ÉCOLE DE GUERRE

PROMOTION *GÉNÉRAL GALLOIS*

2016 -2017

Cyber et Geoint militaires, quelles contributions pour un décideur ?

Etude comparée France – Etats-Unis

Chef de Bataillon Benoît GAUME

Sous la direction de :

M. Philippe BOULANGER

Professeur des Universités

Cyber et Geoint militaires, quelles contributions pour un décideur ?

Etude comparée France – Etats-Unis

Résumé

Les sociétés digitalisées et interconnectées dans lesquelles évoluent nos armées offrent aujourd'hui deux capacités modernes, interarmées et échappant par essence au cloisonnement d'un milieu spécifique, qu'il convient désormais pour tout officier supérieur de maîtriser.

Le Cyber est actuellement en pleine structuration en France, où l'EMA tente d'organiser les savoir-faire issus du monde numérique civil, avec une flagrante similitude avec le modèle américain de 15 ans son aîné. S'affranchissant des frontières, le cyber apporte par ses capacités de veille et d'investigation numérique une réelle contribution en termes de connaissance et d'anticipation au chef militaire. Il est aussi devenu un appui hors du commun aux opérations de tous types, ainsi qu'une arme offensive de riposte, aux effets dévastateurs.

Le Geoint, quant à lui, est une forme naissante et très pertinente de recherche de renseignement au niveau interarmées. Il fusionne d'énormes masses de données numériques géolocalisées, à la recherche de tendances et de clés de compréhension permettant d'orienter le chef militaire dans sa quête de certitudes avant une action armée potentielle. Dans ce monde confidentiel et high-tech de la gestion de la donnée informatique, les Armées tente également de s'organiser et le parallèle avec les Etats-Unis est éloquent.

D'ailleurs, par les comparaisons et les réflexions posées au fur et à mesure des travaux menés, ces deux domaines du renseignement militaire, aujourd'hui distincts, nous apparaitront de plus en plus proches, leur complémentarité encore peu exploitée à ce jour promettant de réelles capacités à connaitre et défaire son ennemi dans un espace-temps qu'aucune capacité militaire n'a encore proposé à ce jour. Dans un contexte d'engagement contre le terrorisme international jusque sur notre propre territoire, nous verrons que les Armées ont de réels enjeux de prospection notamment dans le monde du *Bigdata*, où la porosité entre recherche civile et capacités militaires n'a jamais proposé autant d'opportunités opérationnelles.

Cyber et Geoint militaires, quelles contributions pour un décideur ?

Etude comparée France – Etats-Unis

Sum up

The digitized and interconnected societies in which our armed forces evolve today offer two modern and joint capabilities, avoiding in essence the partitioning of a specific environment, which is now appropriate for any senior officer to master.

Cyber issues are currently being restructured in France, and the French Joint Staff tries to organize the knowledge arising from the civil digital world, with a clear similarity to the American model of 15 years its predecessor. Freed from borders, Cyber mastery brings a real contribution in terms of knowledge and anticipatory ability to the military leader, through its intelligence and investigational capabilities. It has also become a very important support for military operations of all types, as well as an offensive response weapon, with potentially devastating effects.

Geoint is in a second hand a recent and highly relevant form of joint intelligence research. It merges massive amounts of geolocalized digital data, in search of trends and keys of understanding, in order to guide the military commander in his quest of absolutes before a potential joint armed operation. In this very secretive and high-tech world of computer data management, the French Armies also are trying to organize themselves. Similarities in the French process with the United-States of America are also very important.

Moreover, in comparison and over certain reflection, these two distinct areas of military intelligence will appear to be becoming increasingly close. Their complementary and as yet little exploited potential at present promises a real ability to understand and defeat our enemy, in a space-time framework that no military power has yet proposed. In the context of a commitment against international terrorism in our own territory, we will see that the armed forces have a real prospecting issue, particularly in regards to *Bigdata*, where the extreme links between civilian research and military capabilities have never offered as much operational opportunities.

Cyber et Geoint militaires, quelles contributions pour un décideur ?

Etude comparée France – Etats-Unis

Introduction

Notre société contemporaine, si encline à remettre en cause les repères ancestraux, se caractérise notamment par une pénétration profonde de la numérisation, et les Armées ne peuvent échapper à cette réalité. Internet, systèmes interconnectés, production exponentielle de données, propagande, cyberagressions… Ces thèmes sont autant de domaines sur lesquels de nombre de réflexions ont cours actuellement pour positionner l'outil militaire *a priori* mal adapté, comme le plan de la *Transformation Digitale*. La sphère numérique transgresse en effet toutes les frontières et tous les milieux, mais héberge bel et bien nos ennemis.

Le Cyber – l'arme numérique individuelle ou étatique - et le Geoint – la fusion de données de masses géolocalisées - sont de fait les deux capacités militaires modernes illustrant parfaitement le bouillonnement intellectuel de la FIR (Fonction Interarmées du renseignement) et de l'Etat-major des Armées (EMA) pour définir et intégrer ces savoir-faire au sein de l'outil militaire. Mais ces deux composantes sont aussi modernes qu'inintelligibles pour de nombreux officiers. La nécessité de les maîtriser pour pouvoir les employer étant une évidence, ce mémoire s'attèle donc à cette tâche fondamentale de présentation des enjeux croisés de ces deux capacités militaires émergentes, où tant de choses restent encore à créer de manière transverse, et sur la base d'écrits de réflexions stratégiques parus ces dix dernières années dans chacun de ces deux domaines distincts. Et c'est bien là tout l'intérêt : étudier en quoi le Cyber et le Geoint pourraient finalement être complémentaires dans la quête d'anticipation est une démarche prospective totalement innovante peu documentée à ce jour.

Alors qu'en France la stratégie militaire Cyber est en pleine définition, et qu'en parallèle le renseignement militaire redécouvre le potentiel de la fusion des données par le Geoint, il est légitime de présenter dans une approche thématique ces deux nouvelles capacités pour bien les appréhender. Cette étude, menée volontairement en silo, permettra d'identifier progressivement les points de connexions potentiels du Cyber et du Geoint. Une réflexion d'ensemble sur les liens entre renseignement technique et opérations militaires se dessinera alors au fur et à mesure, permettant d'élaborer une ébauche inédite de rapprochement des deux disciplines. Dans quelle mesure cette nouvelle situation pourrait améliorer la compréhension globale de l'ennemi par les autorités militaires et faciliter leurs prises de décision, maintenant que la menace d'un « Pearl Harbor numérique [1]» est intégrée aux plans nationaux ?

[1] Discours de Leon E.Panetta, alors secrétaire de la défense américain, peu de temps après l'attaque informatique ayant détruit plus de 30000 postes du groupe pétrolier Aramco en Arabie Saoudite en 2012.

Cyber et Geoint militaires, quelles contributions pour un décideur ?

Etude comparée France – Etats-Unis

« ***Savoir est peu de chose, l'essentiel est de savoir tirer parti de ce que l'on sait*** **»**

Montaigne, Essais, 1580

« Une armée victorieuse l'est avant même de livrer bataille »

Sun Tzu, l'Art de la Guerre, V^{e} siècle avant J.C

Analyse par E. BUMILLER et T.SHANKER, «Panetta Warns of Dire Threat of Cyberattack on U.S. », *New York Times,* du 11 octobre 2012.

Cyber et Geoint militaires, quelles contributions pour un décideur ?

Etude comparée France – Etats-Unis

SOMMAIRE

I. Le Cyber militaire, du renseignement aux opérations

1) Contribution du Cyber à l'appréciation de situation du chef

a) Dualité cyber : structuration du besoin militaire sur une capacité civile

Le Cyber, anciennement NTIC[2], entendu comme touchant à la fois à la sécurité informatique (cyberdéfense) et aux manipulations en tout genre des données informatiques jusqu'aux cyberattaques (ou cyberagressions), allant de la couche physique à la sphère cognitive[3], se caractérise avant tout comme un domaine *high-tech*, numérique et informatisé, transfrontalier et battant en brèche par son innovation permanente de nombreux repères. L'espace cyber, souvent conceptualisé comme 4e milieu d'intervention[4], est de ce fait difficile à appréhender pour la plupart dans sa globalité. Rien que définir l'ensemble des termes foisonnant préfixé par « cyber » (cyberprotection, cyberattaque, cyberespace, cyberrésilience….) requiert de nombreux débats au sein de l'EMA, tant les avis d'expert diffèrent[5].

Le Cyber se définit avec certitude par son innovation et ses évolutions permanentes, conduit en cela par la prééminence des acteurs économiques civils comme Thalès, Sogeti ou Orange en France. Mais la dualité de leurs activités est aussi une heureuse réalité qu'il ne faut pas omettre. Toutefois, cette situation met en exergue une prospection militaire à la traine, même si les besoins militaires sont historiquement à l'origine de nombreuses innovations[6]….

Par ailleurs, en France, notons la présence de véritables pépites industrielles du numérique, qui représenteraient une formidable opportunité de souveraineté nationale dans ce domaine si les pouvoirs publics le souhaitaient. Citons par l'exemple l'entreprise Vupen, aujourd'hui disparue, spécialisée dans la recherche et la vente stratégiques de vulnérabilités *0-*

---

[2] NTIC : nouvelles technologies d'information et de communication, désormais remplacé usuellement par IT ; information et télécommunication pour parler du secteur d'activité éponyme.

[3] Le Cyber est parfois représenté par un modèle à 3 ou 4 couches : physique, logique, logicielle et cognitive. Source : O.Kempf, FB Huyghes et N.Mazucchi, *Gagner les Cyberconflits, au-delà du technique*, Economica, 2016, 175p

[4] O.Kempf, *ibid*. De même, « *la conception américaine montre bien que le cyberespace arrive au même rang que les milieux traditionnels : Terre, Mer et Air. Elle traduit également la transversalité de ce milieu y compris dans les paradigmes de sécurité et de défense*.» N. Pierson, *les défis du Cyber pour les Armées*, la Tribune, 07/01/2016.

[5] A.Bonnemaison et S. Dosse*, Attention Cyber ! : Vers le combat Cyberélectronique,* Economica, 2014, 224p.

[6] N'oublions pas l'Arpanet américain, précurseur de l'internet, fonctionnel en 1969 et créé par la Défense américaine au profit de l'Us Air Force et « au commencement de tout » sur notre étude générale !

day[7], ou encore Gemalto, leader mondial de la puce électronique aux multiples applications (carte SIM, cartes bancaires, documents d'identité sécurisés..) et de l'internet des objets (*IoT - Internet of Things*).

Ainsi, dans le domaine militaire hautement stratégique du Cyber, la **DGA Maîtrise de l'Information** (DGA-MI) est désigné comme l'unique pourvoyeur du besoin des Armées, « *le cœur de l'expertise technique du ministère de la Défense pour les systèmes d'information et de communication, la guerre électronique, […] et le cyber* »[8]. Cette structure, basée à Bruz (Bretagne) au sein du Pôle d'Excellence Cyber, est le dispositif essentiel de partenariat Défense-privé créé par le ministre de la Défense M Jean-Yves Le Drian, par ailleurs président de la région Bretagne. Par ce positionnement, la Défense tente de reprendre l'initiative dans le cadrage du besoin Cyber des Armées, en s'appuyant sur les innovations et les recherches des acteurs civils[9]. Vu autrement, il pourrait aussi s'agir de constituer le volet Cyber de la Base Industrielle et Technologique de Défense (BITD)[10], couvrant ainsi les volets économiques, industriels et de recherche d'un domaine stratégique et touchant à la souveraineté nationale[11].

DGA-MI est donc tacitement en charge de reprendre l'initiative dans la satisfaction du besoin formulé par les Armées « ***L'innovation n'est pas accessoire, c'est un besoin existentiel*** »[12]. Pour se convaincre de la pertinence de cette posture, il suffit de considérer les réelles menaces Cyber connues désormais du grand public :

[7] *0-day* : failles critiques majeures d'un système ou logiciel, faisant l'objet de recherches d'acteurs parfois peu recommandables. Un marché opaque existe sur le Darkweb pour la Cybercriminalité notamment. En effet, la connaissance et l'exploitation d'un 0-day donne un avantage quasi stratégique à l'attaquant, tant que la faille n'est pas révélée puis corrigée.

[8] Discours fondateur de la Cyber en France de Monsieur le Ministre de la Défense Jean-Yves Le Drian, prononcé sur le site de DGA-MI à Bruz le 12 décembre 2016. Disponible sur http://www.defense.gouv.fr/ministre/prises-de-parole-du-ministre/prises-de-parole-de-m.-jean-yves-le-drian/Cyberdefense-discours-de-jean-yves-le-drian-lundi-12-decembre-2016, consulté le 13 décembre 2016.

[9] Voir annexe 1 sur les dispositifs d'aide à l'innovation de la DGA.

[10] JP Dunne, *The Defense Industrial Base*, Handbook of Defense Economics, Vol.1, Elsevier 1995, p401. L'auteur y définit la BITD comme les entreprises qui permettent aux Armées de conduire leurs opérations. Il les ventile en 3 catégories : - les unités qui concourent à la production des systèmes d'armes et des équipements létaux (de la R&D jusqu'à l'entretien) - les unités qui fournissent des produits non létaux mais stratégiques comme carburant- les unités qui fournissent des produits courants utilisés par les armées type nourriture).

[11] Le *Livre blanc sur la défense et la sécurité nationale* place la sécurité et la défense des systèmes d'information au cœur des priorités stratégiques de la Nation. Cependant, la DGA ne le comptabilise pas encore dans une capacité stratégique. Voir le Plan Stratégique PP30 (cf.note77).

[12] Analyse par L. Lagneau du discours de M. le Ministre de la Défense J.Y Le Drian, prononcé lors du Forum DGA Innovation du 24 novembre 2016 sur le camus de l'Ecole Polytechnique à Palaiseau. Disponible sur http://www.opex360.com/2016/11/25/m-le-drian-confirme-la-creation-dun-fonds-dinvestissement-dedie-aux-entreprises-innovantes/.

- le 06 novembre 2007, l'aviation israélienne bombarde le site nucléaire de Deir-ez-Zor en Syrie. Tout le réseau de défense aérienne a été paralysé au préalable par une attaque informatique, en particulier ses radars (la pénétration des systèmes s'est vraisemblablement faite en utilisant les ondes radars retour, corrompues aux préalable).
- A l'été 2008, c'est l'invasion de la Géorgie par la Russie qui est précédée par une cyberattaque massive sur les serveurs gouvernementaux afin notamment d'influencer la population et paralyser l'exécutif.
- En janvier 2010, une grande partie des 8700 centrifugeuses d'enrichissement d'uranium militaire iranien sont endommagées par l'action du virus Stuxnet – Opération globale *Olympic Games.*[13]
- Enfin, en 2016 pendant le conflit russo-ukranien, c'est une application innovante développée sur smartphone à l'initiative d'un soldat ukrainien pour coordonner plus efficacement les moyens d'artillerie qui est détournée par les Russes pour localiser indirectement les canons ukrainiens et les détruire[14].

Bien sûr, les cyberattaques sont diligentées par une multitude d'acteurs aux motivations diverses et extrêmement versatiles. L'exemple géorgien est à ce titre dimensionnant pour la réflexion dans le cadre d'une composante opérationnelle Cyber pendant un conflit d'envergure[15], mais d'autres menaces font aujourd'hui peser de grands risques sur la pertinence de l'outil de militaire : radars passifs, brouillage GPS, drones et cyber-drone[16]…

La Défense œuvre également à la mise en place de chaires de cyberdéfense, chargées de cadrer la réflexion des acteurs civils du Cyber dans une sphère d'application militaire (« Chaire de Cyberdéfense et Cybersécurité Saint-Cyr/Sogeti/Thales » de Saint-Cyr

[13] Cette attaque est considérée par beaucoup comme étant le premier usage d'armes cybernétiques. Source : TTU, Et la NSA inventa la guerre cybernétique, TTU n°929 du 06 avril 2014. LA poursuite de Prism est documentée par David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran* , The New York Times, 1er juin 2012, consulté le 17 novembre 2016.

[14] Information issue d'un rapport de la firme de cybersécurité californienne CrowdStrike de décembre 2016. Source : D.Volz, *Russian hackers tracked Ukrainian artillery units using Android implant,* agence Reuters, Washington, 22/12/2016. Disponible sur http://www.reuters.com/article/us-cyber-ukraine-idUSKBN14B0CU, consulté le 23 décembre 2016. Par extension, ce risque Cyber est désormais pris en compte, comme pour le développement du système français *Auxylium* pour les soldats de la mission Sentinelle.

[15] La prise de conscience de l'OTAN s'est traduite par la mise en place d'un centre d'excellence situé à TALINE en Estonie (*NATO Cooperative* Cyber *Defence Centre of Excellence*). Il s'agit d'un lieu d'échange multinational et interdisciplinaire sur les sujets d'expertises liés à la Cyberdéfense.

[16] Cyberdrone : article prospectif *Drones, vers des Cybermissions*, revue Air&Cosmos N°2513 du 09 septembre 2016.

Coëtquidan pour l'Armée de Terre -, **«** Chaire de Cyberdéfense des systèmes navals » animés par l'École navale, Telecom Bretagne, DCNS et Thalès pour la Marine Nationale).

Enfin, la structuration active de la réserve opérationnelle du Cyber par l'EMA, autour du nouveau CRPOC[17], est un autre témoin de la prise de contrôle actuelle des instances militaires françaises sur le monde stratégique du Cyber, en s'appuyant notamment sur le maillage avec les acteurs privés au nom de la préservation des intérêts de la nation, en passant notamment par la protection OIV.[18]

b) Emergence du COMCYBER français

Les acteurs Cyber de la Défense française sont pluriels et se répartissent de manière encore très hétérogène.

D'abord, et eu égard à leur ancienneté dans le domaine, se trouvent les principaux services de renseignement (DGSE, DGSI et DRM). Tous se concentrent par essence sur la fonction **« se renseigner** », qui vise à mettre à disposition de l'autorité de tutelle les informations valorisées, afin de l'aider dans son appréciation autonome de situation. Il faut noter que chacune de ces 3 entités, pour ne citer qu'elles, agissent au niveau stratégique, en lien avec les plus hautes sphères de l'appareil d'état. Les théâtres d'opérations sont en outre bénéficiaires de leurs travaux.

Le Commandement Cyber, ou COMCYBER, a été mis en place en décembre 2016, et sous les ordres directs du CEMA[19], traduisant immédiatement l'aspect interarmées et transverse du Cyber, à la fois composante opérationnelle et milieu d'intervention à part entière. Ce positionnement est également révélateur de **la dimension stratégique du Cyber militaire**, explicitée dès 2013 au sein du Livre Blanc de la Défense[20]. Le COMCYBER en

[17] CRPOC : centre de la réserve et de la préparation opérationnelle de Cyberdéfense.

[18] « *4400 réservistes de Cyberdéfense, soit 4000 réservistes citoyens de Cyberdéfense, et 400 réservistes opérationnels* ». Extrait du discours de J.Y Le DRIAN*, op. cit (note 08)*

[19] Cet état-major est en pleine construction à l'heure de rédaction de ce mémoire, avec une première structure de pré-configuration, et une cible fonctionnelle prévue pour l'été 2017.

