégie comporte une multitude de tâches notamment des actions psychologiques qui visent des populations particulièrement étrangères, des actions civilo-militaires avec comme cible la population sur le théâtre, la communication opérationnelle qui permet de mobiliser son opinion publique personnelle et celle des alliés dans un éventuel cas. Il existe également des manœuvres de diffusion de rumeurs pour perturber les services de renseignement adverses, des opérations de désinformation auprès de contacts aux positions et aux rôles clés. Le Centre interarmées de concepts, de doctrine et d'expérimentations (CICDE) explique que : « *influencer les acteurs du « champ de bataille » vise à faire évoluer leurs représentations, leurs perceptions et leurs comportements. Informer les opinions publiques doit les inciter à soutenir les soldats en opérations et contrecarrer les effets de propagande adverse. Combattre, affaiblir les idées des opposants et influence le processus décisionnel adverse participent à l'atteinte des objectifs politiques et à la protection de notre propre processus décisionnel* »[218].

Cependant, les terroristes et les criminels livrent une guerre psychologique en commettant des attentats dans le but de provoquer des changements par la force. À cet effet, leur méthode d'influence passe par la diffusion des messages qui expliquent et justifient leurs actions. Boko Haram dans la région de l'Extrême-Nord du Cameroun s'est souvent servi de divers moyens de communication pour asseoir son influence auprès de la population. Cette nébuleuse a choisi de prêcher dans la langue haoussa qu'elle enregistrait sur des cassettes, des CD, des clés USB et distribuait au sein de la population. Elle allait plus loin en produisant des fils montrant des entraînements, des combats ou des exécutions.

[218] Centre Interarmées de Concepts, de Doctrines et d'Expérimentations (CICDE), L'influence en appui aux engagements opérationnels, Réflexion doctrinale interarmées RDIA-2012/008_INFLUENCE (2012), N°073 DEF/CICDE/NP du 31 mars 2012, p.12.

L'objectif est de montrer à la population ciblée qu'elle a en face d'elle des hommes forts et déterminés, voire des guerriers invincibles. L'information pour laquelle les différents acteurs dans une crise ou un conflit s'affrontent, Boko Haram l'utilisait à des fins de déstabilisation du Cameroun et pour saper le moral de l'armée camerounaise. Le moyen le plus accessible pour parvenir à leurs fins est Internet, où le groupe terroriste diffusait des vidéos notamment celle de l'enlèvement des lycéennes de Chibok, en 2014. La finalité de leurs actions est de radicaliser une grande partie de la population pour qu'elle rejoigne les rangs de leur groupe.

Par ailleurs, la Division de la Communication produit deux fois par an un numéro spécial de son traditionnel magazine « Honneur & Fidélité », qui paraît en mai et en décembre, et valorise le concept Armée-Nation. Le journal, produit en près de 10 000 exemplaires, s'adresse en particulier aux autorités civiles et militaires, attachés de défense des pays amis, ambassades accréditées au Cameroun, institutions internationales, représentations diplomatiques du Cameroun à l'étranger, services de communications des organes publics et parapublics, académies militaires à vocations nationale, régionale et internationale, ainsi que des universités et centres de recherche. Dans le même sillage, la Division de la Communication produit également des calendriers avec des images représentant les valeurs des forces de défense camerounaises.

En sus, le ministère de la Défense dispose d'un magazine radiophonique « Honneur & Fidélité », qui sensibilise et informe sur les activités des forces de défense camerounaises. C'est l'émission phare de la Division de la Communication, diffusée chaque samedi de 14 heures à 15 heures, sur la fréquence 88.8 du poste national de la Cameroon Radio Television (CRTV). L'objectif majeur de la Division de la Communication à travers cette émission hebdomadaire, est de promouvoir le lien Armée-Nation, tout en informant la population sur toute l'étendue du territoire au sujet des questions de défense et de sécurité. Elle a également pour objectif de promouvoir l'image du ministère de la Défense.

Christian Harbulot précise que : « *la société de l'information est une nouvelle aire conflictuelle qui génère ses propres formes d'affrontement. L'enjeu n'est plus la manière de tromper la perception du concurrent, des parties prenantes (stakeholders) ou de l'opinion publique, mais la capacité de produire plus de connaissances pertinentes qui fragilisent la position de l'adversaire* »[219].

