

Séminaire « Soutenabilités »

Contribution - Covid-19 : pour un « après » soutenable

Nom : Angibault

Prénom : Jean-Luc

Institution ou entreprise : Wintellis

Axe(s) :

- Quelles attentes à l'égard de la puissance publique face aux risques ?

Intitulé de votre contribution : Intelligence stratégique : quelles attentes à l'égard de la puissance publique ? Quelles complémentarités avec le secteur privé ?

Résumé de votre contribution :

Les attentes à l'égard de la puissance publique pour affronter risques et menaces sont très fortes, d'autant que les facteurs de déstabilisation sont particulièrement dynamiques (terrorisme, cyber, infox), et pour certains émergents (pandémie mondiale) ou annoncés (biodiversité, dérèglement climatique).

Dans ce cadre, l'État doit-il couvrir tous les champs ou des pans peuvent-ils être délégués au secteur privé ?

La réponse se situe probablement dans un partage entre la détection et l'entrave des "flux de mort" qui mettent en péril la stabilité à l'État et la préservation des "flux de vie" pour conserver une fluidité de fonctionnement au secteur privé.

Intelligence stratégique
Quelles attentes à l'égard de la puissance publique ?
Quelles complémentarités avec le secteur privé ?

Contribution à l'appel de France Stratégie¹ sur le thème
COVID-19 : pour un « après » soutenable

La révolution des technologies de l'information et de la communication (TIC) a généré un monde plus ouvert en permettant à chacun d'accéder pour un coût négligeable à un volume d'informations en expansion constante et d'échanger librement avec tous². Cette révolution a entraîné parallèlement le développement d'une exigence de transparence, les ONG souhaitant exercer un droit de regard sur les activités des états, les citoyens sur l'action de leurs gouvernants, les consommateurs sur les producteurs et les actionnaires sur leurs entreprises. Enfin, l'explosion des réseaux sociaux renforce ces dynamiques, accroissant mécaniquement le volume d'informations généré, densifiant les relations entre les individus, augmentant les capacités de chacun à être entendu par tous.

Dans ce monde d'information, de transparence et de réseaux, le renseignement étatique³ suscite l'étonnement tant il apparaît comme un univers fermé, opaque et entretenant des liens ténus avec le reste de la société. Quelle est sa réelle utilité ? Ne souffre-t-il pas d'un cloisonnement préjudiciable à son évolution ? Ne peut-on envisager de privatiser tout ou partie de ses activités afin de le rendre plus réactif, moins bureaucratique, plus adapté aux réalités de notre monde perturbé ? A tout le moins, n'existe-t-il pas des champs du renseignement qui pourraient être traités par le secteur privé ?

Le renseignement est en fait confronté à un triple paradoxe -ouvert/fermé, concentration/expansion et public/privé- qui lui donne une vitalité particulière de par l'affrontement, la coexistence et l'interpénétration de ces caractéristiques, même si le flou stratégique des décideurs politiques en limite la portée. Sa concentration sur les menaces vitales ouvre des pans que le secteur privé investit déjà.

*

1 – Le paradoxe ouvert/fermé

Le monde du renseignement est ambivalent. Il est à la fois très fermé dans son fonctionnement et très ouvert sur les réalités du monde, comme la série *Le Bureau des légendes* le démontre de manière saisissante.

¹ <https://www.strategie.gouv.fr/actualites/appel-contribution-covid-19-un-apres-soutenable>

² Cette affirmation mérite d'être nuancée de par son caractère occidental-centré. La carte de l'accès à Internet dans le monde est disponible à l'adresse : <http://www.journaldunet.com/web-tech/chiffres-internet>

³ Le champ de cet article se limitera, sauf mention particulière, au renseignement extérieur.