[20] Le Livre blanc de 2013 (LBDSN 2013) pose en effet les bases d'une doctrine nationale qui combine un fort renforcement de la résilience et de la protection des systèmes d'information des Armées face aux attaques avec une capacité progressive de réponse : *« La doctrine nationale de réponse aux agressions informatiques majeures repose sur le principe d'une approche globale fondée sur deux volets complémentaires. D'abord la mise en place d'une posture robuste et résiliente de protection des systèmes d'information de l'État, des opérateurs d'importance vitale (OIV) et des industries stratégiques, couplée à une organisation opérationnelle de défense de ces systèmes, coordonnée sous l'autorité du Premier ministre, et reposant sur une coopération étroite des services de l'État, afin d'identifier et de caractériser au plus tôt les menaces pesant sur notre pays. Ensuite d'une capacité de réponse gouvernementale globale et ajustée face à des agressions de nature et*

surtout en charge, sous l'autorité du sous-chef opérations de l'EMA, **de concevoir, planifier, préparer et conduire les opérations militaires au niveau stratégique** en apportant une expertise Cyber au commandement des Armées, et en particulier du CPCO[21].

Le COMCYBER se structure en 4 fonctions [22]: se renseigner, se protéger, se défendre et agir. Se renseigner, comme nous l'avons vu précédemment, est inclus dans la fonction « connaissance-anticipation » constitutive des actions de planification et de conception des opérations militaires. La fonction « **se protéger** » est induite par la prérogative du COMCYBER d'assurer la défense et la protection des SIOC[23] dans un cadre juridique strict[24]. **Se défendre** englobe toutes les capacités de défense informatique de l'avant (détection de l'attaque, premières actions) et en profondeur (consolidation de la circonscription, solution d'élimination et de résolution), nécessitant un état résilient des SIOC. L'ensemble des acteurs est coordonné par le CALID[25]. Compte tenu de sa spécificité, la fonction « agir » fait l'objet d'un développement spécifique en partie I.3.

Une dernière prérogative du COMCYBER doit aussi retenir l'attention **: coordonner** la contribution des Armées et les besoins spécifiques du domaine Cyber militaire. L'hétérogénéité du monde du cyber militaire développé supra est ici clairement admise.

---

d'ampleur variées faisant en premier lieu appel à l'ensemble des moyens diplomatiques, juridiques ou policiers, sans s'interdire l'emploi gradué de moyens relevant du ministère de la défense, si les intérêts stratégiques nationaux étaient menacés. »

[21] CPCO : centre de planification et de conduite des opérations, véritable cerveau des opérations militaires françaises. Un centre d'opérations (CO) Cyber y est intégré.

[22] Ces 4 fonctions fondamentales de la Cyber militaire française sont décrites in extenso par le ministre de la défense. Voir discours de J.Y Le DRIAN*, op. cit (note 08).*

[23] SIOC : Systèmes d'information opérationnels et de communication

[24] 2 documents régissent le cadre juridique : l'Article L2321-2 créé par Loi n°2013-1168 du 18 décembre 2013 – art 1 : « *Pour répondre à une attaque informatique qui vise les systèmes d'information affectant le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation, les services de l'Etat peuvent, dans les conditions fixées par le Premier ministre, procéder aux opérations techniques nécessaires à la caractérisation de l'attaque et à la neutralisation de ses effets en accédant aux systèmes d'information qui sont à l'origine de l'attaque. Pour être en mesure de répondre aux attaques mentionnées au premier alinéa, les services de l'Etat déterminés par le Premier ministre peuvent détenir des équipements, des instruments, des programmes informatiques et toutes données susceptibles de permettre la réalisation d'une ou plusieurs des infractions prévues aux articles 323-1 à 323-3 du code pénal, en vue d'analyser leur conception et d'observer leur fonctionnement.* ». Le 2e document est l'instruction ministérielle N°900/DEF/CAB/DR du 26 janvier 2012 relative à la protection du secret de la défense nationale au sein du ministère de la défense.

[25] CALID : Centre d'analyse de lutte informatique défensive. Il assure des missions de veille, d'analyse et d'alerte pour le ministère de la Défense.

Bien sûr, d'autres acteurs militaires sont concourants aux effets des opérations Cyber. Nous retiendrons parmi eux le CIAE[26], basé à Lyon, qui a rejoint le nouveau COMRENS de l'Armée de Terre à l'été 2016. Par son action dans **le domaine de l'influence**[27] militaire, et plus généralement sur le champ immatériel des perceptions (espace cognitif et social), le CIAE a de nombreux points de convergence avec le cyber notamment par son action sur les RSN[28]. L'intégration de l'influence militaire dans la sphère de responsabilité du Cyber[29] est d'ailleurs un autre débat doctrinal, prouvant s'il en était encore besoin l'ampleur des réflexions en vigueur.

Dans ce contexte de réforme, une question s'impose : le modèle français du Cyber militaire ne tendrait-il pas, toute proportion gardée, à rejoindre celui établi de longue date par les Etats-Unis ?

c) L'USCYBERCOM : un FR-COMCYBER américain ?

Après la version classifiée du 5 février 2014, le *Joint Staff* - l'équivalent américain de l'EMA - a publié en 2014 une version publique[30] de sa doctrine interarmées sur les opérations Cyber, la *Joint Publication 3-12 Cyber Operations*[31]. Les opérations Cyber sont intégrées aux opérations traditionnelles, définissant ainsi la place des cyberopérations dans la planification, la préparation, la conduite et l'évaluation des opérations interarmées. Cette doctrine rappelle également la signification et la spécificité des cyberopérations, visant ainsi à les intégrer

[26] CIAE : Centre interarmées des actions sur l'environnement. Créé en 2012, ses missions consistent à mieux faire comprendre et accepter l'action des forces françaises auprès des acteurs locaux. Le CIAE concoure aussi à obtenir une compréhension toujours plus fine de l'environnement dans lequel les militaires français évoluent.

[27] J.D Merchet, « propagande, l'armée tâtonne », *blog secret défense/L'opinion*, http://www.lopinion.fr/edition/international/propagande-web-l-armee-tatonne-21073 consulté le 14 décembre 2016.

[28] RSN : réseaux sociaux et numériques. L'EMA a diffusé un « guide du bon usage des réseaux sociaux » à destination des personnels du ministère de la Défense et de leur entourage pour les sensibiliser aux risques et dangers de ce milieu particulier. DICOD, www.defense.gouv.fr/guide-medias-sociaux/telecharger.pdf, décembre 2016. Consulté le 7 janvier 2017.

[29] Un des premiers exemples d'intégration de l'influence au Cyber est l'hypothèse de l'existence d'une TaskForce offensive qui aurait été mise en place par la France (DGSE) pour lutter contre le djihadisme dans le cyberespace Source : TTUn°984 du 8 juillet 2015.

[30] Si une diffusion sur Internet peut surprendre pour une doctrine pilotant une activité de renseignement et d'opérations sensibles, cette situation relève surtout de la volonté prononcée de se faire connaître au plus grand nombre. Une classification trop élevée du document l'empêche par construction d'être lue, et obère ainsi toute possibilité de développement vers l'extérieur.

[31] *Department of defence, Joint-Publication 3-12 (R), Cyberspace Operations »,* version du 05 février 2013. Disponible sur www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf, consulté le 10 octobre 2016.

davantage dans les opérations militaires interarmées. A la vue de notre étude précédente, il semble très probable que la nouvelle doctrine française Cyber[32] tende vers ce modèle[33].

Il n'est un secret pour personne que les forces américaines conduisent des opérations Cyber depuis des années. La *Joint Task Force Computer Network Defense* a en effet été créée dès 1998, et était responsable des opérations de cyberdéfense du *DoD*[34], sous la direction de la *Defense Information Systems Agency*, équivalent américain de la DIRISI[35]. Puis, à partir des années 2000, elle a pris en compte les aspects offensifs en prenant le nom de *Joint Task Force Computer Network Operations* sous l'autorité de l'US STRATCOM. Dissoute en 2010, elle a intégré le nouvel US CYBERCOM.[36]

Les procédures américaines sont donc en place depuis plus de vingt ans, là où la France crée le COMCYBER fin 2016… Les capacités offensives étaient déjà réparties entre la guerre électronique et les opérations d'information au sein de la communauté du renseignement, ce que l'EMA tente encore de structurer avec ses 3 états-majors de force[37].

Le point à retenir est bien **l'intégration systématique des opérations cyber,** défensives comme offensives, avec un effort initial au sein du volet renseignement, lui-même décisif pour la planification des opérations. Il permet en effet d'appréhender précisément l'ennemi, par l'évaluation plus ou moins complète de ses infrastructures, des zones clés, des acteurs, des points d'accès, et surtout des menaces qu'il représente.

Cette préparation des opérations par le cyber requiert donc une anticipation très importante, bien en amont d'un éventuel conflit. On imagine en effet aisément que la sphère numérique, déjà complexe en temps de paix, se comportera encore bien différemment pendant un conflit. L'espace-temps restera toutefois toujours aussi peu compatible avec une dynamique opérationnelle militaire. La **problématique des accès** amont est donc primordiale pour la Cyber afin d'offrir au décideur des alternatives crédibles en cas de besoin. Aux Etats-Unis, la présence systématique d'un *Joint Cyber Center* auprès des *Geographic Combattant*

[32] Doctrine InterArmées (DIA) 3.20 de 2014 initialement 3.40 en 2012. Classifiée Diffusion restreinte. Actuellement en refonte à l'EMA/COMCyber, sa consultation a eu lieu à l'occasion de la vIC-ITE de l'EMA/CPCO.
[33] Voir discours de J.Y Le DRIAN*, op. cit (note 08)*
[34] *DoD* : *Department of Defense,* le ministère de la défense américain.
[35] Dirisi : direction interarmées des réseaux d'infrastructure et des systèmes d'informations de la défense. Service interarmées dépendant du CEMA créé le 1er janvier 2004 installé au Kremlin-Bicêtre, il est l'opérateur unique de télécommunications de la défense.
[36] USCYBERCOM ou USCYBERCOMMAND . Voir annexe 2.
[37] Une illustration de ce débat pour l'Armée de Terre est donnée dans « CDEF, Les Forces Terrestres et le cyberespace », Mai 2014, Cahiers du Retex/Recherche, EMA, p71.

Command (*GCC*)[38] offre une capacité inégalée de connaissance à l'échelle régionale de l'espace cyber. La France ne possède pas encore en doctrine ce type de structure, même si la 807e compagnie de Transmissions[39] projette ses spécialistes de la cyberdéfense au sein de chaque état-major en opérations. Mais seule la fonction « défense des systèmes » est alors de mise, ce qui ne satisfait pas à la fonction « anticipation » dont il est ici question.

Cependant, on peut constater que le modèle Cyber français tend, toute proportion gardée, à se rapprocher de la structure américaine : un commandement militaire placé sous ordres directs des plus hautes autorités, une lutte informatique à la fois défensive et offensive, et une contribution directe et parfois autonome aux opérations. Seules les différences profondes de conception dans le commandement américain et français expliquent les variations observées, quant au positionnement des unités et leurs périmètres respectifs.

2) L'anticipation Cyber au service des opérations françaises

a) Le J2 de la Cyber : le CRAC

Le Centre de recherche et d'analyse du Cyberespace (CRAC ci-après) est un nouveau capteur de la Direction du Renseignement (DRM ci-après) créé en juillet 2015. Installée à Creil, cette structure est issue du chantier *Transformation 2014* décidée par le Général de Corps d'Armée (GCA) Christophe Gomart.

Le CRAC agit au profit de la DRM[40], dont il est **le capteur Cyber spécialisé**. Il agit donc bien au profit de la fonction stratégique « connaissance et anticipation », de même qu'un ensemble de capteurs concourant. Le CRAC est ainsi positionné au sein de la sous-direction recherche (SDR), au même titre que les autres centres de la DRM. Cependant, outre ses missions de recherche et de collecte d'informations, il est aussi en charge de l'exploitation de l'information Cyber (analyse, production de renseignement)[41], ce qui aurait pu militer pour un positionnement au sein de la sous-direction exploitation (SDE) comme le CRGI[42].

[38] L'*Unified Command Plan (UCP)* structure les zones de responsabilités des 9 *Unified Combatant Commands* (UCC)du *DoD* : 3 COCOMs (SOCOM, TRANSCOM et STRATCOM) et 6 Geographics COCOMs (GCC) : CENTCOM, AFRICOM, EUCOM, NORTHCOM, PACOM, SOUTHCOM). Source : http://www.centcom.mil/ABOUT-US/COMPONENT-COMMANDS/

[39] La 807e compagnie de Transmissions a été créée le 01 juillet 2016. Elle s'organise autour de 4 pôles : l'anticipation et l'analyse de la menace Cyber, la supervision de sécurité des SIOC et systèmes d'armes, le contrôle du spectre électromagnétique, et la mise en œuvre de la lutte informatique défensive.

[40] Voir annexe 3 dédiée à la présentation synthétique des centres de la DRM.

[41] Voir développement spécifique partie I/2/c.

[42] Voir développement spécifique partie II/3/b.

A ce jour, il est important de garder à l'esprit les nombreuses difficultés résiduelles de définition du Cyberespace et des opérations Cyber. De fait, la répartition de la charge de travail au sein de la toutes les entités du monde numérique est encore délicate : qui du CRAC, du COMCYBER, ou des autres services de renseignement a (ou n'a pas) la responsabilité d'un dossier Cyber ? Quelle(s) complémentarité(s), même restreinte au renseignement d'intérêt militaire (RIM) ? Qui est « propriétaire » de la donnée Cyber collectée, de son exploitation et de son cycle de vie (préparation de la donnée, promulgation en référentiel puis décision de retrait)? Ces questions stratégiques alimentent encore de nombreux débats et introduisent des problématiques que nous développerons en 3e partie.

b) Mission « rechercher » : le renseignement d'origine cyber (ROC)[43].

Comme capteur Cyber, le CRAC s'intéresse par essence au ROC. Pour comprendre comment il concourt à l'élaboration d'une appréciation de situation autonome au profit des opérations militaires, il parait opportun de se consacrer à l'étude du mécanisme des trois sous-domaines constitutifs du CRAC, tout en respectant les restrictions de confidentialité.

i) La recherche large spectre : l'OSINT.

Devant l'énorme quantité de données potentiellement d'intérêt militaire sur Internet, il est devenu extrêmement complexe de savoir « quoi » chercher, « à quel endroit », et avec un degré de fiabilité acceptable de l'information collectée en source ouverte (OSINT ou ROSO)[44]. Le besoin apparait ici de mettre en œuvre une véritable capacité de veille de l'Internet et notamment des flux d'échanges des RSN. Il est toutefois vain et tout pragmatiquement impossible de vouloir tout voir et tout savoir. Le résultat, inatteignable, serait d'ailleurs totalement contreproductif. Le CRAC agit donc principalement sur demande d'un client, à travers une RFI[45], afin de lui fournir en retour une réponse exhaustive, à temps et à jour. Ce travail peut techniquement s'apparenter à **une revue de presse spécialisée**, ce qui n'est en rien un savoir-faire militaire. Face à l'ampleur de la tâche, une nécessaire automatisation des tâches s'impose. Un rapprochement est ici immédiat et naturel avec les métiers civils de la gestion documentaire et du management de l'information[46].

[43] A. Bonnemaison, *op. cit*. (note 05)
[44] OSINT : *open source intelligence*, en français ROSO : renseignement d'origine source ouverte.
[45] RFI : *request for information,* demande d'information.
[46] Pour l'exemple, l'outil de veille automatisé Website Watcher est un outil plébiscité dans la gestion documentaire, en tant qu'outil de veille industriel à destination des professionnels de la veille stratégique.

Nous pouvons ici d'ores et déjà formuler plusieurs observations qui cadreront notre réflexion en 3e partie.

- D'abord, il parait indispensable de posséder des **outils automatisés et dédiés de collecte** de données. Un choix stratégique pour cette capacité sera à opérer entre le financement d'un développement d'outils interne à la DRM, long mais efficace, ou un achat sur étagère de nombreux outils disponibles sur le marché, mais à la pertinence parfois contestable.
- De même, préserver la sécurité de l'officier de renseignement et la confidentialité de sa recherche sont indispensable. La définition d'une chaîne d'**anonymisation** informatique robuste semble de ce point de vue indispensable, et ne peut se limiter à l'usage simpliste d'un VPN[47] ou Tor[48]. Le ratio coût/efficacité de la structure choisie pourrait vite devenir incompatible avec le réel intérêt de la demande du client. Mais la sécurité des agents n'a *a contrario* pas de prix…
- Obtenir l'information en source ouverte implique évidemment d'y avoir accès. Autant **pérenniser l'accès** à une page de l'internet semble aisé, notamment en temps de paix, autant accéder à une information sensible, et/ou chiffrée, ou disponible sur le Darkweb[49], d'autant plus en période de crise (impliquant souvent de la censure et des coupures de réseau) sont autant de défis à relever.
- Une part importante de l'information est disponible sur les RSN du fait de leur rapidité et leur adaptation à la problématique sociétale de l'immédiateté. Y avoir accès puis les veiller induit inévitablement, pour la DRM, la détention d'avatars, dont le profil ne doit évidemment pas être relié à sa réelle appartenance. Outre les aspects de gestion de « légende » ou *pattern of life* qui assurent dans ce cas la crédibilité numérique de l'avatar, il faut remarquer que cette problématique est très prégnante au sein des forces de sécurité. Ainsi, la multiplicité des acteurs du renseignement impose une nécessaire **déconfliction dans la gestion des activités des avatars** de chaque entité, afin de se prémunir de tout

[47] VPN : *Virual Private Network*, ou réseaux privés virtuels, sont conçus pour permettre l'accès à des ordinateurs distants via une connexion cryptée. Plusieurs failles sont toutefois connues (VPN FAIL., redirection de port (http://thehackernews.com/2015/11/vpn-hacking.html) jusqu'à l'affaiblissement supposé de certains protocoles à fin d'espionnage (come le protocole PPTP). Voir l'étude comparée disponible sur https://fr.vpnmentor.com/blog/comparatif-de-protocoles-vpn-pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/

[48] Tor : réseau public « en oignon » garantissant par son architecture un degré d'anonymisation à ses usagers. Le trafic étant routé sur des serveurs/nœuds de confiance, il s'agit aussi de sa principale vulnérabilité : la corruption d'un nœud permettra à son auteur d'écouter tout le trafic y transitant. Voir J.E lyan, *Le réseau Tor, utilisé pour cacher botnets et darknets, LeMondeInformatique*, 07 mars 2014.

[49] *Darkweb/ Deepweb* : internet non indexé, inaccessible par les moteurs de recherche classique. Une architecture Tor et des connaissances précises permettent d'intégrer ce monde opaque et douteux.

risque d'erreurs. Ce schéma existe déjà en ROHUM par les cellules J2X. A notre connaissance, aucun organisme n'assure à ce jour cette mission en France pour les avatars, sources numériques de renseignement Cyber.[50]

ii) La recherche ciblée au service du RIM

Après une recherche OSINT large spectre, un processus complémentaire visant à concentrer ses efforts sur un sujet jugé d'intérêt semble cohérent. Il s'agit de la recherche avancée, où le CRAC s'engage à fournir un **portrait numérique approfondi de l'ennemi** potentiel dans son écosystème. Il s'agit d'une description la plus exhaustive des structures, et méthodes utilisées. Le CRAC s'intéresse ainsi à tous les indices passifs générés et fournis par les sondes surveillant d'Internet utiles dans le cadre de la LID: adresses IP, structure d'hébergement de sites, les tables de routages, l'administration de sites, les métadonnées, les *tracking* de flux …. L'exhaustivité de la recherche induit nécessairement sa sensibilité. Notons enfin que compte tenu de l'investigation menée, et afin de se prémunir des outils potentiels de *forensic*[51] de la cible, une impérative condition d'anonymisation est requise.

