The CREOGN Research Notes

Gendarmerie Nationale Officers College Research Center

Issue 91 – September 2023

Captain Pascal Martin (PhD)

©Gorodenkoff *via* Adobe Stock

Priorité stratégique de la prospective

Gendarmerie et territoires

CREOGN certifies that this document was written by a human being

HUMAN INTELLIGENCE IN THE AGE OF NEW INFORMATION AND COMMUNICATION TECHNOLOGIES (NICT)

Technical intelligence is now irreplaceable within intelligence services. The set of sensors it covers seems to be a response to many operational constraints and is one of the priorities of the most sensitive government departments. This trend towards the *'technologisation'* of services has been growing steadily since the beginning of the 21st century, despite the significant budgetary resources it requires. This is particularly true in the United States, where Edward Snowden's revelations in 2013 demonstrated not only the scale of the surveillance system, but also the importance of technology in the intelligence services, particularly in terms of data collection and analysis[1].
However, this preponderance of technical sensors cannot overshadow the importance of human intelligence (HUMINT[2]), the importance of which was emphasised as early as 2008 in the French White Paper on National Defence and Security: "*Special attention will be paid, in the overall effort, to human intelligence. This implies improving the recruitment and training of personnel responsible for this mission, increasing the number of sources and improving their geographical distribution according to our priority areas of interest*"[3].

Human sources are an unquestionable and indispensable capability enhancement, as they enable the collection of protected information that is not accessible through open sources, and can also facilitate the contextualisation of information. This paper opts to discuss the use of human intelligence within intelligence services and the prospects offered by technological developments. The present document does not address the rules and standards that govern and regulate the action of intelligence services.

I) Complementary sensors: a consensus within intelligence services

The French intelligence community is unanimous in its view that sensors should complement each other, because "*it is the cross-fertilisation of human, technical and operational sources that gives us our strength*"[4]. The aim of these agencies, which are designed to defend the State and its interests, is to obtain protected and vital information by any means (in compliance with the laws and regulations in force). With this in mind, all possible capabilities must be combined to achieve this goal, as Director General of the Directorate General of Internal Security (DGSI) Patrick Calvar stated in 2016: "*I also intend to demystify all that is constantly being said about technical intelligence and human*

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 Committee on National Defence and the Armed Forces, hearing of Prefect Érard Corbin de Mangoux, Director General of External Security (DGSE) at the Ministry of Defence, 2012-2013 Ordinary Session, Minutes No. 56, Wednesday 20 February 2013, 09:30 sitting.

intelligence, because this distinction means nothing. I've been in this job for thirty-nine years: there's intelligence and then there are the methods by which we can obtain it, the main thing being to obtain it"[5].

The coordinated use of several types of sensor, both remote and close (SIGINT[6], IMINT[7] , HUMINT and CTI[8]), has enabled intelligence to be acquired on the organisation of terrorist groups operating in Libya and the Levant, and a systemic analysis of Daesh and its modus operandi to be established. Cross-referencing this information has also made it possible to produce military targeting files used by French forces or by the coalition[9].

The complementary nature of the sensors has thus acquired doctrinal value since the publication of the 2013 White Paper on Defence and National Security, which recognises that HUMINT, SIGINT and IMINT "*are complementary and inseparable. It is the combination of information gathered through these three channels that gives intelligence its value*"[10]. However, while the capacity balance between human intelligence and technical intelligence is often mentioned and praised, it remains theoretical because of the weight that the latter represents in the output of intelligence services[11].

II) Human intelligence : a vital sensor

While the quality of human intelligence is more heterogeneous than that derived from other sensors, particularly technical sensors[12], it nevertheless offers certain advantages. Unlike the raw information obtained from technical sensors, HUMINT provides a more detailed understanding of local situations and, in areas where technological development is limited, such as the Sahel, allows access to extremely important data, particularly in terms of military operations[13]. In addition, a human source can infiltrate human networks that are inaccessible to technical sensors which, despite their increasing performance and sophistication, are limited in their use[14]. Human beings can gather impressions or rumours, capture a particular state of mind or plans hatched in private, which they can then contextualise and compare with the observation of their environment.

In this respect, current Director of the Central Intelligence Agency (CIA) William Burns emphasised the urgent need to develop human intelligence networks in China in order to capture high value-added information that can determine an adversary's intentions, despite the massive flows of information gathered by other methods and despite the development of surveillance technologies that hamper the deployment of human intelligence networks[15]. So while the volume of information gathered is often smaller than with technical intelligence, the contributions of HUMINT can be of great strategic or operational value.

