

Exploiter le potentiel du *New Space* au profit du renseignement extérieur

Par Nicolas LERNER

Directeur général de la Sécurité extérieure (DGSE)

L'avènement du *New Space* représente une opportunité majeure pour le renseignement extérieur français. Les constellations de nanosatellites offrent en effet des possibilités sans précédent en matière de surveillance des télécommunications mondiales. Cependant, pour exploiter tout le potentiel de ce nouveau « capteur » de renseignement, plusieurs défis de taille restent à relever :

- nous devons construire des partenariats étroits et mutuellement bénéfiques avec les entreprises françaises innovantes du *New Space*, dans une approche résolument duale ;
- nous devons nous préparer à intégrer ce capteur dans une stratégie « multi-capteurs », en le considérant non pas comme une capacité additionnelle juxtaposée aux capacités historiques, mais comme un nouveau rouage d'un appareil de renseignement multi-vectoriel ;
- enfin, et c'est probablement le point le plus structurant, nous devons sans attendre décupler notre capacité à traiter, exploiter et analyser les volumes de plus en plus importants de données que nous collectons sur les réseaux internationaux, en nous appuyant sur l'intelligence artificielle.

UN NOUVEAU CAPTEUR AU POTENTIEL INÉDIT

Les nanosatellites, moins coûteux et plus rapides à produire que les satellites traditionnels, offrent des possibilités sans précédent en matière de surveillance des réseaux de télécommunications. Le lancement d'une constellation de nanosatellites dédiée au renseignement électromagnétique permettrait en effet de superviser une grande partie de l'activité radioélectrique mondiale, et donc de suivre des événements d'intérêt en tout point du globe. En outre, de telles constellations sont susceptibles d'offrir des « taux de revisite » très élevés, et donc une quasi-permanence de notre visibilité télécom. Leur caractère modulaire permettrait enfin de leur confier un large spectre de fonctionnalités et de les concevoir de façon agile et évolutive. Le *New Space* porte ainsi un immense potentiel pour le renseignement extérieur, comparable à aucun autre capteur technique par son caractère global et quasi-permanent.

Les cas d'usage potentiels d'une constellation de renseignement télécom pour un service extérieur sont presque illimités :

- la connaissance, depuis l'espace, des réseaux télécoms mondiaux (téléphonie mobile, *wifi*, communication et navigation par satellite, réseaux militaires, réseaux IoT, etc.) ;
- la détection précoce de crises en toute zone du monde, en identifiant des anomalies radioélectriques (augmentation ou réduction soudaine de l'activité télécom

d'une zone, par exemple), qui sont souvent des indicateurs d'activités humaines inhabituelles. La détection de ces anomalies pourra conduire à déployer sur la zone concernée des capacités de renseignement plus ciblées ;

- la caractérisation des flux qui présentent un intérêt en matière de renseignement, et le recueil de premiers éléments techniques (signatures, métadonnées, clés cryptographiques, etc.) permettant de préparer des opérations de renseignement plus complexes ;
- la géolocalisation précise, depuis l'espace, d'une large variété d'émetteurs (drones, satellites de communication, véhicules, radars, téléphones mobiles, équipements radio, etc.).

Il convient par ailleurs de noter les nouvelles générations de satellites de communication sont, et seront de plus en plus, en mesure de communiquer entre eux, constituant de véritables « réseaux en orbite » s'affranchissant des infrastructures terrestres et permettant ainsi des liaisons « point à point » entre utilisateurs. Disposer de capteurs placés dans l'espace sera sans doute utile pour être en mesure, demain, de recueillir du renseignement sur de tels réseaux.

LA NÉCESSITÉ D'UNE APPROCHE DUALE

En matière de *New Space* comme dans la plupart des domaines technologiques de rupture (intelligence artificielle, calcul quantique, etc.), le temps où les services régaliens disposaient d'une avance technique sur la sphère privée civile est révolu. L'innovation dans ces domaines est aujourd'hui largement portée par les entrepreneurs et pensée avant tout pour des usages civils. Dans le domaine des télécommunications, les services offerts par les opérateurs privés ont dorénavant des performances avancées susceptibles d'être exploitées par les États.

Pour les États, et en particulier pour les services de renseignement, la seule stratégie viable pour éviter le décrochage technologique est donc de construire des partenariats stratégiques avec les entreprises innovantes nationales. Ces partenariats doivent être pensés dans une logique de réciprocité. D'un côté, l'État doit soutenir ces entreprises en mobilisant les leviers à sa disposition : financements, commande publique, mise à disposition d'installations techniques, protection contre la prédation étrangère, soutien à l'exportation, projets de R&D communs, etc. Réciproquement, l'État doit pouvoir bénéficier, y compris au profit de ses usages les plus régaliens comme le renseignement, des solutions innovantes de ces entreprises, voire d'une certaine capacité à orienter l'innovation à leur profit. La clé de voûte de cette démarche reste évidemment le maintien du caractère souverain de ces entreprises – dont certaines, qui peinent à trouver en Europe les financements nécessaires à leur croissance, envisagent de se tourner vers des investisseurs étrangers, notamment américains. Cette situation nécessite des politiques publiques ambitieuses qui dépassent largement les missions des services de renseignement, mais qui sont nécessaires pour répondre aux besoins de ces derniers.