Mais un facteur limitant pour le CRAC réside dans la prise de conscience généralisée des opérateurs numériques civils de la nécessité de protéger leurs données en ligne afin de conserver la confiance de leurs clients. Citons deux exemples pour illustrer les approches sécuritaires auxquelles est confronté le CRAC :

- De plus en plus d'accès étant sécurisés, les RSSI [52] traquent toute menace potentielle à l'encontre de l'intégrité de leurs services. Ainsi, l'outil *Nmap*[53], très pratique pour le CRAC dans ce cadre de recherche, est aussi très signant quant aux réelles intentions de son utilisateur. Il doit donc innover continuellement dans ses approches silencieuses.

---

[50] La problématique juridique complexe posée par la problématique de la détention d'avatars par un service de l'état, qui plus est sous légende, n'est volontairement pas traitée ici.

[51] *Forensic : « ou informatique légale en français, désigne l'application des techniques ou des protocoles d'investigation numérique respectant les procédures légales pour recueillir et apporter la preuve numérique. Elle regroupe l'ensemble des méthodes permettant la conservation, la collecte et l'analyse de la preuve numérique en vue de les produire dans le cadre d'une action en justice »,* M Quemener, magistrat, spécialiste de la Cybercriminalité, et Procureur Adjoint responsable du Pôle criminel au Tribunal de Grande Instance de Créteil

[52] RSSI : Responsable en sécurité des systèmes d'informations, c'est-à-dire les veilleurs de la Cyberprotection.

[53] *Nmap* ou *Network Mapper* est un outil open source très connu des informaticiens chevronné, spécialisé dans l'exploration réseau et l'audit de sécurité. Il a été conçu pour rapidement scanner de grands réseaux, mais il fonctionne aussi très bien sur une cible unique.

- Les métadonnées des contenus diffusés sur les RSN sont désormais supprimées par l'opérateur. Ainsi, les données de localisation, l'auteur, l'horodatage, les données techniques du système d'origine sont autant d'informations intéressantes qui ne sont plus disponibles, compliquant ainsi la tâche de l'exploitant du CRAC.

iii) L'investigation numérique sur le matériel

Si Internet est la source d'information privilégiée du CRAC, le matériel numérique utilisé, connecté ou non, en est une autre tout aussi pertinente. Il s'agit donc du troisième volet du processus de recherche, complémentaire aux deux autres. Il s'agit **d'exploiter l'ensemble des matériels** saisis lors des opérations militaires sur l'ennemi, afin d'en extraire le maximum des données et caractéristiques d'intérêts militaires (contacts, localisations, images et vidéos, métadonnées diverses, historiques, données effacées…).

Il est évident qu'une telle capacité repose sur le développement d'outils et de capacités de pointe. La volatilité des solutions techniques développées et la vitesse d'innovation sont ici fondamentales. D'ailleurs, le domaine de l'investigation numérique et des *forensic* (notamment les *UFED - universal forensic extraction device*) est un domaine civil en plein essor. Il cristallise en effet de très nombreux appétits, notamment dans le secteur sécuritaire. Pour s'en convaincre, il suffit d'observer l'augmentation des piratages de ce type de société dans le monde civil comme Cellebrite[54].

Deux remarques préliminaires à notre 3e partie peuvent être ici formulées :

- De nombreux acteurs peuvent mettre en œuvre les outils d'investigation de support numériques (ISN), notamment au sein de la Défense. Le principal problème réside dans la capacité à exploiter, partager et fusionner les données techniques collectées : qui en est responsable ? La DRM tendrait à terme à s'organiser autour d'une base de données unique et un SIOC d'exploitation unique, mais les écueils notamment de classification interdomaines sont encore nombreux et représente un défi à relever pour la DRM.

[54] La société Cellebrite est connue pour son UFED phare vendu à la police et aux gouvernements qui permet aux enquêteurs d'extraire les données d'un grand nombre de téléphones portables. Parmi ses clients figurent notamment la police aux Etats-Unis et au Royaume-Uni, et la société pourrait avoir aidé le FBI à pénétrer dans l'iPhone d'un des deux terroristes de San Bernardino, alors que les autorités étaient en plein bras de fer avec Apple. Le piratage du fichier client de Cellebrite a été rendu public le 12 janvier 2017. Quotidien Le Monde, http://www.lemonde.fr/pixels/article/2017/01/12/cellebrite-entreprise-qui-decortique-les-telephones-pour-les-autorites-victime-d-un-piratage_5061822_4408996.html du 12 janvier 2017.

- La question juridique n'est jamais très loin de la rhétorique de l'ISN : où s'arrête le droit à la liberté individuelle et de la propriété, et où commence la nécessité de savoir pour raison de sécurité ? Quel droit est accordé aux services de renseignement dans cette collecte des données? Pour quel usage? Quelles sont les responsabilités en jeu? Cet écosystème juridique représente à lui seul une limite importante que le CRAC doit prendre en compte dans son action numérique.

En synthèse, il faut humblement reconnaitre que tout acteur spécialisé dans la veille numérique s'organise peu ou prou de cette façon (recherche large puis ciblée, au niveau informationnel et matériel, utilisation de la rétro-ingénierie), preuve supplémentaire de la grande dualité du Cyber. Seule l'origine numérique des informations (ROC) pour un dossier touchant au RIM, prédestine son traitement par le CRAC. Pour les mêmes raisons, il parait évident que ce centre s'intéresse également au renseignement d'intérêt Cyber.

c) Mission « exploiter » : le renseignement d'intérêt cyber (RIC)

L'intérêt Cyber d'un RIM concoure *in fine* à caractériser l'ennemi, au sens doctrinal et militaire du terme. Ainsi, nous pouvons décrire les processus d'analyse et d'exploitation du renseignement d'intérêt pour les opérations sous trois aspects dont toute méthode de raisonnement militaire[55] s'inspire : le qui, le quoi et le comment.

i) Le « qui » : les acteurs du cyberespace

Le CRAC identifie et caractérise les acteurs du monde Cyber, avec un impérieux besoin de maintenir à jour les informations détenues, au profit de la DRM et des opérations militaires. Cette assertion mérite toutefois une précision d'importance : seul l'intérêt militaire pourra déclencher la réalisation de ces travaux. Cela ne signifie pas *a contrario* que la cible soit forcément militaire, surtout en s'appuyant sur le concept de guerres hybrides[56]

Il s'agit ici, pour les opérations Cyber, de catégoriser les acteurs (étatiques ou non, économiques, sociaux…), d'évaluer leurs menaces et de caractériser leurs modes d'actions potentiels. L'objectif est donc bien de recenser puis de connaître son ennemi, et ne pas attendre qu'il se dévoile pour le faire…

[55] Notamment la COPD - Comprehensive Operations Planning Directive. Voir PIA 5(B)_PNO(2014), planification du niveau opératif : guide méthodologique, CICDE, Ministère de la Défense, lettre n°152/DEF/CICDE/NP du 26 juin 2014, 136p.

[56] Elie Tenenbaum*, Le piège de la guerre hybride*, IFRI, 2015, 51p.

Toutefois, l'intérêt Cyber d'un acteur risque inévitablement de cibler la population très particulière des *hackers*, dont le métier, la passion ou la cause défendue, par ailleurs très versatile, leur imposent depuis longtemps de se cacher par la mise en œuvre de stratagèmes techniques complexes et robustes. Il peut dès lors sembler ambitieux à une jeune structure militaire comme le CRAC de s'attaquer avec pertinence et efficacité à ce type de population rompue à l'innovation technologique permanente par nécessité de survie.

ii) Le « quoi » : les infrastructures de communication

Il s'agit ici de caractériser les structures à la fois physiques et logiques de la cible traitée (réseau filaire, fibre optique, flux satellitaire ou radio, mappages, tables de routages, *backbones*[57], mais aussi localisation des serveurs, des relais, des bâtiments protégeant ces infrastructures….). Dans une approche purement militaire de l'étude de l'ennemi, il s'agira de d'appréhender son centre de gravité et d'identifier ses vulnérabilités à la fois :

- logiques, par la recherche de *0-day*, de vulnérabilités non corrigées, de *backdoor*…
- et physiques : utilisation de serveurs corrompus, flux transitant sur une fibre maitrisée ou un satellite écouté par la guerre électronique, absence de redondances du réseau ou concentration de flux sur quelques points clés, dépendance énergétique externe de l'infrastructure, etc.

Nous pouvons formuler ici trois remarques que nous approfondirons en 3e partie.

- La notion omniprésente de localisation crée une connexion naturelle avec le Geoint ;
- L'immensité des recherches, et le coût humain qu'elles représentent, induisent une impérieuse nécessité de capitaliser les recherches effectuées, et de partager entre tous les organismes du renseignement les informations recueillies. Le développement d'infrastructures dédiées à cette tâche sera alors nécessaire ;
- L'adhérence opérationnelle du Cyber et de la guerre électronique/ROEM est ici flagrante, notamment dans la dimension physique des vulnérabilités recherchées.

[57] Backbones : il s'agit des serveurs « cœur » du réseau maillé Internet, ceux par lesquels transitent tout le traffic internet d'une région mondiale (à l'échelle de plusieurs pays). Traduit par le terme « épine dorsale interne », un *backbone* est une cible de choix pour un hacker tant en terme de capacité d'écoute, de caractérisation de cible ou d'action malveillante tant la cible stratégique est considérable.

iii) Le « comment » : décrire l'activité numérique

Il s'agira pour le CRAC de caractériser en complément des travaux précédents l'activité numérique de la cible d'intérêt militaire, c'est-à-dire définir et cartographier ses relations. Avec qui échange-t-il numériquement ? Quand ? Quel contenu ? Avec quelle fréquence ? Avec quel protocole de sécurité ? L'empreinte numérique ainsi définie, souvent sous forme de diagramme de mise en relation[58], vise à faciliter l'approche indirecte de la cible notamment par ingénierie sociale[59]. De même, l'approche multicapteurs/multisources nécessaire à cette étude place le CRAC dans une posture d'exploitation et de fusion d'informations, et non plus de simple capteur, aussi complexe techniquement soit-il.

3) De l'intérêt d'une capacité offensive nationale stratégique…

Comme énoncé dans les travaux précédents de structuration à dimension doctrinale du Cyber français, le COMCYBER intègre une **fonction « agir »** qu'il convient ici de démystifier. Cette capacité offre au Cyber le statut à part entière « d'arme » et de capacité opérationnelle Si le débat d'arme de dissuasion pouvait encore exister il y a peu, la stratégie du ministre de la défense est désormais explicite[60] : il s'agit d'une arme conventionnelle, certes atypique et potentiellement dévastatrice à l'échelle d'un groupe de pays.

Outre les fortes restrictions de confidentialité qui nous limiteront ici, la LIO (lutte informatique offensive) vise, selon le LBDSN 2013, à offrir à la France une capacité progressive de réponse par le recours aux moyens coercitifs du ministère de la défense, tant dans les champs physiques traditionnels que dans l'espace numérique : « […] *sans s'interdire l'emploi gradué de moyens relevant du ministère de la défense, si les intérêts stratégiques nationaux étaient menacés.* ». Les effets attendus vont de la simple mise en garde à l'égard d'un agresseur à son entrave, voire la destruction des infrastructures visées. Un cadre de réflexion doctrinal est d'ailleurs en cours de construction et articulé autour de deux termes :

[58] La solution logicielle utilisée est souvent « i2 Analyst's Notebook » d'IBM, et ses nombreuse déclinaisons.
[59] Ingénierie sociale : employé ici dans son assertion de manipulation mentale, psychologique ou de l'esprit dans un but de nuisance. L'exemple le plus classique est l'envoi d'un mail corrompu à une cible en se faisant passer pour un collègue légitime, un chef ou autre, afin de profiter de la naïveté de la victime pour lui soutirer des mots de passe en retour. Il s'agit de la principale méthode d'attaque informatique en termes de volumes de pertes financières engendrées à l'échelle mondiale.
[60] « *Le mode de fonctionnement de la dissuasion nucléaire est profondément différent des batailles Cyber. C'est la raison pour laquelle je rattache plus volontiers, dans nos modes de raisonnement, les problématiques Cyber aux problématiques conventionnelles* » J.Y Le Drian*, op.cit.,* note 08.

riposte et *neutralisation*[61]. Le mode opératoire est détaillé par le ministre de la défense lui-même : « *nous permettre de nous introduire dans les systèmes ou les réseaux de nos ennemis, afin d'y causer des dommages, des interruptions de service ou des neutralisations temporaires ou définitives, justifiées par l'ouverture d'hostilité à notre encontre. En utilisant pour cela des moyens sophistiqués, dont nous sommes parfois les concepteurs et qui doivent résister à tout risque de détournement. C'est aussi un enjeu technologique complexe, mais devenu fondamental* ».

Toutes les composantes constitutives de la LIO sont ici explicitées par le Ministre[62] :

- D'abord, une **conception nationale**, où selon nos travaux précédents, on peut imaginer aisément le rôle de la DGA-MI. Le mot « parfois » utilisé pourrait d'ailleurs sous-entendre l'emploi par la France de moyens d'attaques cyber non nationaux : outils *opensource*, outils LIO d'origine étrangère compromis mais toujours efficace, voir volé à une autre nation, permettant alors de se prémunir subtilement de la problématique d'attribution grâce à l'usage d'une technologie étrangère.
- Une **protection renforcée** des capacités développées, contre le détournement par une rétro-ingénierie potentielle et adverse. Cet impératif du ministre souligne l'intérêt majeur et stratégique de la LIO pour les autorités françaises.
- Un cadre d'action militaire de **réponse graduée**, contre un ennemi Cyber ayant eu l'initiative ayant dévoilé clairement ses intentions. Cette posture conventionnelle est cohérente avec la conception LID de résilience des systèmes français.

On peut par ailleurs se poser la question de savoir si **l'acte de revendication** serait assumé par la France en LIO. A titre d'exemple, les parutions spécialisées en 2015 sur l'existence et la compromission d'un arsenal numérique de cyber-espionnage actif depuis 2009 *(*outils *Casper*[63], *Babar*, *Evil Bunny*…), et attribué potentiellement à la France[64], ont toujours donné lieu à un refus catégorique de commentaires, quels qu'ils soient, des autorités.

[61] Le droit français a été récemment modifié pour permettre des actions de neutralisation, en particulier des effets d'attaques sensibles (article 21 de la LPM du 18 décembre 2013, codifié à l'article 2321-2 du code de la défense).informatiques visant des systèmes d'information particulièrement sensibles (article 21 de la LPM du 18 décembre 2013, codifié à l'article 2321-2 du code de la défense).

[62] Une première mention publique de l'existence d'une capacité LIO a été faite par l'amiral A.Coustillère dès avril 2014. Source : P.Y Bocquet, *La France est-elle prête pour la cyberguerre*, 01Net du 03 avril 2014, p32.

[63] Source : M. Untersinger, *Casper, le logiciel espion cousin de Babar qui surveillait la Syrie*, 05 mars 2015, disponible sur http://www.lemonde.fr/pixels/article/2015/03/05/casper-le-logiciel-espion-cousin-de-babar-qui-surveillait-la-syrie_4586723_4408996.html, Consulté le 08 novembre 2016.

Pour tenter d'**illustrer les capacités réalistes** d'une composante telle que la LIO, intimement liées aux services de renseignement, la compromission en 2012 du programme américain PRISM[65] de la NSA est édifiant : capacité de *Ddos* multiples, écoutes massives et interception de flux gigantesques, outils de traçage comme Xkeyscore[66], nombreux développements de *backdoors* spécifiques, comme l'outil Regin[67], pour orchestrer à la demande l'exfiltration de données numériques isolées et de valeur, attaques de nombreux protocoles de sécurité comme des algorithmes de chiffrement volontairement affaiblis, ou le maintien de failles structurelles dans les VPN, déroutage de flux vers les serveurs de la NSA (détournement BGP[68], détournement de nombreux serveurs de fournisseurs de services américains comme Facebook, Google, Yahoo…), corruption de nœuds Tor… La liste des possibles est impressionnante, et beaucoup d'experts imaginent que cet arsenal, certes non militaire, n'est que la partie émergée de l'iceberg Cyber américain offensif. Une extrapolation semble ainsi tout à fait possible, et raisonnable, pour imaginer ainsi un arsenal LIO français, tant les différents aspects doctrinaux des deux nations se rejoignent.

Ainsi, le Cyber français est en pleine structuration stratégique, afin d'atteindre sous la responsabilité du COMCYBER l'efficacité militaire *full spectre* souhaitée, en anticipation et, fait notable, d'arme de destruction dédiée. Le Geoint, autre domaine du renseignement fortement dual, et né également de la numérisation exponentielle de nos sociétés, semble faire face aux mêmes défis pour tenter d'apporter une réelle plus-value aux opérations militaires.

---

[64] L'attribution formulée de ces outils a été effectuée par des méthodes de profilage indirect: étude des fuseaux horaires de synchronisation des serveurs de communication, détection de sémantique soit-disante française dans les commentaires du code source…L'attribution à la France reste donc une simple hypothèse technique. Source : M. Untersinger, *La ferme des animaux, concepteurs de logiciels espions depuis au moins 2009*, Le Monde, 06 mars 2015, disponible sur http://www.lemonde.fr/pixels/article/2015/03/06/la-ferme-des-animaux-concepteurs-de-logiciels-espions-depuis-au-moins-2009_4588510_4408996.html. Consulté le 08 novembre 2016.

[65] Voir l'analyse de F.B Huyghe, *Cyberespace : le temps de l'après Snowden*, IRIS-Observatoire géostratégique de l'information, Paris, Mars 2014, 20p.

[66] J Lausson, *xkeyscore le programme de la nsa pour suivre chaque internaute à la trace*, Numerama, 1er août 2013, disponible sur http://www.numerama.com/magazine/26655-xkeyscore-le-programme-de-la-nsa-pour-suivre-chaque-internaute-a-la-trace.html. Consulté le 04 octobre 2016.

[67] L.Lagneau, *un logiciel espion très sophistiqué découvert*, blog zone militaire, 25 novembre 2015, disponible sur www.opex360.com/2014/11/25/logiciel-espion-tres-sophistique-decouvert/
et M Marquis-Boire C Guarnieri R Gallagher, *Secret Malware in European Union Attack Linked to U.S. and British Intelligence,* The Intercept, 24 novembre 2014, disponible sur https://theintercept.com/2014/11/24/secret-regin-malware-belgacom-nsa-gchq/. Consulté le 24 octobre 2016.

[68] BGP : *Border Gateway Protocol.* Voir *Détournements BGP, Etat des lieux*, Lettre mensuelle de l'OMC n°36, Décembre 2014.