Le secret est un impératif, même s'il n'exclut pas une certaine transparence manifestée au travers de la nomination d'un porte-parole, de sites web officiels, de décrets d'organisation en ligne, d'auditions parlementaires⁴. Il est d'abord impératif car il assure la protection des personnels des services et de leur famille ainsi que celle des sources humaines⁵. Il permet ensuite de cacher les capacités (et les incapacités) des services, autrement dit leurs forces et leurs vulnérabilités⁶. Il nourrit enfin la singularité de cet outil de souveraineté, à la disposition des plus hautes autorités de l'État pour l'appréciation indépendante des situations (par rapport aux intérêts nationaux, mais aussi pour le rôle de la France comme membre permanent du Conseil de sécurité des Nations unies), la détection et l'entrave des menaces ou toute mission à la discrétion du gouvernement.

A l'inverse, l'ouverture est une nécessité pour remplir sa mission de « vigie ». En effet, l'appareil de renseignement scrute les réalités du monde, parfois très éloignées des panoramas médiatiques ou des messages officiels, ce qui commande d'être étroitement connecté au terrain, aux organisations, aux réseaux, et surtout aux individus, car, au final, toute action est décidée et menée par un ou des humains. Les personnels du renseignement, par essence, sont donc très ouverts sur le monde, sur les cultures, les sociétés, leur histoire, et s'attachent aux faits. Ils disposent d'une multitude de capteurs complémentaires, autorisant une perception plus fine et des recoupements indispensables à l'exactitude des renseignements. En effet, l'abondance d'informations n'est pas une garantie de fiabilité, la désinformation, le parti pris, la recherche d'influence sont des réalités de notre monde surinformé⁷.

Le renseignement profite ainsi d'une fertilisation à sens unique provenant de l'extérieur. Ses personnels se nourrissent des travaux des universités, des centres de recherche, des *think tanks*, des instituts, des journalistes, ..., pour appréhender le connu et concentrer alors leurs recherches sur l'inconnu. A l'image d'un trou noir, ils absorbent la matière visible pour valoriser la matière invisible et la faire renaître dans une autre dimension, celle du renseignement.

Toutefois, cette dichotomie ouvert/fermé évolue et génère de nouvelles limites.

Les agents sont de moins en moins secrets : l'explosion, pour des raisons de sécurité, de l'identification biométrique, combinée à celle de la traçabilité par la

⁴ Pour la DGSE, voir les adresses suivantes pour, le décret d'organisation, <https://www.legifrance.gouv.fr/eli/arrete/2012/12/21/DEFD1243577A/jo/texte/fr>, le site web, <http://www.defense.gouv.fr/dgse>, une audition parlementaire, <http://www.senat.fr/compte-rendu-commissions/20160215/etr.html#toc3>.

⁵ Les sources humaines peuvent être définies comme des personnes conscientes, non membres des services, qui fournissent des renseignements, selon des motivations diverses généralement classées en 4 familles : argent, ego, compromission, idéologie.

⁶ Si, par exemple, dans le cadre de la lutte anti-terroriste, je suis capable, à l'insu des cibles suivies, de percer les conversations échangées sur un réseau social, je dispose d'un avantage décisif, dont il me faut absolument préserver la confidentialité. Si je ne sais pas les percer, je dois cacher cette incapacité afin d'alimenter l'incertitude.

⁷ Voir l'article de Guillaume Serries, *Soft power : l'usine à troll russe s'oppose à la technicité américaine*, à l'adresse <https://www.zdnet.fr/actualites/soft-power-l-usine-a-troll-russe-s-oppose-a-la-technicite-americaine-39824056.htm>

multiplication des objets connectés (aux premiers rangs desquels le téléphone cellulaire, avec la possibilité de remonter cette traçabilité dans le temps par exploitation des métadonnées archivées par les opérateurs), compromet la clandestinité, à savoir la capacité pour un agent d'opérer avec une identité fictive.

Cette même limite réduit également la furtivité et la sécurité des personnels non clandestins engagés sur le terrain, avec pour corollaire une dérive vers le « tout technique » pour la recherche du renseignement. A l'image du drone armé, qui permet de « neutraliser » une cible sans engager la vie des opérateurs, le recueil de renseignement par moyens techniques reste discret, sûr, rapide et sans danger pour les personnels... au prix d'une fermeture sur les réalités de terrain.