Ce n'est que par cette démarche, fondamentalement « duale », que le renseignement extérieur français pourra demeurer à la pointe de la technologie. C'est un changement de paradigme important, puisqu'il implique que des services de l'État, pour des missions régaliennes, s'appuient dans certains domaines sur des services commerciaux privés, et non sur des capacités patrimoniales. C'est le cas dans le domaine spatial, où l'État s'appuie historiquement sur des capacités patrimoniales développées dans le cadre de grands programmes spatiaux.

Cette approche duale, fondée sur la coopération publique-privée, est particulièrement pertinente dans le domaine du *New Space*, dans lequel la France dispose d'un tissu indus-

triel dynamique et performant. Les constellations de surveillance du spectre électromagnétique, en particulier, sont adaptées à des usages duaux : à titre d'exemple, une telle constellation serait en mesure, au-delà de son apport pour le renseignement extérieur, de suivre le déploiement de la 5G sur le territoire national (en localisant les antennes), de surveiller l'usage des fréquences accordées aux opérateurs télécoms, d'être mobilisée à des fins de surveillance de l'espace et de surveillance maritime, ou de détecter des avions au profit de l'aviation civile et militaire.

Une des clés du succès de cette démarche publique-privée dans le domaine du *New Space* sera la capacité des industriels et des services de l'État à travailler main dans la main, en mettant en commun leur expertise, dès la phase de conception des projets. En effet, une spécificité des satellites est l'impossibilité d'intervenir physiquement, après leur lancement, pour renouveler les capteurs qu'ils embarquent. La conception d'une constellation de renseignement télécom nécessite donc une capacité avancée à anticiper les évolutions télécoms sur plusieurs années, pour s'assurer que les capteurs placés dans l'espace demeurent pertinents dans les années qui suivent leur mise en orbite.

LA CLÉ DU RENSEIGNEMENT TECHNIQUE : L'APPROCHE MULTI-CAPTEURS

Si l'émergence de ce nouveau capteur offrira des possibilités inédites en termes de recueil de données, et s'il sera performant pour une large gamme de tâches, son efficacité restera limitée s'il est utilisé isolément. La complexité des missions de renseignement, notamment lorsqu'il s'agit de cibles « dures », c'est-à-dire bien protégées et difficiles à atteindre, requiert une approche plus holistique.

Pour demeurer dans le peloton de tête des services de renseignement occidentaux, nous devons continuer à développer notre capacité à intégrer et à combiner les différents types de capteurs et d'effecteurs de notre arsenal. Cela est indispensable pour être en mesure de recueillir du renseignement sur les cibles les plus dures, car la sécurité de ces cibles est souvent pensée pour « résister » à chaque capteur pris isolément : mesures d'hygiène numérique contre les intrusions cyber, chiffrement robuste contre les interceptions passives, etc.

Rien que dans le milieu spatial, les opérations de renseignement sont d'autant plus efficaces que nous sommes en mesure de penser chaque vecteur comme un rouage d'un système de renseignement multi-vectorel. À titre d'illustration, dans le cadre d'une opération de lutte anti-terroriste sur une zone donnée : tandis que les nanosatellites offriront une vue d'ensemble et permettront de suivre les changements à grande échelle, les drones embarqueront des capteurs plus flexibles pour des missions tactiques, et les plateformes de haute altitude fourniront quant à elles, de façon complémentaire, une surveillance discrète, continue et stable de la zone, grâce à leur capacité à embarquer des capteurs plus lourds et plus complets.

Au-delà du domaine spatial, pour aborder des cibles dures, il est indispensable d'intégrer toutes les capacités de renseignement technique dans une approche multi-capteurs. Qu'il s'agisse des interceptions passives, de la cryptanalyse, des intrusions cyber, du piégeage des terminaux ou des capacités spatiales, chacune de ces capacités apporte un élément unique et complémentaire dans la construction d'un accès ou la conception d'une opération. La combinaison de ces diverses capacités de renseignement crée une synergie où l'efficacité globale dépasse de loin la simple addition de la force de frappe individuelle de chaque capteur. La capacité à apprécier comment ces capteurs et effecteurs s'entrecroisent et se renforcent mutuellement, dans le cadre d'opérations sophistiquées, est la marque des rares services de renseignement capables de pénétrer les cibles les plus dures.

Si l'approche multi-capteurs est déjà une réalité dans le domaine du renseignement, un défi structurant dans les années à venir sera de nous doter d'une capacité à coordonner automatiquement la manœuvre de nos capteurs, en particulier à l'aide de systèmes d'intelligence artificielle. L'introduction de cette forme d'automatisation nous permettra de franchir une nouvelle étape dans l'intégration de nos capteurs, pour atteindre des performances opérationnelles inédites. Les capteurs issus du *New Space*, en particulier, auront un impact d'autant plus massif sur nos capacités de renseignement qu'ils seront intégrés dans une telle approche globale.