II. Le Geoint, l'exploitation massive des données au service du décideur

1) L'apport du Geoint à l'évaluation d'une situation

a) Un « nouveau » service de traitement de données géolocalisées à la demande

i) Conceptualisation du Geoint

Les définitions du Geoint sont nombreuses, fait révélateur du bouillonnement intellectuel en vigueur dans cette discipline, à l'instar du Cyber. Pour le besoins de notre étude, nous retiendrons celle du Professeur Philippe Boulanger[69] :

*« Le Geoint est l'abréviation de « GEOspatial INTelligence » que nous traduisons par « **renseignement géospatial » en France. […)** Le terme de Geoint est synonyme de « fusion des données », c'est-à-dire qu'il désigne le processus complexe de **collecte et d'analyse** de tout type d'informations issues de **multiples capteurs** : imagerie spatiale, écoutes électromagnétiques et géolocalisation, renseignement humain, données informatiques et sources ouvertes (médias, rapports, etc.). L'intérêt du Geoint est de disposer d'une **fusion de données en temps quasi réel**, dans une logique d'''**anticipation**, pour apporter une aide à la décision aux autorités militaires et politiques comme un soutien aux opérations.* »

Le Geoint n'est donc en aucun cas une science militaire, l'approche est duale comme pour le Cyber. Les Armées, parties intégrantes de sociétés interconnectées et ultra numérisées, redécouvrent à rebours ce domaine et les opportunités qu'elles pourraient en tirer en termes d'anticipation et de connaissance au profit des opérations. Le Geoint s'intéresse en effet à l'exploitation et la fusion d'informations multisources géolocalisées, de formats d'origine très hétérogènes, produites par des systèmes connectés (senseurs) dédiés ou non. Le but du Geoint est de dégager des éléments de compréhension des dynamiques en jeu, spatialisées et territorialisées, d'où son rapprochement avec les sciences géographiques (physiques et humaines). Il est de plus capable d'offrir une précision et un détail sur n'importe quelle

[69] Propos de P.Boulanger interviewé par J.Guisnel, *En France, le renseignement géospatial a 20 ans de retard*, Le point du 22 septembre 2015. P. Boulanger est professeur des universités à l'Institut français de géopolitique (université Paris-VIII). Disponible sur http://www.lepoint.fr/editos-du-point/jean-guisnel/philippe-boulanger-en-france-le-renseignement-geospatial-a-20-ans-de-retard-22-09-2015-1966874_53.php, consulté le 20 octobre 2016.

donnée (par corrélation, association, recherche immédiate etc…), en fournissant des images de synthèses aisément exploitables par un décideur, militaire ou non.

Figure 1: Exemple de contribution à l'élaboration d'un produit Geoint.

Source : http://www.mta.ro/Geoint/about.html

Notons bien que la fonction « fusion des données » (collecte, traitement et mise à disposition) **n'est pas nouvelle**[70] dans les Armées françaises. Seules les nouvelles capacités offertes par les NTIC suscitent le nouveau dynamisme observé depuis plusieurs années. Elle était une tâche spécifique du poste IKM (*Informationl Knowledge Management*) dans un PC opératif par exemple, mais les doctrines opératives et stratégiques en vigueur actuellement ne la différencie plus au sein de la fonction IMC (*Info Management Center*). Par ailleurs, en Afghanistan, au sein de la *TaskForce* française Lafayette, une *Fusion Cell* était déployée et dédiée à certaines tâches de renseignement lié au *targeting des JPEL*[71].

La particularité du Geoint, pour notre étude, est de **placer la notion de données géolocalisées** au cœur de la réflexion. Mais les problématiques suivantes sont aussi incluses : utilisation et gestion de capteurs multiples, accès aux données produites, stockage, diffusion des produits et constitution de bibliothèque de connaissances, définition nécessaire d'entités coordinatrices légitimes…. Nombre de ces aspects identifient déjà **des sous-systèmes critiques** du Geoint dont l'intérêt Cyber évident constituera une piste de nos réflexions en 3e partie.

[70] Le Général de brigade aérienne J.D Testé, commandant interarmées de l'espace (CIE), explique que « *Napoléon faisait du Geoint à sa manière* ». Source : Colloque Geoint, *Révolution technologique, représentation spatiale et analyse géopolitique, en partenariat avec le département de géographie de l'Ecole normale supérieure-Ulm, Airbus Defense and Space*, sous la direction de P. Boulanger, Paris, 11 et 12 Septembre 2015.

[71] JPEL : *Joint priority effective list*. « *L'exemple de la Task force La Fayette, engagée en Afghanistan, met en relief l'importance d'une cellule de son centre des opérations en charge de [la] coordination (entre autres missions) : la Fusion Cell*. ». Source : CNE L. de LINGUA de SAINT BLANQUAT, « mission capturer », Pensées-Militaires, CDEC, Paris. Disponible sur http://www.penseemiliterre.fr/mission-capturer_2013600.html. Consulté le 12 octobre 2016.

Figure 2: Illustration de l'aspect multisources et transverse du Geoint. Source : geo4i, disponible sur http://geo4i.com/wp-content/uploads/2014/01/Capture.jpg.

ii) Les données de masse

Une donnée de masse, matière première du Geoint, peut prendre deux formes génériques : le mode matriciel ou **raster** [72](l'image) et le mode vectoriel ou **vecteur**[73]. Il est reconnu que le traitement de ces deux type de données diffèrent largement, et ne font pas appel aux même outils, ni aux mêmes compétences. Le traitement des rasters et des données qu'ils contiennent est en effet complexe et réclame des outils spécialisés. C'est pourquoi dans une majorité de cas ils ne servent que de support à des couches vectorielles. *A contrario*, les données vectorielles sont plus simples à manipuler, notamment à des fins d'analyse.[74].

iii) Les principes clés de la géolocalisation

La donnée d'intérêt pour le Geoint a une propriété exclusive : elle est **géolocalisée**, ou **géolocalisable** indirectement. Les méthodes techniques de localisation sont aussi nombreuses qu'il y a de moyens de produire de l'information, il serait donc vain de les répertorier de manière exhaustive. Retenons toutefois une catégorisation en 2 principes de base :

- Une **localisation directe,** tel un relevé de position effectué par le capteur lui-même et associé à la donnée, type position GPS (localisation satellite). Le

[72] Raster : Données images où l'espace est divisé de manière régulière, comme les pixels. A ces derniers sont associées une ou plusieurs valeurs décrivant les caractéristiques de l'espace. Source : http://www.portailsig.org/content/qu-est-ce-qu-un-raster.

[73] Vecteur : Le format vectoriel utilise le concept d'objets géométriques (points, lignes, polygones) pour représenter les entités géographiques. Ces objets sont définis par leurs coordonnées dans un système de projection. *Ibid.*

[74] Source : http://www.ente-aix.fr/documents/118-demoGeo/demo/4_BasesIG/co/20_gr_PubliRasterVecteur.html, consulté le 25 novembre 2016.

relevé de position peut être intentionnel (option du capteur utilisé) mai, plus pernicieux, peut aussi être lié à la technologie employée et indépendante de l'utilisateur. Par exemple, la trame technique d'une communication *Thuraya* intègre le positionnement GPS du boitier utilisé.

- Une **méthode indirecte,** intrinsèquement liée à la technologie de diffusion de la donnée collectée par le capteur : par réseau GSM (méthode du *Time advance*[75] sur une BTS, ou triangulation selon la puissance des signaux des BTS perçues), par réseau Wifi (exploitation des cartographies de routeurs Wifi connus par leurs adresses Mac, bases de données disponibles grâce au *War Driving*, ou IP[76] ou RFID en intérieur), fonctionnant toujours sur le même principe de triangulation, ou radiogoniométrie, un des fondamentaux de la guerre électronique.

Mais il existe une constante dans ces deux cas : c'est bien la position géographique du capteur qui sera associée à la donnée collectée, en aucun cas celle de la cible traitée. Il faudra donc en extrapoler le géoréférencement pour pouvoir associer l'information et sa localisation.

iv) Les produits exploitables du Geoint

La qualité essentielle du Geoint est de proposer des visualisations synthétiques, exclusivement fondées sur l'image, faciles à interpréter pour le décideur. L'intérêt pour le chef militaire est en effet de se consacrer à sa seule appréciation de situation pour acquérir sa légitime certitude afin d'agir. La facilité d'accès de la carte ou de l'image comme produit de synthèse est de ce point de vue indéniable[77], ce que le Cyber ne pourra jamais concurrencer.

Il existe de multiples produits de synthèse élaborés à partie de données géo-référencées[78] : cartes (un produit qui délimite, à l'aide de symboles et de texte, l'emplacement d'objets spécifiques sur le terrain), graphiques codifiés, imagerie (raster, ROIM, radar

[75] *Time advance*, ou différence de temps observée ou EOTD (*enhanced-observed timed difference*) : le terminal calcule le temps écoulé entre l'émission et la réception de la requête envoyée à l'antenne, il peut alors estimer sa distance par rapport à celle-ci ce qui donne une position relative par rapport à l'antenne BTS. Celle-ci couvrant généralement un secteur de 120°, on obtient alors un croissant de localisation probable. Par triangulation sur 3 BTS perçues, on obtient par recoupement le positionnement plus ou moins précis selon le maillage du réseau GSM déployé.

[76] La localisation par IP n'est pas des plus précises : « *Lorsque l'adresse IP de l'utilisateur est chargée sur un serveur proxy qui n'expose pas l'adresse IP de l'utilisateur, il est pratiquement impossible de localiser physiquement l'utilisateur. Certaines estimations placent la précision du pays à environ 99%. Pour les adresses IP aux États-Unis, elle est à 90% exacte au niveau de l'État et estimée à 81% exacte dans un rayon de 25 miles. Dans beaucoup d'autres pays, la précision n'atteint qu'un taux de 55% de précision dans un rayon de 25 km* » source : https://www.e-education.psu.edu/geog479/node/557 consulté le 02 décembre 2016.

[77] En application du vieil adage populaire attribué à Confucius : "*une image vaut mieux que mille mots*".

[78] Voir les exemples possibles de produits commerciaux Geoint en annexe 4.

LIDAR[79] ou SAR[80], images orthophotographiques[81], etc. Il existe aussi, numérisation oblige, les fichiers digitaux tridimensionnels (3D) avec des apports possibles issus des technologies de réalité augmentée, mais aussi 4D grâce à l'intégration des facteurs temps et mouvements. Ces deux derniers domaines ouvrent d'ailleurs la voie à la simulation dynamique opérationnelle[82].

v) Le Geoint ou la géographie ?

La notion de localisation ou de géoréférencement, couplée à l'étude des acteurs en charge du Geoint notamment en France, peuvent aisément porter à confusion entre la géographie et le *Geospatial Intelligence*.[83]

Une étude simple des définitions n'aide finalement pas à lever les doutes. La géographie se définit en effet comme une science qui a pour objet **la description et l'explication** de l'aspect actuel, naturel et humain, **de la surface** de la Terre[84]. Si nous prenons le Geoint sous son simple aspect « géospatial », la définition supra fonctionne. De même si nous prenons les produits cartographiques fournis par les deux disciplines…

En restreignant le problème au domaine militaire, la géographie est un élément incontournable des activités militaires et de la stratégie des Etats. Elle est « *plus qu'un savoir stratégique. Elle constitue une manière de penser l'espace depuis les origines de la guerre. Longtemps, ce sont les stratèges qui y font référence dans leurs traités de tactique ou de stratégie, comme Frontin, Napoléon, Clausewitz et d'autres .[…] Se préparer à la guerre, aussi bien à la lutte contre d'autres appareils d'Etat, qu'à la lutte intérieure contre ceux qui*

[79] Lidar : détection par laser. Voir les applications LIDAR dans *Geospatial Information Science*, Vol. 4, 2001, No 1, pp. 37-42.

[80] SAR *: Synthetic Aperture Radar*, ou radar à synthèse d'ouverture. Comme le laser, l'imagerie SAR permet de différencier la nature des « objets » présents par étude comparative des propriétés de l'onde radar réfléchie.

[81] Photographie globale reconstituée par de multiples clichés et corrigée en perspective pour représenter une vue verticale de la zone couverte par le senseur.

[82] Une des illustrations est le programme français SCORPI0N. Voir à ce propos la présentation exhaustive de H. BUENAVIDA, *la simulation opérationnelle au profit de l'armée de Terre,* CDEC disponible sur http://www.penseemiliterre.fr/la-simulation-operationnelle-au-profit-de-l-armee-de-terre_2013663.html.

[83] Pour illustrer cette confusion doctrinale entre ces deux domaines, voir l'article *Afghanistan : le détachement géographique de la Task Force La Fayette*, EMA, 21 Avril 2010 disponible sur http://www.defense.gouv.fr/terre/actu-terre/archives/afghanistan-le-detachement-geographique-de-la-task-force-la-fayette. Consulté le 7 décembre 2016.

[84] Définition du Larousse

*mettent en cause le pouvoir ou veulent s'en emparer, **c'est organiser l'espace** de façon à y pouvoir agir le plus efficacement* »[85].

Sur ce point, les travaux d'A.LIEGE[86] sont très pertinents. Si paradoxalement l'avènement du numérique aurait pu tuer la géographie traditionnelle dans les années 90, avec l'apparition de l'imagerie ou de la 3D, c'est bien dans la fusion et l'exploitation des données numériques géolocalisées que réside la relation forte entre la géographie et le Geoint.

A l'ère de l'explosion des données et la logique du temps réel, la géographie ne peut pas tout suivre et synthétiser, ce que le Geoint permet quant à lui et en théorie par ses capacités de fusionnement et de maîtrise de l'information[87] De fait, « *la Géographie devient de façon croissante le « carburant » indispensable aux systèmes de commandement, aux systèmes d'armes et à toute décision politique ou militaire. Elle est également incontournable dans son rôle de référence commune pour le renseignement, la planification, la conduite et l'exécution des différentes missions confiées aux forces et de tout élément d'aide à la décision.»* L'étude menée sur les conséquences géostratégiques des opérations *Desert Storm* et *Iraqi Freedom en Irak* offre une grille de lecture pour appréhender le rôle du Geoint. Fonction alors balbutiante, et entendue comme *« Géographie militaire moderne »,* les travaux démontrent l'impact des études géographiques de terrain sur les choix opérationnels effectués par les Américains : étude et caractérisation des enjeux constitués par les zones humides, le positionnement et l'écosystème des puits de pétrole, problématique de l'accès à l'eau, cartographie ethnique et religieuse… autant de thèmes qui, **par superposition et corrélations multiples,** permettent de comprendre le comportement humain sur l'espace géographique concerné (on pourrait alors aisément parler de géopolitique) et tenter d'expliquer objectivement nombre de comportements belliqueux transfrontaliers auquel le conflit étudié est inexorablement lié. Le nier serait un non-sens stratégique majeur.

[85] P. Boulanger, 2002.

[86] A. Liège, *De l'action militaire à l'après-guerre, une gestion toujours conflictuelle de l'espace : L'exemple des guerres du Golfe,* Revue Géographique de l'Est,, vol. 51 / 1-2 | 2011, mis en ligne le 19 décembre 2011, consulté le 14 octobre 2016. http://rge.revues.org/3280, pages 2 à 4.

[87] Selon le plan prospectif à 30 ans de la DGA, pour la stratégie française, le « commandement et la maîtrise de l'information » fait partie d'une des 5 capacités majeures à détenir, http://www.ixarm.com/PP30-Le-plan-prospectif-a-30-ans,4074, document d'entrée A-1 page 22 et A-2 page 50

Notons enfin qu'en France, la géographie militaire, au niveau opératif et stratégique, est bien une composante du J3, et est gérée en France par l'Etablissement Géographique Interarmées (EGI)[88]. Le Geoint est *a contrario* une composante de la DRM, donc du J2.

b) La transformation de données géolocalisées en renseignement ciblé

i) Les Systèmes d'Information Géographique (SIG), plateforme du Geoint

L'enjeu du Geoint résidant avant tout dans le mécanisme du traitement de masse de données, l'emploi de systèmes d'informations géographiques (SIG) parait fondamental. Il s'agit d'un ensemble apte à identifier, associer, fusionner et exploiter les données géolocalisées afin de fournir un renseignement valorisé et géoréférencé. Un SIG est constitué schématiquement de 5 grands éléments structurants :

- **Le matériel/*Hardware*** : les SIG fonctionnent sur tout type d'ordinateurs, du plus simple à la ferme de serveurs interconnectés. Le rendement de la capacité sera donc directement lié à la performance et au coût consenti pour l'infrastructure.
- **Les logiciels/*software*** : ils permettent de stocker, analyser et afficher toutes les informations collectées. Ils sont composés des outils pour manipuler les données, un système de gestion de base de données, les outils géographiques de requête et d'analyse et surtout de visualisation, via une interface graphique utilisateur (GUI[89]).
- **Les données/*data*** : géolocalisées, elles sont le cœur des SIG. Protéiformes, (images, tables attributaires, données de modélisation de surface, mesures de géomètre), elles peuvent être constituées par le détenteur du SIG par des senseurs dédiés, ou acquises auprès de fournisseurs de données spécialisés (*dataprovider*).
- **L'opérateur** : un SIG étant un outil, c'est dans la virtuosité de l'opérateur que réside l'aptitude à en exploiter toute la puissance pour obtenir les synthèses pertinentes.
- **Les méthodes** : comme tout système global, et compte tenu de l'immensité du champ des possibles, l'exploitation d'un SIG est intimement tributaire du développement de processus normatifs.

[88] EGI : Créé le 1er juillet 2008, l'EGI succède à l'établissement de production de données géographique (EPDG) de Creil et à la section géographique militaire (SGM) de l'armée de terre de Vincennes. Organisme interarmées, l'EGI relève du CEMA. Il entretient d'étroites relations avec l'institut géographique national (IGN). L'EGI produit et diffuse les informations géographiques aéroterrestres, numériques et papier, au profit du ministère de la défense. Il s'appuie sur l'imagerie spatiale pour la production de données cartographiques, d'images ortho-rectifiées ou de modèles numériques de terrain pour la planification et à la conduite des opérations. L'EGI est le pôle d'expertise technico-opérationnelle dans le domaine de la géographie aéroterrestre.

[89] GUI : *graphical user interface*, interface graphique par laquelle l'opérateur humain interagit avec un logiciel au niveau de la couche 7 du modèle OSI.

Relevons ici la position ultra-dominante du SIG ArcGIS[90] de la société américaine ESRI - *Environmental Systems Research Institute*, qui équipe notamment l'OTAN[91] et le NGA américain[92], ainsi que le développement de la solution libre QGIS[93]. Ainsi, face à l'ultradominance d'opérateurs civils, qui plus est étrangers, il parait pertinent de se demander si un organisme aussi sensible que la DRM possède ou non son propre SIG unifié.

Trois remarques consécutives à cette « vision système » peuvent ici être formulées :

- Comment déterminer si le besoin spécialisé des Armées peut être couvert par des outils majoritairement issus du monde industriel et civil ? L'intérêt de développements propriétaires et confidentiels peut en effet sembler pertinent, comme pour la veille numérique en Cyber.
- Comme le CRAC, la sécurité de l'opérateur Geoint sera essentielle, notamment lors des consultations des entrepôts externes de données (*Data Warehouse*). Cette situation implique en effet l'interconnexion du renseignement militaire aux opérateurs civils internationaux et impose la mise en œuvre de protections d'anonymisation coûteuses et technologiquement complexes.
- Tout comme le cyber, la problématique de la diffusion de l'information Geoint entre le niveau stratégique et les niveaux opératifs et tactiques est très prégnante, et conditionne totalement la réelle plus-value opérationnelle de cette discipline.

ii) Une communauté Geoint internationale duale en plein essor

Il existe un autre parallèle entre le Cyber et le Geoint ; **le rôle moteur des multiples acteurs industriels et universitaires civils**. Pour s'en convaincre, il suffit d'observer le dynamisme la communauté Geoint rayonnant à l'échelle mondiale par l'organisation notamment de symposium annuels : *« la révolution Geoint* » de 2016 a « *réuni plus de 3500*

[90] ArcGIS : solution SIG commercialisée en France par la société américaine ESRI. Source et documentation disponible sur http://www.esrifrance.fr/arcgis.aspx.