2 – Le paradoxe concentration/expansion

Avant la chute du Mur de Berlin et l'implosion de l'URSS, le renseignement portait, pour l'essentiel⁸, sur le contre-espionnage (CE) et le politique (comprendre la stabilité ou l'instabilité des régimes politiques en place, les intentions diplomatiques, les alliances, ...). En toute logique, la direction du renseignement de la DGSE s'articulait en un service de renseignement politique et un autre de CE (abritant en son sein, à l'état embryonnaire, des structures de contre-terrorisme -CT-, contre criminalité, suivi des appareils militaires et des mercenaires, sécurité économique).

Cette organisation a progressivement évolué avec l'accroissement ou l'apparition de menaces, sous la pression de ce que l'on pourrait qualifier de vecteurs « chaos » : guerres régionales (y compris au centre de l'Europe) spontanées (crises africaines, Iran-Irak,...) ou provoquées (1^{ère} et surtout 2^{ème} guerres du Golfe) ; effondrement des états (Irak, Syrie, Libye, Somalie, Soudan,...) et son cortège de troubles (réfugiés, prises d'otages, piraterie,...) ; développement de la criminalité transfrontalière (produits stupéfiants, êtres humains, armes,...) ; prolifération liée aux armes de destruction massive⁹ ; guerre économique avec la création des *War room* aux États-Unis en 1993 sous l'impulsion du président Bill Clinton¹⁰ ; espionnage tout azimut (y compris entre alliés comme l'ont révélé les affaires récentes¹¹) ; cyber et bien évidemment le terrorisme d'inspiration islamique.

Le champ des menaces s'est donc élargi et l'organisation actuelle¹² repose sur un éventail de services spécialisés au niveau de la direction du renseignement (CT, contre prolifération -CP-, sécurité économique -SE-, renseignement géopolitique et CE) et d'un centre veille-opérations rattaché à la direction générale, le suivi des appareils militaires ayant été transféré à la Direction du Renseignement Militaire

⁸ En France en tout cas.

⁹ Nucléaire, bactériologique, chimique, balistique.

¹⁰ Pour davantage de détails, voir *La Dissuasion par l'information* de Didier Lucas et Alain Tiffreau à l'adresse http://www.ege.fr/download/13.dissuasion_par_information.pdf

¹¹ Voir l'article de Olivier Chopin, Olivier Schmitt et Yves Trotignon, *Peut-on espionner ses alliés ?* à l'adresse http://www.lemonde.fr/idees/article/2015/06/26/peut-on-espionner-ses-allies_4662677_3232.html

¹² <http://www.defense.gouv.fr/dgse/tout-le-site/organisation>

(DRM) lors de sa création en 1992¹³. Cette dynamique d'expansion des menaces a mécaniquement entraîné un accroissement de moyens, tant en termes d'effectifs que budgétaires¹⁴.

De manière assez paradoxale, ce mouvement d'expansion s'est accompagné d'un phénomène de concentration. D'abord, par nécessité, a été opérée une focalisation des moyens sur les menaces immédiates (CT, CP) dans le champ sécuritaire et les contrats internationaux (SE)¹⁵ dans le champ économique. Ensuite, par flou stratégique et héritage historique, un surinvestissement perdure sur certaines zones. On peut légitimement s'interroger sur le caractère hautement stratégique pour la France des crises politiques africaines en comparaison de la stabilité des pays du Maghreb (pour lesquels nos élites nourrissent un sentiment trompeur de parfaite connaissance du fait des imbrications humaine, historique et culturelle) ou de l'émergence des BRICS et des *next eleven* ¹⁶ ?

Se dessinent ainsi des espaces subis, où l'appareil de renseignement demeure en veille passive, et des intervalles non couverts, ce qui ouvre des marges de manœuvre au secteur privé.

3 – Le paradoxe public/privé

Le renseignement d'État constitue un service public à part entière. La création de valeur et la rentabilité sont donc, par définition, des notions mineures. Par ailleurs, cela exige de tels moyens humains et matériels, dans un cadre juridique si spécifique, que la transposition dans le privé n'est pas possible. Néanmoins, le retrait de l'État, non pas dans un mouvement de désengagement, mais plutôt, comme nous l'avons vu, dans une dynamique de concentration sur des thématiques cardinales (CT, CP, SE) est déjà une réalité.

