LES NOTES DU CREOGN

Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale

Numéro 91 – Septembre 2023

Capitaine Pascal MARTIN (Dr)

©Gorodenkoff via Adobe Stock

Priorité stratégique de la prospective

Gendarmerie et territoires

Le CREOGN certifie que ce document a été rédigé par un humain

LE RENSEIGNEMENT HUMAIN À L'HEURE DES NOUVELLES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION (NTIC)

Le renseignement technique est désormais irremplaçable au sein des services de renseignement. L'ensemble des capteurs qu'il recouvre semble être une réponse à de nombreuses contraintes opérationnelles et constitue l'une des priorités des administrations les plus sensibles de l'État. Cette tendance à la « technologisation » des services ne cesse d'ailleurs de se renforcer depuis le début du XXIe siècle, et ce, malgré les importants moyens budgétaires qu'elle nécessite. Ce constat s'est plus particulièrement imposé aux États-Unis où les révélations d'Edward Snowden en 2013 ont permis de démontrer, outre l'ampleur du système de surveillance, l'importance prise par les technologies dans les services de renseignement, notamment en matière de collecte et d'analyse des données[1].

Cependant, cette prépondérance des capteurs techniques ne peut occulter l'importance du renseignement d'origine humaine (ROHUM ou HUMINT[2]), dont l'intérêt a été souligné dès 2008 par le *Livre blanc de défense et de sécurité nationale* : « *Une attention spéciale sera apportée, dans l'effort global, au renseignement de source humaine. Cela implique une amélioration du recrutement et de la formation des personnels chargés de cette mission, une augmentation du nombre de sources et une amélioration de leur répartition géographique en fonction de nos centres d'intérêt prioritaires* »[3].

Les sources humaines constituent une plus-value capacitaire certaine et indispensable, car elles permettent de collecter de l'information protégée, qui n'est pas accessible en sources ouvertes, et peuvent également faciliter la contextualisation d'une information.

Cette Note s'attache à présenter l'usage du renseignement humain au sein des services et les perspectives induites par l'évolution technologique. Le texte ne traite pas des règles et normes qui conditionnent et réglementent l'action des services de renseignement.

I) La complémentarité des capteurs : un consensus au sein des services

La notion de complémentarité des capteurs fait l'unanimité au sein de la communauté française du renseignement, car « *c'est le croisement des sources d'origine humaine, technique et opérationnelle qui fait notre force* »[4]. En effet, ces administrations, conçues pour défendre l'État et ses intérêts, ont pour objectif d'obtenir, par tout moyen (dans le respect des lois et règlements en vigueur), l'information protégée et vitale. Dans cette perspective, toutes les capacités possibles doivent pouvoir se combiner pour parvenir à cette fin, comme l'indiquait Patrick Calvar en 2016 en sa qualité de directeur général de la Direction générale de la sécurité intérieure (DGSI) : « *J'entends par ailleurs démythifier tout ce qu'on dit en permanence sur le renseignement technique et le renseignement humain, car cette distinction ne signifie rien. Voilà*

1 LAURENT, Sébastien-Yves. *Atlas du renseignement – Géopolitique du pouvoir.* Paris : Presses de la Fondation nationale des sciences politiques, 2014, p. 184.

2 HUMINT : *Human Intelligence.*

3 *Livre blanc sur la défense et la sécurité nationale.* Odile Jacob : La Documentation française, Paris, 2008, p. 135.

4 Commission de la défense nationale et des forces armées, audition du préfet Érard Corbin de Mangoux, Directeur général de la sécurité extérieure (DGSE) au ministère de la Défense, session ordinaire 2012-2013, compte rendu n° 56, mercredi 20 février 2013, séance de 09 heures 30.

trente-neuf ans que j'exerce ce métier : il y a le renseignement et ensuite les méthodes par lesquelles on peut l'obtenir, l'essentiel étant de l'obtenir »[5]. Ainsi, l'emploi coordonné de plusieurs typologies de capteurs, à la fois distants et de proximité (ROEM[6], ROIM[7], ROHUM et cyber[8]), a permis d'acquérir des renseignements concernant l'organisation des groupes terroristes œuvrant en Libye et au Levant, et une analyse systémique de Daesh et de ses modes opératoires a pu être établie. Le croisement de ces informations a également rendu possible la réalisation de dossiers militaires de ciblage utilisés par les forces françaises ou par la coalition[9].