[91] Source : communication de ESRI, disponible sur http://www.esrifrance.fr/rp/CP_NATO/CP_NATO.htm; consulté le 14 janvier 2016.

[92] Source : communication d'ESRI, disponible sur http://www.esri.com/news/releases/10_3qtr/esri-nga.html du 12 juillet 2010. et brochure commerciale *GIS for Defense and Intelligence*, p. 15, *Esri*, 2005 et amendée l e05 décembre 2010, disponible sur www.esri.com/library/brochures/pdfs/gis-for-defense.pdf.

[93] QGIS : SIG libre et *opensource* distribué sous licence publique générale GNU, développé par une communauté de passionnés. C'est un projet officiel de la fondation *Open Source Geospatial* (OSGeo). Il est compatible avec Linux, Unix, Mac OS X, Windows et Android et intègre de nombreux formats vecteur, raster, base de données et fonctionnalités. Source : https://www.qgis.org/fr/site/

participants et 265 organisations […] ainsi que 19 pays»[94]. Ce symposium, unique par sa dimension et sa capacité d'échanges, véritable *think tank* du domaine, est organisé par le lobbyiste attitré du Geoint américain : l'**USGIF**[95] (*United States Geospatial Intelligence Foundation*). Il s'agit d'une fondation créée en 2004 et regroupant les universités et industriels du domaine. La vocation de ce salon mondial est d'ailleurs très explicite : « *influencer la communauté Geoint, tandis que l'intelligence géospatiale joue un rôle croissant, depuis l'IoT*[96] *et la réalité augmentée jusqu'à la technologie mobile et l'analyse des données* »[97]. Toutes les capacités industrielles du domaine y sont rassemblées : fabricants de charges utiles (capteurs et senseurs, de plateformes satellites, analystes de données, développeurs de SIG et des services de conseil et fournisseurs de matériel.

La communauté militaire n'est pas en reste en termes de représentation, mais la posture choisie semble encore de second rang. Cependant, les liens USGIF-NGA traduisent plus concrètement la réelle implication militaire[98].

c) Le Geoint en gestion de crise : les besoins militaires déjà couverts

La gestion de crise est une application civile du Geoint reconnue et en pleine croissance. En effet, suite à une catastrophe majeure (séisme, éboulement majeur, inondations ou rupture d'un barrage en amont[99] d'une ville, explosions de sites industriels, accidents majeurs de métro, attentats multiples…), le Geoint permet aux services de secours de combiner efficacement :

---

[94] Source : http://usgif.org/events/Geoint-symposia. Pour la partie spécifique Geoint 2016 Symposium, voir http://Geoint2016.com/

[95] Source : http://www.usgif.org/

[96] L'Idate (Institut de l'audiovisuel et des télécommunications en Europe) estime « *qu'il y aurait début 2017 15 milliards d'objet connectés à internet contre 4 milliards seulement en 2010. D'après une étude menée par Gartner et l'Idate en 2020 on peut estimer que le nombre d'objets connectés en circulation à travers le monde s'élèvera entre 50 et 80 milliards. En clair chaque personne détiendra environ 6 objets connectés. Rien que pour 2018, on estime à 6 milliards (cabinet Gartner) le volume de nouveaux objets connectés qui seraient mis en circulation à partir de 2018* ». Source : L David, *Quelle place pour les objets connectés dans notre société ?*, magazine obejetconnecte.net, 24 janvier 2017, disponible sur http://www.objetconnecte.net/objets-connectes-chiffres-etudes-2401/. Consulté le 24 janvier 2017.

[97] Source : http://www.usgif.org/

[98] Voir développement partie II/2

[99] La division plan (J5) de l'Etat-major à USCENTCOM a élaboré de multiples études sur l'impact de la rupture du barrage de retenue d'eau au Nord de Mossoul en Irak, pouvant jeter des millions de personnes sur les routes en quelques heures sur l'ensemble de la vallée du Tigre jusqu'à Bagdad inclus, force de la coalition incluse. La coordination des secours était alors considérée comme un enjeu stratégique dans un pays en guerre contre le terrorisme de l'ISIL. Voir l'article *En Irak, un barrage menacé de rupture complique l'offensive vers Mossoul,* l'Express, AFP, 10 février 2016, disponible sur http://www.lexpress.fr/actualites/1/monde/en-irak-un-barrage-menace-de-rupture-complique-l-offensive-vers-mossoul_1762377.html.

- l'étude terrain de la nouvelle situation,
- l'élaboration de scénarii d'intervention (identification des axes de pénétration potentiels ou interdits, étude des flux de population, localisation des zones de danger),
- l'évaluation précise des dommages (le *BDA*[100])

Selon cette étude, *« plus de 90% des données opérationnelles nécessaires à un PC d'urgence sont liées aux localisations géographiques, rendant le SIG indispensable pour élaborer une réponse rapide de sauvetage* ». Le Geoint constitue finalement une aide à la décision très pertinente, permettant aux autorités de définir dans l'urgence la priorisation et l'affectation des ressources rares en moyens de secours. C'est donc bien **un outil d'action au service de la sécurité civile**, et se définira alors comme un **appui direct aux opérations** de secours. La similitude avec une opération militaire n'est alors pas difficile à extrapoler, nous autorisant ainsi à parler d'application duale dans un tel contexte. Enfin, illustrant l'intérêt du Geoint pour les forces, le CSUE, centre satellitaire de l'Union Européenne, localisé à *Torrejón de Ardoz* (Espagne) et dirigé un officier général français, assure depuis 1993 cette mission au sein de l'Europe[101].

Pour les besoins de notre étude, et parmi les nombreux travaux Geoint existants sur le marché, nous retiendrons ceux de l'académie des sciences bulgares[102], visant à convaincre les organismes de secours de l'utilité d'exploiter la carte d'image en réalité augmentée[103] comme plateforme de gestion globale des urgences lors d'une intervention. S'appuyant sur la Chine, cette étude soulève en effet **les enjeux d'un Geoint « temps-réel »** par deux observations :

- La croissance fulgurante de la Chine modifie continuellement le paysage urbain, rendant obsolète toute tentative de cartographie non dynamique. A titre d'exemple « *40% de la cartographie d'une mégalopole comme Beijing change tous les ans* »[104]. Cela concerne les hauteurs des bâtiments, les zones de stockage logistiques, les positions des casernes de

[100] BDA : *Battle dommage assessment,* évaluation des dommages permettant notamment d'estimer rapidement soit l'attrition d'une force ennemie sur un combat, soit d'évaluer la nature des forces de secours à faire intervenir sur une crise humanitaire par exemple.

[101] Source : https://www.satcen.europa.eu/, consulté le 14 mars 2017. Le directeur de CSUE est depuis 2015 le général de brigade aérienne Pascal LEGAI.

[102] L. Ming P.Y Fang, *Visualization Emergency Research Based on Mobile Mapping Technology. Cybernetics and Information Technologies*, Journal of Institute of Information and Communication Technologies of Bulgarian Academy of Sciences, 2015, vol. 15, no 6, p. 204-218.

[103] La réalité augmentée propose d'incruster dynamiquement sur une image ou vidéo des données infocentrées de tout type (texte, chiffres, liens), permettant d'informer de façon complémentaire l'opérateur sur ce qu'il voit. Voir l'exemple d'illustration du programme Scorpion, H. BUENAVIDA, *op.cit.* (note 92.)

[104] L. Ming PY Fang, *op.cit.,* p 205

police/pompiers et donc leurs capacités d'intervention, les capacités des hôpitaux, les plans de circulation, les affectations et activités réelles des lieux publics… Autant de données qui impactent directement l'organisation du terrain et donc la priorisation des secours à réaliser

- Fort logiquement, en cas de crise, il sera nécessaire de reconstruire dans l'urgence (le *tempo des opérations*) un nouveau référentiel géographique que seul le Geoint pourra réaliser grâce à ses algorithmes de fusion de données de masse.

Ainsi, grâce à la collecte et la fusion en temps réel de l'ensemble des données à jour (ou les plus récentes possibles) détenues et partagées pour l'occasion par l'ensemble des services compétents (secours, mairie, institutions civiles et militaires…) et des capteurs déployés (drones Geoint[105], photographies satellites, suivi de flux RSN…) le SIG du PC d'urgence pourra proposer aux décideurs les plans détaillés des zones où la nécessité d'intervention sera caractérisée, présentera les zones à risques sanitaires élevés, les axes d'approche recommandés et compatibles avec les gabarits des engins de secours (volumétrie, tonnage)… La solution Geoint propose même une modélisation 3D des zones d'intervention (stéréoscopie, insertion de réalité augmentée) permettant aux forces de sécurité de s'immerger numériquement dans les structures-terrain, et valider depuis le PC le séquencement de l'intervention avant sa phase de déploiement.

Notons enfin que cette étude d'application du Geoint n'est pas un cas isolé en France : le ministère des affaires étrangères, ainsi que les services de Police de la Préfecture de Paris, ou encore la Gendarmerie Nationale y travaillent, cette dernière à travers le système SC2 (Système de Coordination de Crise)[106], système d'aide à la décision pour les personnels en charge de la planification et de la conduite des opérations de secours. Il permet d'élaborer des conceptions de manœuvres (COA – *course of action*) adaptées selon la configuration réelle, instantanée et évolutive de la zone d'intervention, perturbée par l'évènement déclencheur de la crise. D'autres organismes en charge de la coordination des secours, notamment les CO de crise des Préfectures, se dotent progressivement de solutions Geoint pour les aider dans leurs

[105] Les travaux de recherche pour intégrer des charges Geoint sur des drones sont déjà en cours aux Etats-Unis, prouvant l'intérêt toujours croissant de cette discipline et le besoin immense en données à jour. Source : TTU, *un Reaper Geoint*, TTU 973 du 15 avril 2015.

[106] « *Le POD senseur, embarqué sur un hélicoptère de la Gendarmerie, permet d'élaborer des cartes à partir de photos géo référencées (localisation et inclinaison de l'appareil) et de pouvoir les comparer à la demande pour suivre l'évolution de la crise suivie »* propos du LCL Thibaut LUCAZEAU du Centre de planification et de gestion de crise . Le SC2 « *peut couvrir des zones jusqu'à 200km² avec une résolution de 1 pixel = 20 cm. […] Le document produit au retour de l'engin est une image orthophotographique, la mise à l'échelle rigoureuse étant possible grâce aux relevés GPS* », *id.* Ce projet a reçu le prix de l'Audace 2016 de la Gendarmerie Nationale.

travaux afin de gérer le flux d'informations et aider autant que possible à prendre les moins mauvaises décisions

Face à ces illustrations, il reste encore de nombreux défis à relever : comment unifier tous les moyens concourants au Geoint pour améliorer l'efficacité globale? Comment partager efficacement les données nécessaires à tous les systèmes, les mettre à jour et les exploiter? L'étude de la communauté Geoint américaine est de ce point de vue très instructif.

2) 15 ans de Geoint américain : un exemple à suivre?

Comme le soulignait déjà P. Boulanger[107] « *aux États-Unis, seul pays à disposer d'une véritable doctrine en la matière, le Geoint s'est renforcé après les attentats du 11 septembre 2001. La* National Geospatial Agency, *créée en 2003, est au cœur de cette activité pour obtenir une information géolocalisée grâce aux satellites, puis fusionnée avec d'autres informations comme des écoutes, des sources ouvertes (Internet) ou des sources humaines*. »

a) La NGA, l'influence géopolitique du Geoint mondial

La *National Geospatial-Intelligence Agency* est **la tête de chaîne du Geoint** aux Etats-Unis. Basée à Springfiled en Virginie, elle est dirigé par M Robert Cardillo. La fonction du directeur du NGA est centrale et extrêmement influente: en plus d'être le directeur fonctionnel de Geoint, il reçoit en effet ses orientations directement des plus hautes instances du pays : le *DoD* pour la parte Défense, le Directeur du *National Intelligence* (*DNI*) pour la partie renseignement et le Congrès américain.[108]. Mais dans la sphère du Geoint, il est aussi :

- le chef du **système national d'intelligence géospatial** *(National Systems for Geospatial Intelligence* - **NSG[109]),** véritable coordinateur et fédérateur national des contributions Geoint. En forçant le trait, cette instance joue quasiment le rôle d'autorité normative[110] du domaine, dont on peut ainsi mesurer la puissance d'influence stratégique.

[107] Propos de P.Boulanger interviewé par J.Guisnel,, 2015, *op.cit.* (note 69)
[108] Source : https://www.nga.mil/About/Pages/Default.aspx
[109] Le NSG se définit comme "*the combination of technology, policies, capabilities, doctrine, activities, people, data, and communities necessary to produce geospatial intelligence in an integrated multi-intelligence, multi-domain environment*. Source: *NSG Statement of Strategic Intent*, Mars 2007. Voir annexe 6.
[110] Les nombreux travaux de réflexions de groupes de travail GWG disponibles sur http://www.gwg.nga.mil/guide.php, consulté en décembre 2015 et janvier 2016. Pour les travaux de normes, voir les publications regroupées dans l'annexe 7 « Geoint Standards »

- le coordinateur du **système allié global pour l'intelligence géospatiale** (*Allied System for Geoint*), ce qui lui confère aussi un pouvoir d'influence à portée internationale au sein notamment des sphères décisionnelles militaires (comme l'OTAN par exemple).

Rappelons utilement que la structure défense/renseignement des Etats-Unis est bien différente de celle de la France, assumant notamment une forte imbrication avec les acteurs sécuritaires et civils. Ainsi, la « *NGA fournit des renseignements en appui des objectifs de sécurité nationale américains. Agence à la fois de renseignement et d'appui aux opérations militaires, la NGA est donc mandatée pour participer à la préparation opérationnelle des forces militaires américaines. A vocation fortement duale, la NGA contribue également à des missions humanitaires (suivi des inondations ou des incendies), ainsi que dans les opérations de maintien de la paix* ».[111].

En charge du Geoint, la NGA a enfin une véritable influence sur l'ensemble de la communauté mondiale. A ce titre, elle identifie et anticipe les besoins futurs de ses partenaires au sein de l'USIC[112] et assure un rôle moteur dans la prospective et le développement du Geoint américain. En forçant volontairement le trait, il s'agit d'une sorte de DARPA (*Defense Advanced Research Projects Agency*, à la devise «*Creating Breakthrough Technologies For National Security* » évocatrice, ou la rupture technologique permanente[113] au profit de la supériorité stratégique des Etats-Unis dévolue à la « *révolution Geoint* »[114].

b) Geoint : capacité de synthèse au cœur de l'*US- IntelCommunauty*

De même qu'en Cyber, la doctrine américaine du Geoint de 2012, la *Joint Publication 2-03*, est en accès libre[115], mais elle complète une première version de 2006 fort instructive[116]. Le Geoint est en effet un **appui aux opérations** (et non une composante de renseignement) qui fournit à la demande les synthèses souhaitées. Ces productions sont identifiées soit

[111] Source : https://www.nga.mil/

[112] USIC : *United States Intelligence Community.* Voir annexe 5 dédiée

[113] J. Henrotin*, La technologie militaire en question – le cas américain*, Economica, 2008, 300p.

[114] Source : http://geoint2016.com/news/775-Geoint-2016-embraces-the-Geoint-revolution

[115] Joint Publication 2-03*, Geospatial INtellignece in Joint Operations*, Dod, 31 octobre 2012, 137 pages. Pour l'intérêt d'une parution non classifiée, voir commentaire note 30.

[116]Document intitulé *National System for Geospatial Intelligence – Geospatial Intelligence (Geoint) Basic doctrine Publication 1-0,* cette doctrine âgée de 11 ans désormais pose les fondamentaux de la discipline aux Etats-Unis, qui semblent bien être la base de référence de l'Armée Française pour son organisation contemporaine en 2017. Disponible sur https://fas.org/irp/agency/nga/doctrine.pdf, téléchargée le 17 novembre 2016

comme base de référence[117], soit en contribution à un travail commun pour n'importe quelle opération et au profit de chaque membre de l'US-IC. Le Geoint est donc considéré *as a service*, mais sa dimension de référence potentielle en fait bien un échelon de synthèse et d'exploitation à part entière. Il faut cependant préciser ici que la NGA ne procède pas à des interceptions (mission spécifique de la NSA), se distinguant ici notoirement par son modèle du Geoint français.

Les produits Geoint sont fabriqués à partir d'une grande variété de systèmes et de capacités appartenant à toute la communauté renseignement américaine, militaire ou non. **La description des multiples systèmes de collecte de données** (*data collection systems*) renforce encore davantage le constat de la très forte dualité native du Geoint américain, la logique « tous capteur » étant poussée à l'extrême dans la parfaite philosophie de l'US-IC.

Le rôle de la société américaine dans son ensemble se situe donc bien dans la collecte tout azimut des données. La NGA est alors positionné comme pilote du domaine, coordinateur de la fusion et de la production des synthèses. Cette approche interservices, interarmées, et inter-domaines sous-entend la mise en œuvre de procédures unifiées (rôle du NSG), de systèmes de gestion des données centralisés, interopérables ou uniques, et de réflexion doctrinales d'ensembles pour assurer un tout cohérent. A l'échelle d'une fédération comme les Etats-Unis, ce travail d'harmonisation peut légitimement forcer l'admiration…

Soulignons pour finir les travaux de réflexions de l'IC-ITE - *Intelligence Community Information Technology Enterprise Strategy*[118] et les publications du JIE – *Joint Information Environment*[119]. Dans le cadre toujours plus poussé et stratégique de l'intégration des acteurs civils sur la problématique de défense nationale typiquement américaine, le JIE101 définit une plateforme informatique commune aux 16 agences de l'*IC*, interopérables avec l'ensemble des systèmes informatiques des acteurs économiques majeurs US civils. Ce projet nous

[117] La SITREF, où situation de référence, est pour un PC français un travail collaboratif entier et essentiel à l'initialisation d'une campagne. Il semble que le Geoint ait une place de choix pour ce travail aux Etats-Unis.