En outre, la mission première de l'armée camerounaise est d'assurer en tout temps et en tout lieu, en toutes circonstances et contre toutes les formes d'agressions la sécurité et l'intégrité du territoire national, ainsi que la vie des populations. Il est encore plus vrai que l'exclusivité de la défense du territoire national et de la sécurité des populations ne sauraient revenir aux seuls forces de défense, mais elle est une affaire de tous, surtout dans ce contexte de nouvelles menaces pour le Cameroun. Aujourd'hui plus qu'hier, l'institution militaire est un acteur privilégié dans la réponse à la problématique de défense de la souveraineté et de l'intégrité territoriale du Cameroun de la promotion de la sécurité des femmes et des hommes à travers le pays et le monde. Ainsi, plus qu'une simple option stratégique, cette vision s'impose à la Nation, à un moment où des conflits atypiques liés au terrorisme et à l'extrémisme, à l'expansion de la criminalité organisée et transfrontalière se multiplient et compromettent dangereusement la quiétude des citoyens et la sécurisation du développement économique.

La connaissance de l'Autre est essentielle dans la stratégie d'influence. Cet exercice relève du renseignement opérationnel, qui est relatif à la conduite des opérations militaires. Cela demande ainsi de connaître les intentions de l'ennemi relevant bien souvent par les positions de l'adversaire et l'étude de ses forces. Pour Serge Caplain, « *qui étudie l'ennemi doit tenter de lire l'avenir. Que ce soit au niveau politique ou militaire, l'identification et la compréhension de la menace ne commencent pas à la déclaration des hostilités mais doivent être anticipées autant que possible* »[220]. Des groupes terroristes Boko Haram dans la Région de l'Extrême-Nord aux terroristes-sécessionnistes dans les régions du Nord-Ouest et du Sud-Ouest, voilà

[219] Alain JUILLET, Bruno RACOUCHOT, « L'influence, le noble art de l'intelligence économique », Communication et organisation [en ligne] 42-2012, mis en ligne le 1er décembre 2014, p.164.

[220] Serge CAPLAIN, « Penser son ennemi. Modélisation de l'adversaire dans les forces armées », Focus Stratégique, n°82, Ifri, juillet 2018, p.15.

l'exemple type actuel de l'ennemi hybride qui agit dans les champs matériels et immatériels. La principale caractéristique de l'ennemi hybride est de se fondre dans la population pour contrôler un espace immense, être organisé en réseaux, avoir recours à des capacités bon marché afin de contourner l'avance technologique et utiliser les nouvelles technologies de l'information et de la communication (NTIC) pour sa propagande.

De ce fait, pour obtenir des informations sur l'ennemi, il convient de miser sur le facteur humain, c'est-à-dire la population, car selon Carl Von Clausewitz : « *ce sont des renseignements que l'on peut se procurer sur l'ennemi et sur son pays qui servent de base à toutes les idées et à toutes les actions à la guerre* »[221]. C'est un facteur important, car il permet de savoir ce que pense la population locale sur l'armée, comment elle perçoit ses adversaires, de connaître ce que peuvent faire les décideurs à tous les niveaux pour avoir l'appui de la population. Ceci parce que l'armée, malgré ses bonnes intentions, ne peut pas imposer ses valeurs et ses institutions à une population qui ne les connaît pas ou qui n'a aucune idée de la façon de les développer.