La complémentarité des capteurs a ainsi acquis une valeur doctrinale depuis la publication du *Livre blanc sur la défense et de la sécurité nationale* de 2013 qui reconnaît que le ROHUM, le ROEM et le ROIM « *sont complémentaires et indissociables. C'est la combinaison des informations recueillies par ces trois voies qui donne au renseignement sa valeur* »[10]. Cependant, si l'équilibre capacitaire entre renseignement d'origine humaine et renseignement d'origine technique est souvent évoqué et loué, il demeure théorique en raison du poids que représente ce dernier dans la production des services[11].

II) Le renseignement humain : un capteur essentiel

Si la qualité du renseignement d'origine humaine est plus hétérogène que celle issue d'autres capteurs, notamment techniques[12], elle présente néanmoins certains avantages. En effet, contrairement à l'information brute résultant de capteurs techniques, le ROHUM offre une plus fine appréhension des situations locales et permet d'accéder, dans des zones où l'évolution technologique est limitée, comme au Sahel, à des renseignements d'une grande importance, notamment en matière de conduite des opérations militaires[13]. En outre, une source humaine peut infiltrer des réseaux humains qui sont inaccessibles pour les capteurs techniques qui, malgré leurs performances et leur perfectionnement croissants, présentent des limites d'emploi[14]. L'être humain peut recueillir des impressions ou des rumeurs, capter un état d'esprit particulier ou des projets fomentés en privé, qu'il pourra alors contextualiser et confronter à l'observation de son environnement.

Dans ce cadre, William Burns, actuel directeur de la *Central Intelligence Agency* (CIA), souligne l'impérieuse nécessité de développer des réseaux de renseignement humain en Chine afin de capter de l'information à haute valeur ajoutée, permettant de déterminer l'intention d'un adversaire, et ce, en dépit des flux massifs d'informations recueillis par d'autres méthodes et malgré l'évolution des technologies de surveillance qui entravent le déploiement de réseaux de renseignement humain[15]. Ainsi, si les volumes d'informations collectés sont bien souvent plus réduits qu'avec le renseignement technique, les apports du ROHUM peuvent être d'une très grande valeur stratégique ou opérationnelle.
D'ailleurs, après les attentats du 11 septembre 2001, il a été établi que la CIA avait fortement réduit sa capacité à réaliser des opérations clandestines et de recueil de renseignement d'origine humaine[16]. En outre, lors du déploiement militaire en Afghanistan, ce service ne disposait, pour ce pays, que d'un seul analyste et d'une équipe réduite d'agents maîtrisant les nombreux dialectes. En conséquence, la CIA a dû initier un long travail de reconstruction des réseaux, procéder à des campagnes de recrutement et créer en urgence des formations spécifiques[17].

III) L'évolution du renseignement humain sous l'impulsion des NTIC

Le renseignement d'origine humaine (qui a notamment été employé dans les zones de conflit[18]) fait l'objet d'évolutions pour s'adapter à l'essor des NTIC, considérant qu'une part non négligeable de l'information politique et économique est désormais disponible en sources ouvertes[19] (perturbant la dichotomie classique entre sources ouvertes et fermées[20]). En conséquence, le ROHUM peut s'appuyer sur l'ensemble des données librement accessibles (réseaux sociaux notamment,