[118] J.R. Clapper, DNI, explicite la stratégie duale de l'IC-ITE : « *We protect the homeland by providing critical information […] from the White House to the foxhole. We enable our customers to make informed critical policy decisions across the spectrum of our national interests, in a rapidly shifting international security landscape. The core function of ODNI is intelligence integration; everything else we do revolves around, supports, and enables that function. Successful integration requires a global IT infrastructure through which the IC can rapidly and reliably share intelligence with those who need it* » Source : Intelligence Community Information Technology Enterprise 2012-2017, Leading Intelligence Integration, 2012, 20p, p2

[119] JIE 101, *Enabling the Joint Information Environment - Shaping the Enterprise for the conflicts of Tomorrow,* DISA – Defense Information Systems Agency, 5 mai 2014, 28 pages.

intéresse ici en tant que facteur facilitant le traitement de sujets transverses propres au Geoint, démultiplicateurs de puissance dont on peut mesurer humblement l'ambition…

En synthèse, il est évident que le Geoint - au service de l'anticipation opérationnelle – est une réalité totalement maitrisée par les Etats-Unis depuis plus d'une décade. En cela, nous retrouvons un autre point commun avec le monde du Cyber… Mais l'influence majeure du NGA au sein de l'*USIC*, le lobby international de l'USGIF et la position hégémonique de l'industrie américain (ESRI) pour le développement des SIG font des Etats-Unis le leader mondial incontesté du Geoint, secteur de la Défense inclus. Mais il est aussi flagrant que le *DoD* a bien repris la main sur le Geoint, notamment au nom de la sécurité nationale post 11/09.

Fort de ce constat sans appel, il parait légitime de se demander comment la défense française se positionne, au nom cette fois de l'impérieuse nécessité stratégique d'autonomie d'appréciation et d'indépendance nationale.

3) Naissance à marche forcée du Geoint militaire français

a) 2014 : la prise de conscience des Armées

Pour le GCA Gomart, « *la France est en retard dans le domaine du Geoint et la modernisation du renseignement géospatial, est une nécessité* »[120]. Ce domaine de synthèse de l'information est l'exemple parfait où les autorités françaises doivent absolument conserver une autonomie d'appréciation. Le renseignement géospatial visant « *à capitaliser le renseignement à travers une approche spatiale orientée vers l'action et la manœuvre* », la DRM a ainsi décidé en 2014 *« la création d'une cellule de Geoint en son sein et vise à booster les capacités des armées en matière de connaissance et d'anticipation. »* [121]

b) Le CRGI, référant interarmées

i) Contexte

Le centre de renseignement géolocalisé interarmées (CRGI) a été créé un an avant le CRAC à l'été 2014. Centre en charge du Geoint au sein de la DRM à Creil, il est placé organiquement au sein de la sous-direction exploitation (SDE)[122], illustrant ainsi sa mission

[120] Propos rapportés du GCA Gomart, Lettre d'informations stratégiques et de défense TTU, La DRM et le Geoint, TTU n°967 du 04/03/2015.
[121] *Id.*
[122] Pour mémoire, le CRAC est positionné au sein de la SDR. Voir page 08.

d'exploitation et de fusion des données géolocalisées, quelque soient leurs origines, pour répondre à une problématique opérationnelle et militaire de la DRM.

Le CRGI a été fondé à partir de la section d'appui géographique (SAG) de la DRM, en charge jusqu'alors de la réalisation des cartes de synthèse au profit de la SDE. La numérisation puis la nécessité de croiser les multiples informations géolocalisées, disponibles en interne de la DRM et en *opensource*, ont abouti logiquement à la prise en compte du Geoint en lieu et place. Notons qu'à l'instar des Etats-Unis l'**approche multicapteurs est naturelle au Geoint français.** Le CRGI est donc en charge de la fusion l'information géoréférencée de tous les capteurs accessible à la DRM (dont le CRAC), et de la réalisation à la demande de produits géographiques issus de leurs SIG au profit de la SDE, et donc in fine au profit du décideur militaire de l'EMA.

ii) Enjeux

L'enjeu du Geoint est clairement exprimé pour la DRM au sein de la seconde étape du plan de transformation, et inscrite dans la réforme des armées du CEMA (Cap 2020) : « *faire du CRGI l'organisme référent dans le domaine Geoint afin de fournir aux armées, jusqu'au niveau tactique, un renseignement complet fusionnant l'ensemble des données disponibles sur un même support géoréférencé* [123]». La similitude avec la NGA est frappante, même si la valeur ajoutée du CRGI, sans chauvinisme, est supérieure à celle du NGA….

Car encore plus que dans le Cyber, le Geoint est en France un secteur d'activité dominée par le secteur civil. L'ouverture croissante de l'accès aux données *(opendata*[124]), enjeu économique majeur en France, tend à démultiplier les acteurs de l'exploitation de données géolocalisées sur des thématiques précises. Les Armées ne sont toutefois pas en reste : pour l'exemple, la sécurité des *Fan-zones* lors de l'Euro de football 2016, d'ordre de sécurité publique mais aussi défense sous le prisme de la lutte antiterroriste (Opération Sentinelle), a vu de multiples travaux exploratoires se réaliser au sein du 28e Groupement Géographique, du CIAE, du CF3I, du CRGI, de la police, des pompiers, des cellules de crise des Préfectures concernées, de la Section Technique de l'Armée de Terre, et sans doutes de bien d'autres acteurs encore…. Tous ont répondu bien légitimement à un aspect de la

[123] Source : http://www.defense.gouv.fr/ema/interarmees/la-direction-du-renseignement-militaire/la-drm/drm-2020-la-drm-se-transforme/drm-2020.-la-drm-se-transforme

[124] Opendata : un exemple d'application récent est l'ouverture de la RATP à l'accès à ses données en temps réel. Source : P. Jacqué, *La RATP ouvre (enfin) ses données « temps réel »,* Le monde, 05 janvier 2017. La loi Macron oblige en effet deûis peu en France les entreprises publiques à se convertir à l'opendata.

question, avec une volonté affichée de maîtriser de nouvelles techniques. Mais l'absence notoire de coordination est à ce niveau très frappante.

Ainsi, si le savoir-faire existe bel et bien, le challenge du CRGI sera de cadrer le besoin des Armées (exprimé au niveau des centres de renseignement respectifs - CRA, CRMar et CRT[125]) et d'homogénéiser la communauté autour d'une **référence unique**, permettant à tous les acteurs militaires de contribuer à une synergie d'ensemble. Ainsi, en tant que référent national, la DRM est légitime dans l'écriture des méthodes Geoint françaises à vocation interarmées.

Contrairement au CRAC qui a une structure organisée selon l'expertise technique envisagée, le CRGI est organisé par pôles que nous simplifierons de la façon suivante :

- Un pôle opérationnel, responsable du **Traitement Informatique de Masse (TIM)**. Il est subdivisé en zones géographiques d'intérêt, en cohérence avec l'approche terrain inhérente à la géolocalisation des études.
- Un pôle connaissance des infrastructures, dont la mission est de caractériser les sites d'intérêts militaires, notamment en suivant les activités relevées par différents senseurs numériques (recouper les données thermiques, les relevés magnétiques de source satellitaire, les mouvements de véhicules, la consommation électrique du site, les flux humains, le maillage des équipements connectés de sécurité…etc). Il s'agira d'exploiter toutes ces données, pour établir la carte d'identité réelle et instantanée du site. Ce travail sera vraisemblablement stocké au sein d'une base de référence, disponible à tout moment, afin de fournir au chef, toujours dans une logique de requête à la demande, toutes les informations de caractérisation pertinentes. La finalité d'action est ici perceptible, mais n'est pas du ressort du CRGI.
- Un pôle d'appui, cœur de la prospective du Geoint. Il est en effet en charge de la définition du *backoffice* et du *frontoffice*[126], de la maintenance et des évolutions des SIG, des problématiques essentielles de stockage des données collectées (définition des infrastructures, des moyens d'accès), de la diffusion des produits Geoint, ainsi que l'adaptation **à des fins militaires** des fonctions civiles existantes d'analyse spatiales :

[125] CRAA, CRMar et CRT : Centre de renseignement respectivement Air, de la Marine Nationale et Terre. Ce dernier est en cours de montée en puissance à Strasbourg auprès du nouveau COMRENS de l'Armée de Terre et intègrera vraisemblablement une composante Geoint. L'enjeu de coordination avec le CRGI sera alors essentiel.

[126] Il s'agit de l'ensemble des sous-systèmes informatiques concourants à la réalisation du produit de visualisation final du Geoint.

géostatistique[127], *geoscoring*[128], *geofencing*[129], au profit de modèles prédictifs ou d'alertes semi automatisées[130].

iii) Processus d'élaboration du renseignement Geoint

Le CRGI fonctionne comme tout organisme en appui, dont le principal défi consiste à répondre dans un temps imparti à la *RFI* externe avec le bon niveau de granularité. L'analogie avec le processus d'exploitation Cyber est sous-jacente. La séquence de travail type peut donc se décrire de la manière suivante :

1. Reformulation par le CRGI de la RFI, afin d'acquérir la certitude de la bonne compréhension du problème, et de la capacité à y répondre.
2. Recensement des données existantes au sein des entrepôts (*Data Warehouse*, partenaires, bases propriétaire de la DRM....) et exploitation au sein d'un SIG.
3. Requête complémentaire vers tous les capteurs de la SDR (approche multisources) pour l'obtention de nouvelles données. Un principe pilote cette étape : la véracité des données collectées doit être absolue. Posséder ses propres capteurs Geoint est ici une plus-value certaine[131].
4. Cœur du process, il s'agit de la corrélation temporelle et spatiale des données collectées, dont l'exploitation dans le temps imparti, et notamment leur report sur un unique support géoréférencé (problématique de compatibilité des systèmes de localisation des données) est un travail fastidieux mais crucial. L'étude des résultats pourra alors commencer sous tous les aspects possibles.
5. Synthèse sous forme d'un produit Geoint opérationnel, réponse à la RFI initiale.

---

[127] Géostatistique : méthode mathématique de traitement de données numériques à support spatial et/ou temporel, et quantification des incertitudes, utilisées notamment dans les industries minières, pétrolières, environnementales, halieutiques, constructions de matériaux, … Cette méthode statistique prend en compte la structure spatiale des données, l'espace de dimension quelconque, l'échantillonnage irrégulier et incomplet (données fragmentaires), et d'autres informations externes pour établir des modèles de référence. Source : Séminaire "*Statistique spatiale pour l'industrie et le marketing - Concepts et méthodes de la géostatistique* », B.Looss, CEA, 2006.

[128] *Geoscoring*: étude de mise en relation d'un territoire et des activités à sa surface. Le projet français LOKEO (ENS Lyon, paré du trophée Réseau CURIE 2011 du Ministère de la Recherche) est un algorithme basé sur les emplacements réels des commerces et permettant de rechercher l'emplacement optimal pour implanter une nouvelle activité. Source : http://www.ens-lyon.fr/recherche/lokeo-de-pablo-jensen-laureat-du-trophee-reseau-curie-2011-du-ministere-de-la-recherche-124331.kjsp, consulté le 4 janvier 2017.

[129] *Geofencing* : Le géorepérage ou gardiennage virtuel (en anglais, *geo-fence* ou *geofencing)* est une fonction d'un logiciel de géolocalisation qui permet de surveiller à distance la position et le déplacement d'un objet et de prendre des mesures si la position ou le déplacement s'écarte de certaines valeurs fixées d'avance.

[130] Approche prédictive, semi automaticité des tâches : ces concepts seront développés en 3e partie.

[131] L'exemple d'un drone Geoint vu précédemment est une piste probante. Se reporter à la note 103.

Comme dans le cas de la Cyber, le demandeur n'est pas un expert du Geoint. La vulgarisation des résultats est donc fondamentale pour assister le décideur final à comprendre les résultats obtenus. Toute l'expertise de l'opérateur du Geoint sera ici nécessaire.

A l'aune de ce processus, une grande similitude avec le Cyber apparait : les enjeux liés aux capacités informatiques disponibles (performance du SIG, puissance des moteurs de recherche, capacité de calcul, disponibilité et indexation des entrepôts/base de données, importance des flux dédiés…) sont fondamentaux pour l'efficacité de l'ensemble. C'est aussi dans l'intelligence des automates qui seront utilisés et dans la définition des algorithmes que résidera la pertinence de l'ensemble de la capacité du Geoint, que ce soit en renseignement ou en appui des opérations. L'effort financier consenti en recherche amont et en équipement sera donc également extrêmement dimensionnant dans le Geoint.

Ainsi, dans le domaine de la Défense, les points de convergence du Geoint et du Cyber, que ce soit en termes d'opportunités ou de vulnérabilités, sont de plus en plus nombreux. Il semble d'ailleurs, dès qu'est abordé le thème de la prospective, que ces deux domaines, opérationnellement séparés dans les organigrammes français ou américains, tendent par nature à converger vers le même idéal : détenir et utiliser la bonne donnée, à temps, pour réaliser les analyses les plus pertinentes possible de la situation opérationnelle au chef militaire. Fort de ce constat, quelle complémentarité pourrait-on alors envisager ?

Figure 3 : exemple de contributions » images » pour l'élaboration 'une synthèse Geoint. Source : geo4i, disponible su http://geo4i.com/wp-content/uploads/2014/02/Schema-Geoint-3.jpg.

III. Cyber ou Geoint, une dépendance stratégique à la donnée numérique

1) Les facteurs limitants à l'autonomie stratégique

a. Maintenir une capacité d'accès nationale aux données

Comme nous l'avons démontré précédemment, l'adhérence structurelle du Cyber et du Geoint au monde de la donnée numérique est total. Dans l'ensemble des réflexions et ouvrages parcourus, un postulat est sans cesse présent et semble pour beaucoup un fait acquis : la donnée nécessaire à ces deux disciplines « est disponible ». Pourtant, rien n'est moins sûr… Car si la donnée informatique existe à un instant -t, rien ne saurait garantir qu'elle le sera ensuite à t+1, qui plus est dans un contexte de crise majeure.

Pour s'en convaincre, prenons deux faits volontairement très récents, illustrant la nouvelle et douloureuse prise de conscience de cette faille structurelle dans la persistance de l'accès aux données pour les états-majors.

Suite à la nomination du 45e président des Etats-Unis M Donald Trump, un des premiers décrets présidentiels[132] vise à supprimer des communications de l'US-EPA[133] toute étude relative au réchauffement climatique, ainsi que la suppression de toutes les données gouvernementales associées à l'étude du climat. Face à cette censure aux répercussions scientifiques colossales, un collectif de hackers s'est lancé dans une vaste opération de sauvegarde à travers le hackathon "*DataRescue*"[134]. La collectivité redécouvre ainsi qu'une donnée peut disparaitre immédiatement sous la pression politique et/ou des lobbies sous-jacents du moment. Par extension, on peut alors s'interroger sur l'utilité du Cyber ou du Geoint, si ces capacités venaient à être isolées des données les alimentant en dehors de leurs propres archives (suppression des données ou cyberattaque d'une puissance hostile) ?

---

[132] Le 20 janvier 2017, des pages entières dédiées au réchauffement climatique ont disparu du site de la Maison-Blanche, whitehouse.gov. Notamment tout ce qui concernait le plan d'action de lutte contre le changement climatique mis en place par Barack Obama.

[133] *L'US-EPA*, *United States Environmental Protection Agency*, est un organisme indépendant rattaché au gouvernement en charge de la protection de l'environnement.

[134] Voir l'article d'H. Gully *Comment les hackers archivent tout ce que Trump veut effacer,* les Echos, 28 janvier 2017. Ce hackathon solidaire est organisé pour sauver quantité de données d'une potentielle disparition, par la mise en place d'une base de données qui rassemblerait toutes les informations d'une ère antérieure au gouvernement actuel et par la sauvegarde d'une copie de cette même base de données à l'extérieur du territoire pour la préserver de toute réquisition administrative. Source : http://www.lesechos.fr/monde/etats-unis/0211729808260-comment-les-hackers-archivent-tout-ce-que-trump-veut-effacer-2060827.php., consulté le 29 janvier 2017.

Notre deuxième exemple tout aussi récent s'appuie sur la même hypothèse de déni majeur d'accès, mais il est pris en compte directement au cœur de l'EMA et des plus hautes autorités de l'Etat : *« Et si Internet s'arrêtait ? Le scénario est pris au sérieux par les Etats. Ils craignent les attaques massives de hackers, de terroristes ou de puissances rivales. Face aux menaces inédites, sommes-nous bien armés ?* »[135]. La réponse est cinglante: si la résilience des OIV[136] est prioritaire dans un tel scénario, la collecte de l'information à fin de renseignement (volet renseignement du Cyber, Geoint) ne semble pas figurer dans les capacités essentielles à mettre en œuvre en cas de coupure massive et hostile des accès nationaux. Geoint et Cyber risquent bien d'être aveugles, curieux paradoxe… Il convient pour nuancer cette approche de poser la question dans l'autre sens : est-ce que l'anticipation opérationnelle est encore de mise dans les premières heures effective d'une crise grave ?

b. Organiser une capacité transverse de stockage

Pour garantir une autonomie d'appréciation et pérenniser l'accès à ses connaissances, le scénario du pire envisagé précédemment éclaire utilement sur la nécessité de posséder pour la France ses propres infrastructures nationales et militaires de stockage des données numériques collectées.

Durant nos travaux, nous n'avons trouvé aucune référence explicite au fait que le Cyber militaire et/ou le Geoint doivent posséder leurs propres *datacenter*. Nul doute que ce soit le cas, mais vraisemblablement sans interconnexions. Chaque entité, ministère, agence de renseignement détient en effet en France ses propres serveurs, autonomes et redondants, afin de satisfaire ses propres exigences opérationnelles. Mais l'interrogation reste entière dans une logique transverse et centralisée propre au Geoint (position de référent national, apte à irriguer chaque utilisateur à l'image de l'infrastructure choisie par le NGA). De plus, nous avons vu que la logique du Geoint de s'appuyer massivement, outre les senseurs militaires dédiés, sur la consultation de *dataproviders* extérieurs, de données *opensource* ou de contributions valorisées de partenaires militaires représente ici une vulnérabilité supplémentaire, puisqu'il est plutôt rationnel de ne pas stocker ce qu'un partenaire tient déjà à disposition.

[135] Source : dossier *le jour où Internet s'arrêtera- la nouvelle Cyberguerre mondiale,* hebdomadaire Le Point n°2316, 26 janvier 2017, pages 51 à 61.

[136] OIV : Opérateur d'Importance Vitale. Il s'agit d'une liste secrète d'environ 200 entreprises dont l'activité est .essentielle à la survie de la France, gérée par l'ANSSI.

Enfin, le choix de posséder ses propres infrastructures est fondamental pour la capacité numérique des Armées (Cyber et Geoint). Les coûts sont certes astronomiques, et l'explosion de la production des données[137] implique un développement exponentiel et sans fin des infrastructures de stockage associées. Cette course stratégique au stockage semble donc soit un enjeu majeur, soit une chimère...

c. Une standardisation utopique de capacités autonomes d'exploitation ?

Nos développements sur la capacité Geoint et notamment les travaux de comparaison avec la structure américaine ont fait apparaitre la volonté marquée du NGA et de l'USGIF de mettre en œuvre un SIG unifié au sein de l'USIC. Cette standardisation est recherchée également au niveau beaucoup plus hétérogène et fragmenté des formats des données géolocalisées, afin de palier l'énergie considérable consacrée à convertir les données collectées afin d'effectuer des synthèses cohérentes. Nul doute que le CRGI souhaiterait atteindre aussi cet état simplifié…

Mais la vraie question est bien celle de la puissance internationale du lobby de l'USGIF, dans un combat normatif embrassant toute la communauté du numérique internationale. Pragmatiquement, cette situation ultra-dominante des Etats-Unis laisse craindre une posture plutôt passive de la France compte tenue de la modestie relative de ses moyens.