After the 11 September 2001 attacks, it was established that the CIA had significantly reduced its capacity to carry out clandestine operations and gather human intelligence[16]. In addition, at the time of the military deployment in Afghanistan, the CIA had only one analyst and a small team of agents with a command of the numerous dialects. As a result, the CIA urgently undertook a long process of rebuilding its networks, carrying out recruitment campaigns and creating special training courses as a matter of urgency[17].

III) The evolution of human intelligence under the impetus of NICTs

Human intelligence (which has been used in particular in conflict zones[18]) is evolving to adapt to the growth of NICTs, given that a significant proportion of political and economic information is now available from open sources[19] (disrupting

5 Committee on National Defence and the Armed Forces, hearing of Mr Patrick Calvar, Director General of Domestic Security (DGSI), 2015-2016 Ordinary Session, Minutes No 47, Tuesday 10 May 2016, 5:00pm session.
6 Signals Intelligence.
7 Imagery Intelligence.
8 Cyber Threat Intelligence.
9 Committee of Inquiry into the means implemented by the State to combat terrorism since 7 January 2015, hearing, in camera, of General Christophe Gomart, Director of Military Intelligence (DRM), Ms Lorraine Tournyol du Clos, Deputy Director, in charge of strategy, and Colonel N, Military Assistant, 2015-2016 Ordinary Session, Minutes No. 31, Thursday 26 May 2016, 2.30 p.m. sitting.
10 *Nota :* Cyber Intelligence (CI) is not mentioned. *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 Committee on National Defence and the Armed Forces, Hearing with General Jean-François Ferlet, Director of Military Intelligence, on the draft military programming law, 2017-2018 Ordinary Session, Minutes No. 52, Thursday 08 March 2018, 09:00 session.
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.*
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.

the traditional dichotomy between open and closed sources[20]). As a result, HUMINT can draw on publicly accessible data (social networks in particular, with a tendency for users to expose themselves[21]), but also on the intrusive capabilities of intelligence services (wiretapping, telephone contacts, infiltrations and deployment of listening or video capture devices, email interception, etc.) in order to establish an extremely advanced background of a target[22] before accosting them and potentially recruit them[23]. The diversity of the information collected and its enhancement through in-depth analysis can thus increase the effectiveness of the targeting process[24] and increase the chances of successful recruitment, including through manipulation[25].

A study published in 2016 by the Berckman research centre at Harvard University considers that, due to the large amount of data generated by the use of connected objects, intelligence services will be able to bypass the protection and encryption methods implemented in the means of communication commonly used[26]. Similarly, former director of the CIA James Clapper has stated that "*in the future, intelligence services could take advantage of the Internet to identify, monitor or locate suspects, discover potential informers, or obtain passwords*"[27]. The Internet of Things (IoT) is a reality, with *"[...] billions of objects that are supposed to represent us*"[28] scattered across public and private spaces, and even in our bodies (pacemakers). It is estimated that by 2025, each person will have an average of 5,000 interactions a day with a connected object[29]. The use of these devices will generate digital traces left by users, making it possible "*to observe and analyse their movements, activities and interactions in real time, and to derive predictive analyses of their needs and behaviour for commercial, strategic, malicious or public interest purposes*"[30]. A combination of the capabilities of the latest technological innovations (artificial intelligence and IoT) will make it possible to categorise individual behaviour, based on real-time analysis of web and IoT data, with the predictive models of big data[31]. It is possible, for example, to determine how many people have entered a given building, or the pattern of use of certain services (water, electricity, etc.[32]). Similarly, autonomous hoovers are now capable of mapping the interior of a house[33]: they can therefore provide very valuable information, such as the surface area and layout of the living space. Voice assistants are also valuable sensors, enabling all spoken conversations in a room to be continuously monitored[34]. All these objects are part of an ecosystem that intelligence services will be able to exploit to their advantage.

These developments are leading to an increase in the amount of data generated, and therefore to the creation of digital fingerprints and identities by individuals, as the boundary between the virtual and the real is gradually eroded, in a cyberspace-physical space *continuum*[35]. The detailed analysis and exploitation of all these pieces of information therefore represents a definite added value in terms of human intelligence, facilitating the targeting phase and personalising

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 "*The aim was to gather as much intimate information as possible about the target, including their professional and personal activities, contact details and social contacts, habits and tastes. Every detail of the target's private life was likely to reveal one or more loopholes that could, with the right leverage, make it easier to obtain their cooperation, under duress if necessary. In all cases, this detailed study also enabled those in charge to find the profile of the EO best suited to the target or, if it was a foreign case officer, to provide him with the means to match the individual's profile and immediately gain the upper hand thanks to an in-depth knowledge of his personality. This was a crucial phase in the recruitment process, as it was necessary to ensure that the interests of the person targeted were more important than the difficulties of getting them to cooperate, in addition to the risks involved*.". In : LHUILLIER, Jean-François. *L'homme de Tripoli. Mémoires d'agent secret.* Paris : Mareuil, 2023, p. 177.