5 Commission de la défense nationale et des forces armées, audition de M. Patrick Calvar, directeur général de la sécurité intérieure, session ordinaire 2015-2016, compte rendu n° 47, mardi 10 mai 2016, séance de 17 heures 00.
6 ROEM : Renseignement d'origine électromagnétique.
7 ROIM : Renseignement d'origine image.
8 ROC : Renseignement d'origine cyber.
9 Commission d'enquête relative aux moyens mis en œuvre par l'État pour lutter contre le terrorisme depuis le 7 janvier 2015, audition, à huis clos, du général Christophe Gomart, Directeur du renseignement militaire (DRM), Mme Lorraine Tournyol du Clos, adjointe au directeur, chargée de la stratégie, et du colonel N, assistant militaire, session ordinaire 2015-2016, compte rendu n° 31, jeudi 26 mai 2016, séance de 14 heures 30.
10 *Nota :* le Renseignement d'origine cyber (ROC) n'est pas mentionné. *Livre blanc sur la défense et la sécurité nationale* 2013, Paris : La Documentation française, p. 70.
11 LAURENT, Sébastien-Yves*, op. cit.* note 1, p. 184.
12 MOUTOUH, Hugues, POIROT, Jérôme. *Dictionnaire du renseignement.* Paris : Perrin, 2018, 864 p.
13 Commission de la défense nationale et des forces armées, Audition du général Jean-François Ferlet, directeur du renseignement militaire, sur le projet de loi de programmation militaire, session ordinaire 2017-2018, compte rendu n°52, jeudi 08 mars 2018, séance de 09 heures 00.
14 DUPONT, Alan. « Intelligence for the Twenty-First Century », *Intelligence and National Security.* Vol. 18, Issue 4, 2003, p. 21.
15 La CIA à la recherche du renseignement humain perdu. *Intelligence Online*, 16 février 2023.
16 DUPONT, Alan, *op. cit.* note 14, p. 21.
17 *Ibid.*
18 *Ibid.*

avec une tendance des usagers à l'exposition de soi[21]), mais également sur les capacités intrusives des services (écoutes, relationnel téléphonique, pénétration du domicile et mise en œuvre de dispositifs d'écoute ou de captation vidéo, interception de courriels, etc.) afin de réaliser un environnement extrêmement poussé de la cible[22] avant un « tamponnage » et son éventuel recrutement[23]. La diversité des informations collectées et leur valorisation par une analyse fouillée permettent ainsi d'accroître l'efficacité du processus de ciblage[24] et de favoriser les chances de réussite du recrutement, y compris à travers la manipulation[25].

Une étude publiée en 2016 par le centre de recherche Berckman de l'université d'Harvard considère qu'en raison de l'importante quantité de données générées par l'emploi des objets connectés, les services de renseignement seront en capacité de contourner les moyens de protection et de chiffrement mis en œuvre dans les moyens de communication habituellement employés[26]. De même, James Clapper, ancien directeur de la CIA, a déclaré qu' « *à l'avenir, les services de renseignement pourraient tirer parti de l'Internet des objets pour identifier, surveiller ou localiser des suspects, découvrir des indicateurs potentiels, ou obtenir des mots de passe* »[27]. En effet, l'Internet des objets (IdO) constitue une réalité avec « […] *des milliards d'objets qui sont censés nous représenter* »[28] et qui seront disséminés dans les espaces publics et privés, voire dans nos organismes (pacemaker). Il est estimé qu'en 2025 chaque personne aura en moyenne 5 000 interactions par jour avec un objet connecté[29]. Or, l'utilisation de ces dispositifs va générer des traces numériques qui seront laissées par les usagers, permettant « *alors d'observer et d'analyser en temps réel leurs déplacements, leurs activités et leurs interactions, et d'en tirer des analyses prédictives sur leurs besoins et leurs comportements à des fins commerciales, stratégiques, malveillantes ou d'intérêt public* »[30]. Une conjonction des capacités des dernières innovations technologiques (intelligence artificielle et IdO) permettra une catégorisation des comportements individuels, fondée sur l'analyse en temps réel des données du web et de l'IdO, avec les modèles prédictifs du big data[31]. Il est possible, par exemple, de connaître le nombre de personnes venant d'entrer dans une maison ou le profil d'utilisation de certains services (eau, électricité...[32]) ; de même, les aspirateurs autonomes sont capables aujourd'hui de cartographier l'intérieur d'une habitation[33]: ils peuvent donc fournir des informations très précieuses comme la surface et l'aménagement du lieu de vie. Les assistants vocaux constituent également un capteur de choix permettant l'écoute continue de l'ensemble des conversations orales tenues dans une pièce[34]. L'ensemble de ces objets s'inscrit donc dans un écosystème que les services de renseignement pourront pleinement exploiter.