De même, notre étude du Cyber a soulevé à de nombreuses reprises la nécessité de standardiser les SIOC, afin de garantir une efficacité optimale des systèmes des Armées. Tous ces combats (unification des SIG, uniformisation du format des données, standardisation des SIOC) sont des opérations majeures pour l'EMA, d'autant qu'elles touchent aux capacités stratégiques d'appréciation où, comme nous l'avons vu, l'indépendance nationale est primordiale. Est-ce possible en s'appuyant sur des standards, des processus, des matériels et des logiciels étrangers ? L'Etat français peut-il rester réellement souverain dans une telle

[137] L'Idate (Institut de l'audiovisuel et des télécommunications en Europe) estime qu'il y aurait début 2017 15 milliards d'objet connectés à internet contre 4 milliards seulement en 2010. D'après une étude menée par Gartner et l'Idate en 2020 on peut estimer que le nombre d'objets connectés en circulation à travers le monde s'élèvera entre 50 et 80 milliards. En clair chaque personne détiendra environ 6 objets connectés. Rien que pour 2018, on estime à 6 milliards (cabinet Gartner) le volume de nouveaux objets connectés qui seraient mis en circulation à partir de 2018 (source : article « Quelle place pour les objets connectés dans notre société ? » du 24 janvier 2017 visible sur http://www.objetconnecte.net/objets-connectes-chiffres-etudes-2401/

approche, face notamment à des fournisseurs privés aux capitaux et intérêts souvent étrangers ?

2) Le challenge : la fusion de données dans l'espace-temps des opérations militaires

a. Réserves et limitations préliminaires

En reprenant l'ensemble des processus et capacités énoncées au sein du Geoint et du Cyber, nous avons imaginé un scénario opérationnel sur lequel le CRGI et le CRAC pourraient agir. Cet exemple vise à illustrer l'apport complémentaire de ces deux domaines stratégiques du renseignement militaire français, à l'appréciation de situation d'un chef militaire. Pour des raisons de sécurité, ce scénario est fictif, mais demeure volontairement réaliste vis-à-vis des engagements opérationnels actuels de la France en 2017 (Bande Sahélo-Saharienne, Levant, contre-terrorisme international).

b. Cyber et Geoint complémentaires et au service des opérations

Sur un premier théâtre d'opération, une compagnie française d'infanterie est attaquée par un VBIED[138] sur sa base de repos et parvient *in extremis* à détruire la menace. La DRM est immédiatement intriguée par le mode opératoire : aucun précédent de cette nature sur cette zone ni aucune revendication. A l'EMA, il s'avère alors nécessaire de répondre à deux questions: qui s'attaque à nos forces ? Et surtout pourquoi ?

Afin de maîtriser au plus vite cette nouvelle menace, une première recherche est initiée. Elle est d'abord menée physiquement par l'unité française sur place, qui récupère sur le cadavre du pilote du VBIED une carcasse de téléphone portable, hors d'usage. Ce téléphone inexploitable localement est donc confié au CRAC, qui à l'aune de son ISN et une première étude large spectre en « source ouverte » identifiera quelques éléments techniques clés (IMSI, IMEI, fragments de données sur la carte mémoire…) Ces données permettent de constituer un premier *pattern of life* de ce boitier et de son possesseur présumé.

Après décision des autorités de la DRM, une recherche avancée, donc multicapteurs, est ordonnée, essentiellement basée sur les données techniques recueillies précédemment. Elle permet de déterminer *in fine* que le propriétaire de ce téléphone a été en lien, notamment par

[138] VBIED : *Vehicle Borne Improvised Explosive Device :* véhicule piégé. Pour les besoins du scénario, celui-ci est piloté par un homme sans identité apparente.

RSN crypté, avec un avatar… Après requête auprès des services de renseignement, il s'avère que cette identité numérique appartient avec une raisonnable certitude à un chef terroriste bien connu des services français. Problème : celui-ci opère dans une toute autre contrée, et excelle dans l'art de se dissimuler, sa tête étant depuis longtemps mise à prix par les autorités militaires…

Ce deuxième pays a toutefois la particularité d'être aussi couvert par une autre opération française, menée dans le cadre de sa stratégie globale contre le terrorisme international.

La cible, car c'en est devenue une pour la DRM, poste régulièrement sur son RSN de la propagande, visant à revendiquer son œuvre de destruction des valeurs occidentales et démontrer son efficacité personnelle[139]… l'ego, une faille sociale bien connue. Très prudent, il diffuse ses œuvres en différé et derrière de sérieuses protections numériques : proxy, VPN, anonymisation Tor… Il prend soin de ne jamais activer les métadonnées de son téléphone, et chaque vidéo ou photo postée n'est par conséquent jamais localisable directement.

Une étude Geoint est donc décidée, alors que le Cyber se charge de traquer son activité numérique à la recherche de la moindre erreur d'opportunité. Il s'agit pour tous de localiser la cible, afin d'envisager des options réalistes de *COA*.

La géographie de la zone supposée d'influence, déterminée par le cumul des positions téléphoniques de la cible remontées par le cyber (triangulation des BTS, *time advance* cumulés, *tracking* permanent), est minutieusement cartographiée et modélisée par le Geoint à l'aide de toutes les données disponibles en *opensource* et les bases de données partenaires dans le cadre de protocoles d'échange : photos satellites, étude de terrain, données météo, études hydrographiques et géologiques, données sismographiques, cadastres, données temps-réel issues des flux non sécurisés des *IoT*, tout est compilé, trié et recoupé afin de déterminer une carte cumulée, numérique et renseignée, de l'AOR du chef terroriste. L'objectif est clair : avec le temps, chaque photo postée par la cible sera immédiatement géoréférencée grâce aux sites visibles sur l'image et reconnus par les algorithmes du Geoint… de même pour les vidéos. Le principe mis en œuvre est assez simple : l'ombre portée et l'angle de prise de vue permettent d'estimer l'axe et l'heure du cliché. La destruction constatée des infrastructures permet de dater réellement le document. Les études sur le réseau télécom disponible à la date

[139] L'ego, mais aussi le recrutement, sont deux leviers qu'utilise l'ISIL pour sa communication numérique. Voir TTU, *actions cognitives et djihadisme*, TTU n°939 du 25 juin 2014 .

déterminée et à l'endroit estimé permettent d'affiner la localisation précise du preneur de cliché… Jour après jour, inexorablement, la toile se resserre et le *pattern of life* de la cible se dessine avec précision. Ses trajets, ses habitudes, ses points d'observation d'où il se filme pour sa propagande sont déterminés et caractérisés à distance.

Le verdict tombe enfin après plusieurs semaines de traque numérique : chaque mardi à 16h00 précise, la cible se filme en extérieur, et toujours du même endroit, pour son point « hebdomadaire » de propagande. Le renseignement est ensuite recoupé et confirmé : il devient par sa nature directement actionnable. Ainsi, la DRM peut proposer différentes options au chef militaire de l'EMA pour lui permettre d'envisager une neutralisation du donneur d'ordre de l'attaque initiale du camp français, par un mode opératoire que seul l'EMA décidera avec le feu vert politique.

c. Une action complémentaire en devenir

Ce scénario sur fond de lutte antiterroriste aboutit volontairement à une hypothèse de de neutralisation potentielle par les Armées de la menace identifiée, qui dans notre cas s'en est pris directement aux intérêts et forces françaises. Ce processus est bien conforme aux déclarations du Président de la République Française M. François Hollande du 13 juillet 2016 « *nous devons frapper et détruire ceux qui nous ont agressé [en France] »*[140].

Lors d'un reportage vidéo sur le CRGI[141], le GCA Gomart présente aussi d'autres aspects du Geoint : caractérisation de site et usage réel par les terroristes, estimation de *BDA* après frappes… Autant d'aspects complémentaires réels que nous aurions pu intégrer. Mais l'objet ici est bien de présenter une des premières raisons opérationnelles des outils Cyber et Geoint du renseignement militaire : d'une part éclairer le chef sur les évènements passés et à venir, et proposer ensemble une gamme d'actions possibles pour traiter la menace identifiée. Il s'agit aussi d'illustrer par l'exemple une complémentarité efficace de ces deux capacités, ce qui à n'en pas douter représente l'avenir proche de l'exploitation géoréférencée.

[140] Discours de M F. Hollande, président de la république, prononcé au ministère de la Défense le 13 juillet 2016 à l'occasion de l'annonce du déploiement du groupe aéronaval nucléaire Charles-de-Gaulle au sein de l'opération Chammal à l'automne 2016. « *Nous devons frapper et détruire ceux qui nous ont agressés ici en janvier et en novembre 2015*"

[141] Reportage diffusé dans l'émission Complément d'enquête sur France2, enregistrée le 09 novembre 2016 et diffusée le 17 Novembre 2016 « *des deux côtés de la bombe* ». Enquête de M. Fauroux, R. Tarsissi, B. Baubit et D. Da Meda.

L'adhérence extrêmement forte de nos deux capacités Cyber et Geoint à la composante du ciblage de l'EMA est naturelle, dès lors que l'action retenue n'est pas exclusivement cyber (entrave, brouillage, destruction numérique) comme de nombreuses opérations par le passé. Si un aspect cinétique est à envisager, l'objet des travaux Geoint et Cyber sera bien d'aider *in fine* le chef militaire à décider en toute connaissance d'une opportunité de frappes sur les objectifs référencés, et surtout localisé, avec une précision compatible avec les systèmes d'armes en charge de cette mission[142].

Nous pouvons enfin formuler deux remarques à l'aune de cet exemple opérationnel :

- si le Geoint fonctionne parfaitement dans sa composante naturelle de « connaissance et anticipation », une certaine marge de manœuvre semble encore nécessaire pour envisager un appui « temps-réel » aux opérations. De nombreuses études sont d'ailleurs en cours pour permettre de "gagner des délais" sur l'élaboration d'une synthèse Geoint compatible avec le tempo des opérations. Ce sera tout l'enjeu des modèles d'alertes prédictives.
- En outre, le Geoint n'a aucune capacité d'effecteur, puisque c'est un échelon de synthèse. Le Cyber, par opposition, en plus d'être un capteur apte au renseignement dans la profondeur, est aussi une capacité offensive capable d'agir dans le cadre d'opérations ciblées. Les études précédentes du COMCYBER français et de l'USCYBERCOM américain l'ont clairement illustré.

3) Le Cyber et le Geoint, le pacte de sang

a. Le Cyber, l'ennemi n°1 du Geoint

Selon le *Weissbuch* allemand[143], la menace Cyber est la seconde menace d'importance[144]. La stratégie française tend également vers ce modèle. En retenant l'étude et

[142] La problématique « du dernier mètre » pour les munitions guidées comme le scalp français, ainsi que la définition de la trajectoire d'approche pour ne pas provoquer des dégâts supplémentaires.

[143] Weissbuch : livre Blanc de la Défense allemand. Le BND (service secret allemand) a déjà pris en compte au moins depuis 2014 la problématique de la cyberguerre, via le programme « Strategische Initiative Technik » (SIT). 6M€ y auraient été consacré en 2014, et plus de 26M€ en 2015, et avec un besoin en financement estimé à 300M€ jusqu'en 2020. Source : TTU, *Allemagne : Le BND et la Cyberguerre*, TTU n°959 du 07 janvier 2015.

[144] Les menaces principales citées dans le document sont le terrorisme transnational, les attaques dans les domaines du Cyber et de l'information, et les conflits hybrides. Les migrations incontrôlées n'arrivent qu'en huitième et avant-dernière place, avant les pandémies.
Source : http://www.lemonde.fr/europe/article/2016/07/13/l-allemagne-s-engage-a-devenir-un-partenaire-militaire-plus-actif_4968879_3214.html du 13 juillet 2016, consulté le 4 décembre 2016.

la définition du Geoint comme la fusion des données numériques, nous pouvons par une étude croisée avec les capacités Cyber expliciter de nombreuses menaces qui font peser un risque inacceptable sur le Geoint.

En marketing du BigData[145], l'optimisation permanente des acteurs du secteur de la donnée cherchent à répondre à la règle des 5V : volume, vitesse, variété, véracité et valeur. Vus côté Cyber, ces 5 axes sont autant d'angles d'attaques qui affaibliront à dessein le Geoint… Imaginons pour s'en convaincre ce scénario : nous avons vu que la gestion exponentielle de données créées était un défi pour toute organisation en charge de la collecte et fusion d'information comme le Geoint. Imaginons désormais un réseau de *bots* fournissant sur ordre (une variété de cyberarme) une série d'informations erronées, géolocalisées et de manière massive : le *Ddos* est inévitable[146] et les crashs des algorithmes de synthèse probables. Plus subtilement, cette technique de diffusion de fausses informations, utilisée avec parcimonie, pourrait corrompre dans la durée de nombreuses données digérées ensuite par le Geoint et les bases de référence constituées. Un mode opératoire *high-tech* proche de l'influence en somme… Enfin, les solutions de corruption GPS sont connues[147] (du brouillage au leurre) rendant le positionnement issu de cette seule technologie potentiellement vulnérable par une action Cyber, aussi redoutable que pernicieuse.

La question du contrôle d'intégrité de la donnée et de sa réelle véracité est donc posée. La réponse pourrait se trouver dans la variété d'informations (multisources). En admettant ce principe intellectuellement rassurant, on avoue implicitement la dépendance du Geoint aux données externes (donc étrangères), remettant ainsi en cause le principe de souveraineté nationale… Autre parade potentielle : disposer de capteurs de collecte propres. Cette solution est malheureusement financièrement irréaliste pour prétendre suivre n'importe quelle problématique à la demande à travers le monde …

Autre vulnérabilité du Geoint : son infrastructure. Elle est forcément tributaire de moyens extérieurs. Prenons une ferme de serveurs de stockage. Dans la partie Cyber, nous

[145] voir partie III 4/

[146] L'attaque du 24 octobre 2016 de type *Ddos* sur le DNS de Dyn aux Etats-Unis, montée à l'origine par un étudiant pour manifester son mécontentement contre un distributeur de jeu vidéo, a eu d'innombrables répercussions internationales : Airbnb, Box, GitHub, Heroku, le New York Times, Reddit, Twitter, SoundCloud, Spotify… Des sites web sont restés inaccessibles pendant près de 11 heures, avec des répercussions économiques et boursières importantes… le réseau bots utilisé et qui a saturé l'infrastructure de géants du web était un réseau de dizaines de millions d'adresses IP d'IoT (caméras de surveillance) non sécurisés…

[147] Ce constat alarmiste militerait pour une double compatibilité des systèmes de localisation militaires, au GPS ainsi qu'au système européen Galileo désormais opérationnel depuis le 15 décembre 2016.

avons vu les capacités de déroutage de flux (tables BGP par exemple) de la NSA, qui fait peser un risque de fuite de données important. Par ailleurs, cette ferme est-elle constituée de matériels entièrement souverains et sûrs ? Un seul composant d'origine étrangère peut être une faille potentielle par l'implémentation volontaire d'un 0-day par le pays hôte en amont de son installation… De même, la ferme sera tributaire d'un approvisionnement énergétique important, lui-même dépendant des vulnérabilités *Scada*[148] tout aussi connue : le risque de *Ddos* est donc réel pour le Geoint. Ce scénario est toujours pertinent en l'appliquant au niveau des logiciels utilisés, massivement élaborés outre- atlantique et donc potentiellement affaiblis par des *backdoors* …

Ainsi, comme tout système informatique, les SIG et l'ensemble du Geoint est vulnérable au risque Cyber. Ce constat est d'autant plus vrai si nous prenons un SIG unifié interconnectant l'ensemble des acteurs de la communauté du renseignement…La nécessité d'une indépendance stratégique nationale sur le plan Cyber a donc une réelle répercussion sur le monde du Geoint, et les appréciations de situation qui en découleront (ou non) en cas de crises graves : fournisseur d'accès, plan de communication, serveurs, *backbone*, bases de données, algorithme de sauvegarde des données, IA nationale sont autant d'aspects stratégiques pour l'autonomie nationale de décision.

b. Le Geoint leurré ou aveugle sans le Cyber

Toujours en s'appuyant sur la règle des 5V, il apparait dans l'étude inverse des relations Cyber-Geoint que la capacité Cyber peut aussi être le principal garant du Geoint.

Le Cyber est en effet apte à contrôler l'intégrité des données et à effectuer en appui du Geoint de nombreux recoupement afin d'isoler les données éventuellement corrompues. Les algorithmes de recherches de signaux faibles ou d'incohérence seraient ici d'une grande aide. Reste toutefois à constituer une base de confiance qui servira ensuite de référence pour les levées de doute. Le Cyber pourrait également caractériser les anomalies de toute sorte, comme les photographies retouchées[149] ou des métadonnées corrompues volontairement.

[148] Le Cert-Fr publie en permanence des mises à jour relatives aux Scada omniprésents dans l'industrie, le seteur de l'énergie, etc. Ces systèmes sont souvent anciens, informatiquement très vulnérables et peu pris en compte par les RSSI des entreprises. Ils sont pourtant au cœur de notre économie.

[149] De petits logiciels gratuits sur Internet s'attèlent efficacement à cette tâche (comme JPEGsnoop, et FotoForensics). Le principe repose sur la recherche d'incohérence par mesure d' *Error Level Analysis,* ou de modifications opérées par des algorithmes connus, ou encore sur les métadonnées de la photo, notamment les données Exif.

Ensuite, tel que présenté actuellement, le Geoint s'appuie sur des données collectées par des senseurs ou au sein d'entrepôts partagés. Cela sous-entend logiquement que ces données disponibles au sein d'une communauté le sont volontairement et de manière assumées par son propriétaire. Dans la communauté méfiante du renseignement, partager une donnée de valeur est assez rare…. Pourtant, c'est bien cette donnée qui représentera un intérêt stratégique pour une analyse d'ordre militaire par exemple. Ainsi, pour « aller chercher » cette donnée en cas de besoin, il apparait assez aisé de faire appel à l'arsenal Cyber offensif que nous avons décrit précédemment, afin d'exfiltrer à l'insu de son détenteur la donnée à haute valeur convoitée (un piratage de satellite de collecte Geoint militaire d'une puissance tiers par exemple). Le Cyber offrirait ainsi une plus-value inimaginable au Geoint, mais l'application du droit fait peser des risques réels sur un tel scénario, en premier lieu le degré de confiance relatif des dits partenaires.

Enfin, il convient de reprendre une limite déjà énoncée à plusieurs reprises dans nos travaux : l'Internet référencé, celui sur lequel tous les modèles « ouverts » de partage de données s'appuient, ne constitue que 10 à 15% seulement du volume total des connaissances numériques. Dit autrement, 85 à 90% des données numériques sont uniquement disponibles sur les *Dark/Deepweb*. Que penser alors d'un renseignement élaboré en grande partie sur un échantillonnage de seulement 15% ? Ce constat volontairement provocateur à l'encontre du Geoint souligne l'impérieuse nécessité pour le Cyber de plonger au sein du Deepweb, afin d'en identifier et surtout d'extraire les données utiles au Geoint, avec toutes les mesures de protection et de contrôle adéquates.

Ainsi, Cyber et Geoint ne sont pas deux silos du renseignement des Armées sans liens, bien au contraire. Explorant tous deux le monde de la donnée numérique, pouvant aller jusqu'à le façonner en partie, il convient de réfléchir désormais aux prospectives et enjeux soulevés notamment par l'indispensable besoin d'automatisation des traitements : le Bigdata pourrait être une réponse.

4) La fusion Cyber-Geoint : vers le Bigdata ?