Les problématiques liées à la dimension communicationnelle du renseignement

La quasi-totalité des auteurs des attentats et des exactions dans les régions de l'Extrême-Nord, du Nord-Ouest et du Sud-Ouest ont un passé de délinquant de droit commun. Les terroristes-sécessionnistes dans les régions du Nord-Ouest et du Sud-Ouest sont des promoteurs de la guérilla et se battent au nom d'un État chimérique et utopique appelé « *Ambazonie* ». Pour eux, il est question de couper les deux régions anglophones du Cameroun et d'en faire un État indépendant. Ces auteurs ne sont pas des étudiants, des enseignants voire des avocats déclassés et haineux, mais des voyous habitués des commissariats et des prisons pour des vols, du trafic de stupéfiants ou autres délits sur la voie publique. Dans la région de l'Extrême-Nord, le groupe terroriste Boko Haram participe au banditisme local à des fins logistiques à travers le vol de bétail et le pillage dans le but de faire croire à une criminalité djihadiste. Ce groupe va jusqu'à entretenir des relations avec des groupes criminels locaux entraînant des acteurs locaux dans leur projet. Ces groupes criminels contribuent à l'ancrage de la secte terroriste dans la région. Pour Moussa Bobbo, « *les interactions entre Boko Haram et les milieux criminels locaux brouillent d'autant plus la frontière entre le crime organisé et le djihadisme que certains groupes de bandits ruraux autonomes opèrent dans les villages frontaliers et sont donc assimilés aux miliciens de Boko Haram alors qu'ils n'ont aucun rapport avec le mouvement djihadiste* »[222]. Le plus impressionnant avec ces groupes est le caractère hybride du combattant islamiste et séparatiste et surtout sa détermination jusque-boutiste. La dangerosité de l'ennemi hybride est liée à sa plasticité. Les djihadistes de la secte islamiste Boko Haram et les séparatistes n'ont pas de profil type, aisément identifiable, ce qui rend l'ennemi hybride protéiforme et insaisissable. Leurs modes d'actions sont variés. Ils vont des cyberattaques aux attentats suicides en passant par les engins explosifs. Ces capacités sont d'autant plus dangereuses qu'elles sont peu coûteuses, très accessibles, et qu'elles se combinent facilement à l'idéal de mort et au fanatisme des djihadistes, ainsi qu'à la terreur des séparatistes.

Cependant, les médias à caractère dominant tant sur le plan national qu'international, donnent une image de la crise sociopolitique dans les régions du Nord-Ouest et du Sud-Ouest, comme celle du fracas des armes lors des bombardements plus ou moins massifs, ou celle des batailles épiques avec d'énormes pertes d'un côté ou l'autre. Ce qu'il faudrait savoir, c'est qu'en arrière-plan de ce flot d'informations soigneusement calibrées, se profile le dessein d'impressionner l'opinion, de la désolidariser des adversaires déclarés ou potentiels, et si possible, de paralyser les moyens de défense adverses. Lassané Yaméogo souligne que : « *le recours simultané à la rhétorique de « guerre » aboutit à une exceptionnalisation du terrorisme, à sa surestimation, mais aussi à sa représentation comme une donnée permanente* »[223].

L'adaptation du renseignement à la société de l'information

La communication institutionnelle est l'une des plus appropriées pour le renseignement comme l'explique

[221] Carl Von Clausewitz, De la guerre, Paris, Editions Ivrea, 2000, p.91.

[222] Moussa BOBBO, Boko Haram dans la région de l'extrême-nord du Cameroun : l'arbre qui cache la forêt, Notes de l'Ifri, Ifri, juin 2022, p.19.

[223] Lassané YAMEOGO, « Les médias, un allié du terrorisme ? », *in* Les Cahiers du Journalisme, Médias et Terrorisme, seconde série, n°1, 1er trimestre 2018, Ottawa, Presses de l'Université d'Ottawa, pp.9-10.

Arnaud Lelièvre : « *il est utile de préciser que la communication des services de renseignement sur le web est principalement une « communication institutionnelle » (parfois aussi appelée « communication corporate »), dans le sens où se sont les services de renseignements qui prennent la parole pour communiquer à propos de leur identité et d'améliorer leur image. C'est donc une communication qui vise essentiellement le grand public, c'est- à- dire les citoyens* »[224]. De ce fait, la communication institutionnelle peut donc jouer un rôle socialisateur dans le sens où la mise en place des actions de communication (conférences de presse, colloques, pages web, etc.) aide le renseignement à s'intégrer dans la société et ainsi à devenir un acteur social à part entière. De cette manière, grâce à la communication institutionnelle, le renseignement n'est plus une institution totalement fermée, mais ouverte à la société sans toutefois mettre de côté son sacro-saint principe qui est le secret. L'instauration de la communication institutionnelle comme un outil stratégique contribue à la socialisation du renseignement de cinq manières différentes : adaptation aux changements du contexte, développement de la réputation, gestion de certains problèmes avec la population, diffusion des connaissances scientifiques et promotion de l'éducation de la population dans les habitudes de renseignement.