LE PLUS GRAND DÉFI DU RENSEIGNEMENT MODERNE : EXPLOITER LES DONNÉES RECUEILLIES

Mais à quoi bon développer de nouveaux capteurs et construire de nouveaux accès si nous ne sommes pas en mesure d'exploiter les données qu'ils produisent ?

En réalité, les services de renseignement modernes sont, aujourd'hui déjà, confrontés au défi immense que constitue l'exploitation de la donnée. L'augmentation des quantités de données recueillies et l'hétérogénéité extrême de leur format constituent un défi inédit. Il s'agit d'un changement de paradigme majeur pour les services de renseignement car, historiquement, le principal enjeu était de recruter de nouvelles sources humaines et de conquérir de nouveaux accès techniques. Or aujourd'hui, le « réactif limitant » est notre capacité à traiter les données déjà recueillies et stockées, pour en extraire du renseignement pertinent. Autrement dit, l'avantage stratégique d'un service de renseignement n'est désormais plus une question de volume de données collectées, mais repose sur la capacité à identifier rapidement la donnée utile.

À mesure que nous déployons de nouveaux types de capteurs et que nous nous intéressons à de nouvelles zones du monde – ce qui s'accompagne généralement de nouveaux formats de données à ingérer – ce défi s'annonce toujours plus titanesque. Les nouveaux capteurs issus du *New Space*, les drones, les plateformes de haute altitude : ces nouveaux capteurs sont prometteurs, mais leur apport concret restera très limité si nous n'avons pas, en amont, su investir massivement dans l'innovation autour de la donnée, pour changer d'échelle dans notre capacité à traiter la donnée.

Relever ce défi majeur suppose avant tout de continuer à investir dans des outils d'intelligence artificielle spécialisés dans l'analyse de la donnée (transcription et traduction automatique, reconnaissance de locuteur, interprétation d'images satellitaires, etc.), afin de permettre aux exploitants de se concentrer sur des tâches à haute valeur ajoutée. Cet effort a été engagé par la direction générale de la Sécurité extérieure (DGSE) depuis plusieurs années.

Mais nous devons aussi, et c'est un des enjeux les plus structurants du renseignement technique pour les années à venir, réussir à exploiter tout le potentiel de l'IA générative pour révolutionner notre capacité à détecter l'information utile dans l'information massive – et, plus généralement, assister les analystes dans tout le cycle du renseignement. Cet axe d'effort nécessite sans doute que la France investisse pour se doter d'un modèle fondateur souverain, car il est difficilement imaginable de dépendre pour cela de solutions commerciales étrangères, à plus forte raison que ces modèles sont nativement bridés pour interdire les usages « offensifs » propres à un service de renseignement extérieur.

Enfin, au-delà des outils, les services de renseignement extérieurs devront changer de culture pour adopter une approche du renseignement qui soit davantage centrée sur la donnée. Il s'agira demain, par exemple, d'identifier une potentielle source humaine en recherchant, dans une zone d'intérêt, un profil adéquat par l'analyse automatique d'un large volume de données géolocalisées. Ce changement de paradigme nous appelle à faire évoluer nos métiers, nos pratiques, nos critères de recrutement, et à préparer tous nos

« officiers traitants » à travailler autour de la donnée, en symbiose avec des intelligences artificielles. C'est notamment pour répondre à ce défi que la DGSE a profondément transformé son organisation ces derniers mois.

CONCLUSION

Ainsi, ce n'est qu'au prix d'efforts majeurs sur plusieurs axes que nous serons en mesure d'exploiter tout le potentiel du *New Space* au profit du renseignement extérieur : un travail « main dans la main » avec le tissu de *start-up* français, l'intégration des capteurs du *New Space* dans une stratégie multi-capteurs et une révolution de notre capacité à travailler la donnée, en nous appuyant sur l'intelligence artificielle.

Pour relever ces défis, la DGSE s'appuiera sur sa relation très étroite avec la direction générale de l'Armement (DGA) et l'Agence de l'innovation de défense (AID), car dans le domaine du spatial comme dans celui de l'intelligence artificielle, il ne serait ni réaliste ni pertinent que la DGSE avance seule. Elle a notamment besoin de la force de frappe de la DGA en matière de veille technologique, d'outils de financement et de planification. Réciproquement, la DGSE constitue pour le ministère des Armées un véritable laboratoire d'innovation opérationnelle, grâce à son agilité en termes d'acquisition et ses capacités de maîtrise d'œuvre, qui lui permettent d'intégrer rapidement l'innovation dans ses opérations.

Enfin, dans le domaine du *New Space* comme dans les autres domaines technologiques de rupture, les projets doivent être pensés dans une logique de co-construction et de mutualisation au sein de la communauté nationale du renseignement (CNR), sous la coordination de la CNRLT : partage des données interceptées, mutualisation des acquisitions de données, co-développement, etc. Dans des domaines aussi dynamiques et complexes que le *New Space*, l'IA ou le calcul quantique, les services de la CNR ne peuvent se permettre d'avancer en silo et nous devons éviter toute forme de compétition entre services sur les talents ou les ressources.