Dans le domaine de la sécurité des entreprises et de leurs personnels à l'étranger, le débat¹⁷ sur les sociétés militaires privées (SMP) et les entreprises de services de

¹³ Voir le décret de création de la DRM à l'adresse

<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000357733&categorieLien=id>

¹⁴ Pour le détail, voir l'article *La DGSE, modèle français d'intégration*, signé de l'ancien directeur général, Bernard Bajolet, en juin 2014, dans la revue *L'ENA hors les murs* à l'adresse

<http://www.defense.gouv.fr/dgse/tout-le-site/la-dgse-modele-francais-d-integration-l-ena-hors-les-murs-juin-2014>

¹⁵ La commission interministérielle d'appui aux contrats internationaux (CIACI), créée en 2008, qui comprend un volet civil et un volet militaire, présidée par le directeur du cabinet du Premier ministre, a pour objectif de mobiliser et de coordonner les moyens de l'État (démarches politiques, dispositifs de financement, etc.) afin de soutenir des grands projets faisant l'objet d'une concurrence internationale et considérés comme importants pour l'économie française.

¹⁶ Voir l'article de Kathryn Koch (senior stratège chez Goldman Sachs Asset Management) de juin 2012 dans *La Tribune Après les BRICS, voici les Next Eleven* à l'adresse

<http://www.latribune.fr/actualites/economie/international/20120622trib000705367/apres-les-brics-voici-les-next-eleven.html> ainsi que *Le Petit lexique des pays émergents* publié en mars 2016 à

l'adresse <http://la-story.over-blog.com/2016/03/petit-lexique-des-pays-emergents.html>

¹⁷ Voir <https://www.cercle-k2.fr/etudes/le-recours-aux-prestations-des-entreprises-de-services-de-securite-et-de-defense-empiete-t-il-sur-les-prerogatives-regaliennes-de-securite-ou-va-t-il-dans-le-sens-de-l-histoire-53>

sécurité et de défense (ESSD) a longtemps occupé l'espace public¹⁸. Certaines interviennent désormais dans le domaine de K&R (*Kidnap & Ransom*)¹⁹, alors que la DGSE a été l'acteur exclusif de ce type d'affaires depuis le début des années 2000.

Dans le domaine économique, en deçà des contrats internationaux, l'espace a été occupé par une multitude d'acteurs²⁰, aux premiers rangs desquels l'agence pour la diffusion de l'information technologique (ADIT)²¹, créée en 1992 et se définissant aujourd'hui comme le « leader européen de l'intelligence stratégique »²². De même, la société Défense Conseil International DCI²³ a permis, à partir de son pôle « intelligence stratégique et intelligence économique », la création du cabinet Intellecto²⁴ en 1998 (et antérieurement de l'École de Guerre Économique EGE²⁵ en 1997).

Dans le domaine Cyber, l'appareil de renseignement dispose de capacités propres. Au niveau régalién, l'État a créé les structures *ad hoc* pour gérer cette menace avec en 2009 l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI)²⁶ et en 2017 le commandement des forces de cyberdéfense des armées²⁷. Néanmoins, à l'instar du domaine économique, l'État apporte des réponses de niveau stratégique, en privilégiant les infrastructures critiques (en attribuant en particulier la qualification d'Opérateurs d'Importance Vitale OIV²⁸). Sous ce seuil, des industriels et des sociétés privées apportent leurs services aux entreprises.