Ces évolutions conduisent à la multiplication des données générées, et donc, à la création d'empreintes et d'identités numériques par les individus, car la limite entre le virtuel et le réel s'érode progressivement, dans un *continuum*

19 HRIBAR, Gašper, PODBREGAR, Iztok, IVANUŠA Teodora. « OSINT : A « Grey Zone » ? ». *International Journal of Intelligence and CounterIntelligence.* Vol. 27, Issue 3, 2014, p. 529-549.

20 PECH, Yannick. Vers une intelligence cyber ? Penser le renseignement augmenté dans la noosphère. *Prospective et stratégie*, n° 10, 2019, p. 75.

21 DÉTRAIGNE, Yves, ESCOFFIER, Anne-Marie. *Rapport d'information relatif au respect de la vie privée à l'heure des mémoires numériques.* Sénat, n° 441, 2009, p. 31.

22 GUILLOT, Philippe, VENTRE, Daniel. *Capacités d'interception et de surveillance. L'évolution des systèmes techniques*, programme « UTIC France-Europe », 2019, p. 5.

23 « *Le but était de rassembler le plus de renseignements intimes possibles sur la cible, ses activités professionnelles aussi bien que personnelles, ses coordonnées et ses fréquentations, ses habitudes et ses goûts. Chaque détail de sa vie privée susceptible de faire apparaître une ou plusieurs failles qui pourraient, à l'aide du levier adéquat, faciliter l'obtention de sa collaboration, sous contrainte si nécessaire. Dans tous les cas, cette étude détaillée permettait aussi aux responsables de trouver le profil d'OT s'adaptant le mieux à la cible ou, s'il s'agissait d'un officier traitant à l'étranger, de fournir à celui-ci les moyens de s'accorder au profil de l'individu et de prendre immédiatement l'ascendant sur lui grâce à la connaissance profonde de sa personnalité. Phase cruciale dans l'opération menant au recrutement, il fallait s'assurer que l'intérêt de la personne ciblée était plus important que les difficultés à la faire collaborer ajoutées aux risques encourus* ». In : LHUILLIER, Jean-François. *L'homme de Tripoli. Mémoires d'agent secret.* Paris : Mareuil, 2023, p. 177.

24 « *La future source est choisie en fonction d'une multitude de paramètres (capacité d'accès à des renseignements utiles ou à désinformer, profil psychologique, environnement familial, etc.)* ». LEFÈBVRE, Paul. Officier. In : MOUTOUH, Hugues, POIROT, Jérôme (dir.). *Dictionnaire du renseignement.* Paris : Perrin, 2018, 864 p.

25 BURKETT, Randy. « An Alternative Framework for Agent Recruitment : From MICE to RASCLS ». *Studies in Intelligence*, Vol. 57, Issue 1, 2013, p. 7-17.

26 GRASSER, Urs, GERTNER, Nancy, GOLDSMITH, Jack, LANDAU, Susan *et al.* « Don't panic. Making Progress on the « Going Dark » Debate ». *The Berkman Center for Internet & Society at Harvard University*, 2016, 37 p.

27 LE MONDE. Le directeur du renseignement américain reconnaît s'intéresser aux objets connectés. *Le Monde*, 10 février 2016.

28 Intervention de M. Laurent Heslault, directeur des stratégies de sécurité, Symantec en France. In : LE DAIN, Anne-Yvonne, Sidot, Bruno. *Sécurité numérique et risques : enjeux et chances pour les entreprises.* Rapport des offices parlementaires, n° 2541, Tome II : auditions, 2015, p. 384.

29 CAILLEAUD, Nicolas. Cyberesécurité : ces appareils qui servent de porte d'entrée aux criminels. *Cnews*, 18 décembre 2021.