Les citoyens s'intéressent de plus en plus à l'Internet comme une source d'information du renseignement, même si l'utilisation qu'ils en font dépend de plusieurs facteurs comme par exemple l'âge, le sujet traité ou encore le niveau de formation et de compréhension de l'information du renseignement. Dans les prochaines années, l'Internet pourrait contribuer à réduire les incompréhensions en ce qui concerne la gestion de l'information. L'importance de l'Internet comme un outil d'éducation de la population peut mener le renseignement à développer des pages Web, y compris certains outils du Web 2.0. Ainsi, le Web 2.0 met en valeur les contenus générés par les utilisateurs, la production collective de connaissances et le partage d'expériences personnelles. Même si la communication institutionnelle constitue un métier qui n'est pas très développé dans le milieu du renseignement, les outils du Web 2.0 peuvent aider le renseignement à mettre en place des stratégies de communication plus efficaces et plus créatives. Ainsi, le renseignement va céder son pouvoir aux agents de renseignement, lesquels grâce aux applications du Web 2.0, deviennent les vrais protagonistes de la communication institutionnelle du renseignement.

Toutefois, la communication publique se présente comme un outil de gestion de crise, car dans la maîtrise des conséquences d'un attentat, la communication publique est vue comme un espace à part entière dans la lutte contre la violence hybride, « *car elle agit sur l'opinion publique et est donc peu ciblée. L'opinion publique est la base des sociétés démocratiques et de fonde sur la souveraineté du peuple et sa liberté d'expression, tout en renvoyant à la somme des jugements des citoyens relative à la vie publique* »[225], souligne Arnaud Lelièvre.

En temps de crise, il est généralement reproché aux services de renseignement de ne pas assez communiquer, ou de ne pas être assez précis, donc de mal communiquer. Il paraît intéressant de mettre en place une politique de communication publique du renseignement axée sur l'éthique du renseignement qui lui permettra « *de se faire connaître (identification) et reconnaître (légitimation)* »[226], souligne Arnaud Lelièvre. L'éthique du renseignement basé sur le secret doit être l'un des piliers de cette communication reconnue par la population, les médias et le politique, car elle participe de la protection des personnes et des biens, ainsi que la sécurisation du territoire national. « *C'est précisément dans ce cadre que les politiques de communication doivent se concevoir. Elles permettent de faire connaître au public le cadre légal des activités des services de renseignement, les méthodes employées, les missions accomplies qui peuvent être divulguées, les valeurs revendiquées des organismes, etc. La réflexion éthique permet donc de justifier le rôle des organes de renseignement en tant qu'organismes d'intérêt public, mais aussi de réguler les activités en fonction de normes partagées par la société au sein de laquelle ils sont amenés à fonctionner* »[227], explique Arnaud Lelièvre.

Face à l'attachement populaire à l'armée et sa primauté dans la lutte contre le terrorisme et la criminalité, il est important de faire usage de la communication publique, afin d'intégrer la population

[224] Arnaud LELIÈVRE, La communication web des services de renseignement. Etude sémio-pragmatique, Thèse en Information et communication, Université catholique de Louvain, Février 2018, p.32.
[225] *Ibid*. p.112.
[226] *Ibid*. p.113.
[227] *Ibid*. p.101.

à la mobilisation étatique et de déployer une stratégie de communication, capable de concurrencer celle de groupes criminalo-terroristes. L'objectif visé est de permettre à la population d'être un acteur lucide et sensibilisé, en évitant qu'elle soit une masse de manœuvre au mieux passive et au pire verbale de l'action terroriste, le risque pouvant naître tant du sentiment d'abandon par les pouvoirs publics que du reste d'associer l'opinion à l'action contre la violence.

La communication doit permettre de réduire l'impact potentiel d'une attaque et de prévenir la perte de confiance et de l'image pour les autorités publiques. Cette stratégie de communication doit être axée sur les réseaux sociaux, car ils constituent un outil stratégique de la communication institutionnelle, autrement dit, un outil capable de satisfaire aux besoins communicationnels du renseignement.

Institut
EGA

JE M'ABONNE EN CLIQUANT ICI

www.institut-ega.org