Un autre aspect relève de l'utilisation par le renseignement de moyens très particuliers et très onéreux, de manière ponctuelle (pour pallier des « trous capacitaires »²⁹), ce qui nécessite, pour le coup, dans une logique économique et

¹⁸ Voir le rapport d'information sur les sociétés militaires privées de la commission de la Défense nationale et des forces armées de l'Assemblée nationale de février 2012 à l'adresse

<http://ddata.over-blog.com/4/31/29/03//Rapport-SMP-version-finale.pdf>

¹⁹ Voir par exemple la société Hiscox à l'adresse <https://www.hiscox.fr/wp-content/uploads/2015/11/fpKR.pdf>

²⁰ Pour un aperçu, voir l'annuaire de l'intelligence économique sur le portail de l'IE à l'adresse <http://www.portail-ie.fr/entreprises>

²¹ Créée en 1992 sous la forme d'un établissement public à caractère industriel et commercial, l'ADIT est devenue une société anonyme en 2003 détenue par l'État, puis a ouvert son capital au fonds Butler Capital Partners en 2010, qui a cédé sa participation au fonds Weinberg Capital fin 2015. Voir le détail à l'adresse

https://fr.wikipedia.org/wiki/Agence_pour_la_diffusion_de_l'information_technologique

²² <http://www.adit.fr/fr>

²³ <https://www.groupedci.fr/>

²⁴ <http://www.intelleco.com/>

²⁵ https://fr.wikipedia.org/wiki/%C3%89cole_de_guerre_%C3%A9conomique

²⁶ <http://www.ssi.gouv.fr/>

²⁷ <https://www.defense.gouv.fr/portail/enjeux2/la-cyberdefense/la-cyberdefense/presentation>

²⁸ <http://www.gouvernement.fr/sites/default/files/risques/pdf/sgdsn-14-03-16.pdf>

²⁹ Voir l'article de Michel Cabirou *Défense : des trous capacitaires dans la panoplie des espions* dans La Tribune du 14/03/2013 à l'adresse <http://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/20130314trib000753988/defense-des-trous-capacitaires-dans-la-panoplie-des-espions-34.html>

opérationnelle (trop cher à développer et trop long à mettre au point de manière autonome), de faire appel à la sous-traitance privée³⁰.

La dichotomie public/privé dans le monde du renseignement apparaît donc comme une dynamique déjà existante. Elle est en voie d'accélération en raison de l'acuité et de la densité des menaces, monopolisant les capacités de l'État au niveau stratégique et laissant mécaniquement un champ de développement au secteur privé. Ce mouvement présente toutefois des limites juridiques, réglementaires, déontologiques et éthiques. Si les unes sont du ressort de l'État, les autres reposent sur les seuls acteurs privés et représentent à terme leur légitimité. Les affaires récentes démontrent que toute dérive déontologique ou éthique est rapidement sanctionnée par le marché dans une société de l'information, transparente et réticulaire.

*

Au bilan, il apparaît peu probable qu'émerge un jour une agence de renseignement privée d'intérêt public. Le renseignement représente en effet le dernier outil de souveraineté, offrant des capacités d'évaluation et d'action autonomes **et** clandestines dans un monde marqué par une incertitude croissante.

Les dynamiques en cours connaîtront consolidation puis accroissement. Ainsi l'activité « renseignement » se répartira entre l'État, au niveau stratégique, et le secteur privé en deçà.

L'acteur régalien se focalisera sur des thèmes vitaux, que nous pourrions qualifier de « flux de mort » car ils mettent en péril la stabilité sécuritaire, politique, économique et sociale du pays.

L'acteur privé apportera de manière croissante un appui opérationnel aux entreprises avec des sociétés d'intelligence³¹ économique, stratégique, sécuritaire et de gestion de crise, afin de permettre la plus grande fluidité possible des « flux de vie » (environnement des affaires, stabilité et intégrité des systèmes d'information, sûreté des personnels et des biens). Ces dernières n'agiraient pas selon un modèle de sous-traitance mais dans un mode complémentaire au service des acteurs privés ou publics.

³⁰ Voir le roman de Jean-Christophe Rufin, *Katiba*, aux éditions Flammarion, 2010, dans lequel une agence étatique privatise un certain nombre de ses activités, pour pallier des « trous capacitaires » mais aussi pour ne pas avoir à assumer certaines actions. Il s'agit bien évidemment de fiction...

³¹ Au sens d'intelligence de situation, c'est-à-dire de capacités à comprendre, à discerner, à agir dans un contexte donné.