30 DOUZET, Frédérick. Du cyberespace à la datasphère. Enjeux stratégiques de la révolution numérique. *Hérodote,* La Découverte, n° 177-178, 2020, p. 3.

31 DE GANAY, Claude, GILLOT, Dominique. *Rapport au nom de l'office parlementaire d'évaluation des choix scientifiques et technologiques pour une intelligence artificielle maîtrisée, utile et démystifiée.* Tome II, 2017, p. 84.

32 Intervention de M. Jean-Luc Moliner, directeur de la sécurité, Orange. Bruno Sido et Jean-Yves Le Déaut, Rapport sur le risque numérique : en prendre conscience pour mieux le maîtriser ?, compte rendu de l'audition publique du 21 février 2013 et de la présentation des conclusions le 26 juin 2013, Assemblée nationale n° 1221 et Sénat n° 721, 2013, p. 41.

33 ROCA, Vincent. Les objets connectés nous espionnent-ils ? [enregistrement vidéo]. In : *France culture*, 13 mars 2019 [9']. Disponible sur : https://www.franceculture.fr/numerique/les-objets-connectes-nous-espionnent-ils

34 CIMINO, Valentin. Alexa et Google Home sont-ils des espions intelligents ?. *Siècle digital*, 23 octobre 2019.

cyberespace-espace physique[35]. La fine analyse et exploitation de l'ensemble de ces informations constituent donc une plus-value certaine en matière de renseignement humain, en facilitant la phase de ciblage et en personnalisant à l'extrême les processus de recrutement[36]. En outre, ces capacités permettent également de simplifier le traitement de la source pendant une longue période en collectant un grand nombre d'informations utiles à l'officier traitant (OT[37]) lors des contacts et de leur préparation[38]. Ce profilage donne l'opportunité au service de renseignement qui projette le recrutement de sélectionner l'OT disposant du profil idoine pour cette mission en fonction de ses aptitudes personnelles et professionnelles[39]. Enfin, de nouvelles perspectives sont également ouvertes avec l'emploi d'avatars par les services de renseignement sur les réseaux sociaux pour faire du « *renseignement humain virtuel* »[40].

IV) L'« agilité numérique » des adversaires face aux capteurs techniques

Si les capacités des services de renseignement en matière de ROHUM sont préservées, c'est que l'on peut supposer que les capteurs techniques présentent certaines limites. Ces dernières résultent en partie d'une adaptation des adversaires aux mesures pouvant être mises en œuvre. Ce constat est d'autant plus prégnant dans le cadre de la lutte antiterroriste, car les djihadistes situés dans la zone sahélienne, et les membres de Daesh, utilisaient des dispositifs de communication de courte portée, dont le rayonnement est limité à quelques kilomètres, complexifiant les interceptions des communications et la localisation des belligérants[41]. En outre, Daesh maîtrisait pleinement des techniques de dissimulation, notamment vis-à-vis des capteurs images (avions, drones et satellites) : par exemple, à Raqqah, les terroristes couvraient les rues de bandes de tissus[42].

Cette adaptation de l'adversaire aux capteurs techniques lui permet également de tirer profit des nouveaux outils en variant les moyens de communication et leurs usages[43] (emploi de plusieurs téléphones mobiles et cartes SIM, messageries chiffrées, etc.). En conséquence, les modes opératoires adverses évoluent constamment afin d'exploiter au mieux les possibilités des technologies, tout en se préservant des méthodes d'identification et de suivi déployées par les services de renseignement[44]. En effet, si la numérisation et la connectivité ont contraint l'exercice de l'action clandestine en raison de la porosité entre espaces physique et numérique, conduisant à une digitalisation de l'environnement opérationnel des clandestins[45], les terroristes, œuvrant également dans la clandestinité, sont touchés par ces mêmes contraintes de limitation des traces numériques (conduisant Daesh à publier un manuel en 2014 à destination de ses membres, déclinant les mesures de sécurité à mettre en œuvre sur Internet[46]).