24 « *The future informant is chosen on the basis of a multitude of parameters (ability to access useful information or to disinform, psychological profile, family environment, 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 Speech by Jean-Luc Moliner, Director of Security, Orange. Bruno Sido and Jean-Yves Le Déaut, Rapport sur le risque numérique : en prendre conscience pour mieux le maîtriser, minutes of the public hearing held on 21 February 2013 and presentation of the conclusions on 26 June 2013, Assemblée nationale no. 1221 and Sénat no. 721, 2013, p. 41.

33 ROCA, Vincent. Les objets connectés nous espionnent-ils ? [enregistrement vidéo]. In : *France culture*, 13 mars 2019 [9']. Available at: 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.

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

recruitment processes to the extreme[36]. In addition, these capabilities also make it possible to simplify the handling of the informant over a long period of time by collecting a large amount of information that is useful to the Case Officer[37] during contacts and preparation[38]. This profiling method provides recruitment-hungry intelligence services the opportunity to select the Case Officer with the right profile for the job, based on their personal and professional skills[39]. Finally, new prospects are also opening up with the use of avatars by intelligence services on social networks for "*virtual human intelligence*"[40].

IV) The "digital adaptability" of adversaries when confronted with technical sensors

The intelligence services' capabilities in terms of HUMINT are so far being preserved because it can be assumed that the technical sensors have certain limits. These are partly the result of adversaries adapting to the measures that can be implemented. This observation is all the more important in the context of the fight against terrorism, because the jihadists in the Sahel region, and the members of Daesh, used short-range communication devices whose range was limited to a few kilometres, making it difficult to intercept communications and locate the belligerents[41]. Daesh also had full mastery of concealment techniques, particularly with regard to image sensors (aircraft, drones and satellites): in Raqqah, for example, the terrorists covered the streets with strips of cloth[42].

The opponent's adaptation to technical sensors also allows him to take advantage of new tools by varying the means of communication and their uses[43] (use of several mobile phones and SIM cards, encrypted messaging, etc.). As a result, adversaries' *modus operandi* is constantly evolving to make the most of the possibilities offered by technology, while avoiding the identification and tracking methods deployed by intelligence services[44]. Indeed, digitisation and connectivity have constrained clandestine action because of the porosity between physical and digital spaces, leading to a digitisation of the operational environment of clandestine operatives[45]. Meanwhile, terrorists, also operate underground, are affected by these same constraints of limiting digital traces (leading Daesh to publish a manual in 2014 for its members, setting out the security measures to be implemented on the Internet[46]).
Ultimately, a "*digital adaptability*[47]" has been observed in terrorist organisations, which keep a watchful eye on information that could allow them to adjust their capabilities and operations, rendering certain traditional techniques, such as security intercepts, virtually inoperative[48]. As a result, the infiltration of terrorist structures and groups is often the most effective[49] (but also the riskiest) way of finding out about the modus operandi, the group's environment, its means of communication and dissensions, all of which are key elements in implementing an obstruction strategy.

***Pascal MARTIN** is at the head of a department at COMCyberGEND and has a PhD in modern and contemporary history.*

Translated by Aude GREGORY, Reserve assistant gendarme

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 « *The Case Officer refers to a member of staff responsible for recruiting and processing human sources (or 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 Committee on National Defence and the Armed Forces, Hearing with General Christophe Gomart, Director of Military Intelligence, on the Intelligence Bill, 2014-2015 Ordinary Session, Minutes No. 49, Wednesday 25 March 2015, 9 a.m. session
42 Committee of Inquiry into the means implemented by the State to combat terrorism since 7 January 2015, hearing, in camera, of General Christophe Gomart, Director of Military Intelligence (DRM), Ms Lorraine Tournyol du Clos, Deputy Director, in charge of strategy, and Colonel N, Military Assistant, 2015-2016 Ordinary Session, Minutes No. 31, Thursday 26 May 2016, 2.30 p.m. sitting.
43 Committee on National Defence and the Armed Forces, Hearing of General Jean-François Hogard, Director of Defence Protection and Security, on the Intelligence Bill, 2014-2015 Ordinary Session, Minutes No 50, Wednesday 25 March 2015, 10.30am session.
44 The American authorities have realised that the more a terrorist group respects security rules, the fewer fingerprints it leaves that can be traced by technical devices. 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 Hearing of General Jean-François Hogard, Director of Defence Protection and Security, Wednesday 25 March 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.