In fine, une « *agilité numérique*[47] » a été constatée chez l'adversaire terroriste qui assure une veille informationnelle lui permettant une adaptation capacitaire et opérationnelle rendant certaines techniques traditionnelles, comme les interceptions de sécurité, quasi inopérantes[48]. En conséquence, l'infiltration des structures et des groupes terroristes constitue bien souvent le moyen le plus efficace[49] (mais également le plus risqué) pour connaître les *modus operandi*, l'environnement du groupe, les moyens de communication et les dissensions qui sont autant d'éléments clés pour mettre en place une stratégie d'entrave.

***Le capitaine Pascal MARTIN** est chef de département au COMCyberGEND et docteur en Histoire moderne et contemporaine .*

35 HAZANE, Éric. Sécurité numérique des objets connectés, l'heure du choix. *Fondation pour la recherche stratégique,* note n° 15/18, 2018, p. 2.

36 CHUZIE, Peter, KLIPSTEIN, Michael. « The Internet of Things Disruptive Evolution for Intelligence Collection », *Journal of Intelligence and Cyber Security.* Vol. 2, Issue 2, 2019, p. 39-52.

37 « *L'officier traitant - « OT » dans le jargon des services – désigne un personnel chargé de recruter et de traiter des sources humaines (ou agents)* ». In : MOUTOUH, Hugues, POIROT, Jérôme, *op. cit.* note 24*,* p. 569.

38 CHUZIE, Peter, KLIPSTEIN, Michael. « The Internet of Things Disruptive Evolution for Intelligence Collection », *op. cit.*, p. 39-52.

39 *Ibid.*

40 Les spécialistes de l'HUMINT virtuel cherchent une nouvelle voie pour faire prospérer leurs avatars. *Intelligence online*, 29 septembre 2022.

41 Commission de la défense nationale et des forces armées, audition du général Christophe Gomart, directeur du renseignement militaire, sur le projet de loi relatif au renseignement, session ordinaire 2014-2015, compte rendu n° 49, mercredi 25 mars 2015, séance de 09 heures 00.

42 Commission d'enquête relative aux moyens mis en œuvre par l'État pour lutter contre le terrorisme depuis le 7 janvier 2015, audition, à huis clos, du général Christophe Gomart, directeur du renseignement militaire (DRM), Mme Lorraine Tournyol du Clos, adjointe au directeur, chargée de la stratégie, et du colonel N, assistant militaire, session ordinaire 2015-2016, compte rendu n° 31, jeudi 26 mai 2016, séance de 14 heures 30.

43 Commission de la défense nationale et des forces armées, Audition du général Jean-François Hogard, directeur de la protection et de la sécurité de la défense, sur le projet de loi relatif au renseignement, session ordinaire 2014-2015, compte rendu n° 50, mercredi 25 mars 2015, séance de 10 heures 30.

44 Les autorités américaines ont compris que plus un groupe terroriste respecte les règles de sécurité, moins il laisse d'empreintes traçables par des dispositifs techniques. In : MOUTOUH, Hugues, POIROT, Jérôme, *op. cit.* note 24*,* p. 663.

45 LORD, Jonathan. « Undercover Under Threat : Cover Identity, Clandestine Activity, and Covert Action in the Digital Age », *International Journal of Intelligence and CounterIntelligence*. Vol. 28, Issue 4, 2015, p. 666-691.

46 JONES, Sam, SOLOMON, Erika. « Isis closes the cyber blackout blinds to avoid attack ». *Financial Times,* 27 octobre 2014.

47 Audition du général Jean-François Hogard, directeur de la protection et de la sécurité de la défense, mercredi 25 mars 2015, *op. cit.* note 43.

48 « *Il en tire parti et certaines techniques traditionnelles, il faut le reconnaître, deviennent quasi inopérantes* ». *Ibid.*

49 RONDOT, Philippe. Face aux menaces diffuses, le renseignement humain devrait pouvoir garder sa place. *Après-demain*, n° 37, 2016, p. 35.

ISSN : 2428-7733