Devant l'explosion de la production des données de tout type et l'ensemble des problématiques inhérentes que nous avons développées (stockage, accès, gestion de flux, indexation, recherche), Geoint et Cyber touchent très logiquement au problème connu sous

l'appellation Bigdata, qui n'est pas nouvelle[150]. Les forces de sécurité et militaires sont également de la partie comme en témoigne, notamment côté US, les nombreuses productions sur le sujet (voir Bibliographie).

Il n'existe pas de réelles définitions de l'objet complexe et polymorphe du Bigdata, hormis ses traductions en « mégadonnées » ou « données massives ». Nous retiendrons que ce concept englobe l'ensemble des techniques automatisées et développées pour faire face aux 2,5 trillions d'octets de données générés quotidiennement à travers le monde, sans compter que ce flux est désormais essentiellement généré par des réseaux de bots[151] (télémétrie, *scada*, remontée d'informations techniques[152]). Certains vont jusqu'à affirmer qu'il s'agit d'une véritable révolution industrielle, d'autres estiment qu'il s'agit de **la dernière étape de la troisième révolution industrielle de** l'information. Pour ne citer qu'un exemple militaire et connu d'application du Bigdata, celui du programme PRISM de la NSA est sans doute le plus pertinent (et révèle au passage nombre d'aspects de la stratégie Cyber globale américaine).

De nombreux colloques et séminaires, notamment en France[153], tentent de définir et cadrer les contours du Bigdata appliqué à la Défense. Car dans ce domaine plus que tout autre, largement dominé par les nombreux appétits de l'écosystème des NTIC[154], les outils existants contraindront inexorablement le besoin, alors que l'approche à retenir pour la Défense est bien d'un besoin qui façonnera ensuite les outils.

Le processus du renseignement appliqué aux données (Cyber et Geoint) peut se décomposer de la manière synthétique suivante par extrapolation du cycle du renseignement :

---

[150] L'appellation et la conceptualisation du Bigdata remonteraient à octobre 1997 dans les archives de la bibliothèque numérique de *l'Association for Computing Machinery* (ACM), au sein d'articles scientifiques concernant les défis technologiques à relever pour visualiser les « grands ensembles de données »

[151] En 2017, il y aura 8.4 milliards d'*IoT*, soit une hausse de 31% par rapport à 2016. Source : Gaetan R, *plus d'objets connectés que d'humains sur Terre en 2017*, objetconnecte.com, 8 février 2017.Disponible sur http://www.objetconnecte.com/gartner-objets-connectes-milliards-0802/, consulté le 09 février 2017.

[152] Lors du crash toujours inexpliqué du vol Malaysia Airlines MH370 du 08 mars 2014, l'opinion publique découvrait que les moteurs d'un avion envoyaient automatiquement par liaison satellite des données techniques (température, usure, consommation…) à son constructeur, afin que celui-ci puisse planifier ses travaux de maintenance. Sachant qu'en 2014, un avion décollait toutes les secondes environ dans le monde, cela faisait 37,4 millions de vols sur l'année, en croissance permanente… comme le volume de données générées !

[153] Le 23 octobre 2015 à Arcueil, la DGA TIM - Traitement de l'Information Multi-Modale a organisé un colloque étendu aux technologies, infrastructures et applications du Bigdata, en plus des traitements automatiques des Langues (TAL) et les traitements d'images.

[154] Voir annexe 8. D'après le calcul effectué par le cabinet Vanson Bourne, dans le monde, l'ensemble des dépenses consacrées au Bigdata, dans les budgets IT des grandes entreprises, devrait représenter un quart du budget total IT en 2018. Cap Gemini a aussi commandité une étude en mars 2015. Le résultat a montré que 61% des entreprises sont conscientes de l'utilité du Bigdata en tant que « moteur de croissance à part entière »

- Orienter, veiller (large spectre), surveiller (une cible précise) et collecter ;
- Mettre en forme (conversion, association de métadonnées), indexer et stocker ;
- Traiter (traduire, transcrire, identifier, associer…) ;
- Rechercher (faire émerger des tendances par requête, rebond, critères…) ;
- Exploiter, Visualiser.

C'est bien l'indispensable besoin d'automatisation des tâches de collectes, de fusion et d'analyse (*analytics*) des informations qui nous a amené sur la voie du Bigdata, mais ce serait commettre une erreur que de se limiter à ce seul aspect. Le Bigdata se cache en effet dans le détail de la mise en œuvre de chacune de ces étapes (les fonctions) qui seront propres à chaque organisation selon ses besoins et, dans notre cas, couvertes par la confidentialité.

Ensuite, plus conceptuellement, le Bigdata doit amener les acteurs de la Défense à penser autrement les chaines de traitement de l'information, en les invitant à décloisonner les compétences et à raisonner de manière transverse. Par exemple, un algorithme de traduction en cyber pourrait servir à la traduction des couches vectorielles du Geoint. Mais après plusieurs échanges avec les experts en charge de la prospective de ce domaine, nous arrivons au constat que les approches Bigdata sont particulièrement bien adaptées pour améliorer les chaînes de traitement de grandes masses de données, sur lesquelles on viendrait appliquer des traitements automatiques et/ou des algorithmes d'intelligence artificielle (IA)[155]. Mais avec le Bigdata, il s'agit également de permettre une action dans un cadre prédictif[156] ou de rechercher des signaux faibles. Les algorithmes (à réaliser, et c'est bien là tout l'enjeu) ou IA, pourraient ainsi alerter automatiquement les agents du renseignement

- d'une anomalie par des approches statistiques, par comparaison avec des suites d'évènements ayant déjà eu lieu (en application de l'approche déterministe de causalité), ou par détection d'anomalies infimes au sein d'un flux global de données et prévenir ainsi de l'imminence d'une potentielle attaque Cyber complexe.
- ou au contraire, par une approche différentielle ou par comparaison de modèles issus du *Datamining*[157], faire remarquer que la chute massive d'activité dans une zone

[155] DGA-Lab Paris (fonctionnement similaire aux Fabs Labs) s'intéresse également aux apports de l'Intelligence Artificielle, notamment appliqués à la Cybersécurité (Prévention, détection, réaction).

[156] L'approche prédictive, en fonction des données capitalisées, va identifier des trajectoires futures possibles, sans pour autant les garantir, comme l'illustre la théorie du Cygne noirs du philosophe Nassim Nicholas Taleb.

[157] *Data Mining :* cet outil de prospection du Bigdata est à même de trouver des structures originales et d'établir des corrélations informelles entre les données, donc de déterminer des « motifs » réguliers dans les données. Le secteur commercial est très consommateur de cet outil.

habituellement très dynamique peut laisser présager d'un évènement grave (répression féroce, nettoyage ethnique…).

Le côté massif du Bigdata n'est alors plus donné par les entrées du système, mais par l'étendue du champ d'exploration, ce que le Geoint et le Cyber traduisent parfaitement dans leurs disciplines numériques transfrontalières.

On comprend ainsi par ces exemples que le champ du possible offert par les technologies du Bigdata est sans limites, l'important étant de bien définir les besoins des Armées dans ce domaine. Pour aider à la réflexion, le Geoint et la Cyber semblent apparaitre comme deux disciplines, certes encore peu matures, mais qui préfigurent ce que le renseignement fusionné issu des données numériques pourra être demain : une seule et unique intelligence, transverse et multisources, capable de suivis multiples et de prédiction, abolissant au besoin les frontières à la fois géographiques et temporelles (*time line*) pour les besoins opérationnels, et aptes à proposer des produits de synthèses directement exploitable par le chef militaire.

CONCLUSION

Le Cyber militaire français est un capteur de renseignement et un échelon autonome de synthèse en pleine structuration, et totalement opérationnel au sein de la fonction « connaissance et anticipation » des Armées. Il est apte à œuvrer efficacement avec des modes opératoires inédits pour aider le chef militaire à connaître son ennemi, quel qu'il soit. Mais le Cyber est aussi un effecteur, une arme redoutable, pouvant réduire au silence un ennemi, de manière autonome ou fortement concourante. De la même manière, le Geoint et ses formidables capacités de fusion de données offrent aux décideurs, militaires notamment, des outils numériques de compréhension du champ de bataille jusqu'alors inimaginables et particulièrement pertinents. Le Geoint permet, par l'exploitation croisée permanente de tous types d'informations, de concentrer les efforts sur une cible identifiée, afin d'offrir à son encontre des modes d'actions cinétiques ou numériques au décideur.

Ces deux capacités œuvrant par essence sur le même monde interconnecté de nos sociétés modernes, ce mémoire révèle de nombreuses opportunités offertes par le Cyber et le Geoint, d'abord séparément puis dans une recherche commune et prospective inédite d'effets. Il signale également dans son travail de recherche, et de réflexion complémentaire à l'existant, les risques induits et les limitations constatées dans un milieu où l'outil militaire peine à reprendre la main sur l'expression et la satisfaction de son propre besoin.

Pour reprendre l'initiative, l'avenir des opérations militaires pourrait aussi passer par un rapprochement opportuniste et inédit du Cyber et du Geoint. Au premier la force de ses attaques pour traquer la donnée de valeur chez l'ennemi, l'analyser et identifier ses vulnérabilités majeures. Au second, le Bigdata, l'intelligence artificielle et les prédictions pour épauler l'exploitation et la fusion des données toujours plus nombreuses, avec un appui Cyber indispensable pour protéger les bibliothèques de savoirs acquises. Ainsi, la conjugaison de ces deux talents permettra d'aider le chef militaire à agir, dans une logique de ciblage toujours plus efficace, sur la vulnérabilité ennemie majeure identifiée et caractérisée, dans une parfaite compréhension à la fois des enjeux et des répercussions de l'action envisagée, notamment au sein des populations. Une sorte d'approche globale, mais numérique…

Cyber et Geoint militaires, quelles contributions pour un décideur ?

Etude comparée France – Etats-Unis

TABLE DES MATIERES

SOURCES ET BIBLIOGRAPHIE

1. Sources primaires

F. Hollande, Présidence de la République, et Commission du livre blanc sur la défense et la sécurité nationale. *Livre blanc sur la Défense et sécurité nationale 2013*, 2013, Paris: documentation française, 142p.

F. Hollande, Présidence de la République, *programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale*, Texte de loi n°2013-1168 du 18 décembre 2013, JORF n°0294 du 19 décembre 2013, Paris, page 20570.

GCA C.Gomart, *rapport d'audition de la commission sénatoriale des affaires étrangères, de la Défense et des Forces Armées*, Sénat, mercredi 8 avril 2015 9h30. URL : http://www.senat.fr/compte-rendu-commissions/20150406/etr.html

J.Y Le Drian, Ministre de la Défense, discours prononcé sur le site de DGA-MI à Bruz le 12 décembre 2016. URL : http://www.defense.gouv.fr/ministre/prises-de-parole-du-ministre/prises-de-parole-de-m.-jean-yves-le-drian/cyberdefense-discours-de-jean-yves-le-drian-lundi-12-decembre-2016, consulté le 13 décembre 2016.

Department of Defense, *Joint-Publication 3-12 (R), Cyberspace Operations »*, version du 05 février 2013, 70 p.

Department of Defense, *Joint-Publication 2-03, Geospatial INtelligence in Joint Operations*, version du 31 octobre 2012, 136p.

2. Sources secondaires

a. Ouvrages

A. Bonnemaison, S. Dosse, *Attention Cyber ! : Vers le combat cyberélectronique*, Economica, 2014, 224p.

B.Boyer, *Cyberstratégie : l'art de la guerre numérique*, Nuvis, 2012, 235p

J.P Dunne, *The Defense Industrial Base*, Handbook of Defense Economics, Vol.1, Elsevier, 1995, 606P.

Instruction ministérielle N°900/DEF/CAB/*Diffusion Restreinte* du 26 janvier 2012 relative à la protection du secret de la défense nationale au sein du ministère de la défense, Ministère de la Défense, Paris.

CDEF, Les Forces Terrestres et le cyberespace, Mai 2014, Cahiers du Retex/Recherche, EMA, 92p.

PIA 5(B)_PNO(2014), *planification du niveau opératif : guide méthodologique*, CICDE, Ministère de la Défense, lettre n°152/DEF/CICDE/NP du 26 juin 2014, 136p.

J. Henrotin, *La technologie militaire en question – le cas américain*, Economica, 2008, 300p.

F.Lasserre et E.Gonon, *Manuel de géopolitique: enjeux de pouvoir sur des territoires*, A. Colin, Reédition 2e édition 2016, 368p.

O. Zajec, *Introdution à l'Analyse géopolitique : histoires, outils, méthodes*, Ed. du Rocher. 2016, 249p.

J.R Clapper, *DNI, Intelligence Community - Information Technology Enterprise 2012-2017*, Leading Intelligence Integration, 2012, 20p.

JIE 101, *Enabling the Joint Information Environment - Shaping the Enterprise for the conflicts of Tomorrow*, Defense Information Systems Agency, 5 mai 2014, 28 p.

E. Tikk-Ringas, *Evolution of the cyber domain: the implications for national and global security*, Abingdon, New York: Routledge, for the International institute for strategic studies, 2015, 212 p.

C.Bronk, *Cyber threat: the rise of information geopolitics in U.S. national security*, Santa Barbara, California: Praeger, 2016, 232 p.

L.Baudin, *Les cyber-attaques dans les conflits armés : qualification juridique, imputabilité et moyens de réponse envisagés en droit international humanitaire*, Paris : l'Harmattan, 2014, 246 p.

O.Kempf, FB Huyghes et N.Mazucchi, *Gagner les cyberconflits, au-delà du technique*, Economica, 2016, 175p

H. Coutau-Bégarie, *Traité de Stratégie*, Economica, 1999, 1200p.

Y.Lacoste, *La géographie, ça sert, d'abord, à faire la guerre*, Paris, Maspéro, 1976 187p.

M. Lowenthal, *Intelligence: From secrets to policy*, Los Angeles, Sage, 6e Edition, 2015, 534p. *Consulté à la Royal Military Academie, Shrivenham – Angleterre.*

B.Akhgar, G.B. Saathoff, H.R Arabnia, R. Hill, A. Staniforth et P. Bayerl, *Application of Big Data for National Security: A pratitioner's Guide to Emerging Technologies*, Butterworth-Heinemann, 2015, 316p. *Consulté à la Royal Military Academie, Shrivenham – Angleterre*.

b. Presse

Quotidien New-York Times, Etats-Unis, nombreux articles.

Quotidien Le Monde, France, nombreux articles.

Hebdomadaire Le Point, France

Notamment le n°2316 *le jour où Internet s'arrêtera- la nouvelle Cyberguerre mondiale* du 26 janvier 2017.

Hebdomadaire Air&Cosmos, France, nombreux articles.

Hebdomadaire Lettre d'informations stratégiques et de défense TTU, nombreux articles.

Mensuel DSI – Défense et Sécurité Internationale, France

Notamment DSI hors-série N° 52 *Cyberguerre, l'heure de l'action*, Février-mars 2017, publié le 31 janvier 2017.

c. Etudes et publications

A. Desforges, *Cyberespace et Internet : un réseau sans frontières ?*, CERISCOPE Frontières, 2011, URL : http://ceriscope.sciences-po.fr/content/cyberespace-et-internet-un-reseau-sans-frontière

B. Schütze, *Internet à la croisée des chemins — néocolonisation dans le cyberespace ou terrain de résistance*, Inet 96, Inter : art actuel, Numéro 66, 1996, p. 59-60, URI : http://id.erudit.org/iderudit/46421ac

CEIS, *Observatoire du monde Cybernétique*, DAS, Mars 2014, 25p

F.B Huyghe, *Cyberespace : le temps de l'après Snowden*, IRIS-Observatoire géostratégique de l'information, Paris, Mars 2014, 20p.

LCL H. de Lavaissière, *La nouvelle arme Cyber se construit au sein de l'US Army*, Cahier du CESAT, 2015, 3p

E. Tenenbaum, *Le piège de la guerre hybride*, IFRI, 2015, 51p.

H. Buenavida, *la simulation opérationnelle au profit de l'armée de Terre*, CDEC, URL : http://www.penseemiliterre.fr/la-simulation-operationnelle-au-profit-de-l-armee-de-terre_2013663.html.

L. Ming P.Y Fang, *Visualization Emergency Research Based on Mobile Mapping Technology. Cybernetics and Information Technologies*, Journal of Institute of Information and Communication Technologies of Bulgarian Academy of Sciences - Special Issue on Logistics, Informatics and Service Science, 2015, vol. 15, no 6, 239p.

A. Liège, *De l'action militaire à l'après-guerre, une gestion toujours conflictuelle de l'espace : L'exemple des guerres du Golfe*, Revue Géographique de l'Est,, vol. 51, 1-2, 2011

DGA, *PP30 – plan prospectif à 30 ans*, Ministère de la Défense, 2009, 784p.

Research on Laser Range Scanning and Its Application, Geospatial Information Science, Vol. 4, 2001, No 1, pp. 37-42.

EMA, *Pacte Défense-Cyber, Ministère de la Défense-Dicod, 07 février 2014*, 22p.

Col O.Thibesard, *Rapport d'étude relatif à la cyberconflictualité dans les opérations interarmes*, CDEF, Division doctrine, Paris : CDEF, 2014. - 1 vol., 83 p.

Col R.E Barrowman, *Geospatial Intelligence: The New Intelligence Discipline*, ndupress.du.edu, .US Joint Forces Command, Norfolk, 2007, 6p. URL : http://www.dtic.mil/dtic/tr/fulltext/u2/a480963.pdf

M.G.Lee, *Geospatial Intelligence (GEOINT) and Intelligence Surveillance and Reconnaissance (ISR) convergence*, SPIE Defense, Security, and Sensing, Vol. 8740, 16/05/2013, 8p.

N. Tandarić, *Geospatial Intelligence: A Review of the Discipline in the Global and Croatian Context*, Kartografija i geoinformacije (Cartography and Geoinformation), 2015, vol. 14, n) 23, p. 38-49.

P.Boulanger, *La géographie militaire I*, Revue stratégique, n° 81, 184p.

P.Boulanger, *La géographie militaire II*, Revue stratégique, n° 82-83, 246p.

d. Sites Internet

Notions sur le Geoint :

- https://www.e-education.psu.edu/
- http://www.ente-aix.fr

- http://www.portailsig.org/
- http://www.ens-lyon.fr

Documentation, acteurs et offres commerciales Geoint

- http://www.esri.com
- http://www.qgis.org
- http://www.usgif.org (nombreux rapports)
- http://geoint2016.com
- https://www.nga.mil/

Nombreuses analyses factuelles des blogs spécialisés sur le Défense :

- T.Lagneau, Zone Militaire, URL : http://www.opex360.com/
- J.D Merchet, Secret Défense/L'Opinion,URL : *www.lopinion.fr/blog/secret-defense*

e. Témoignages et entretiens recueillis

Pour préserver l'indispensable sécurité des officiers rencontrés au cours de mes recherches, aucun nom ne sera publié. Je tiens cependant à les remercier chaleureusement pour leur soutien et le concours précieux de leurs témoignages notamment pour les aspects prospectifs. Seules les affectations génériques seront donc citées :

- DRM/CRAC – Creil.
- DRM/CRGI – Creil
- EMA/CPCO - Balard
- DRM - Balard

ANNEXES

Table des matières :

Annexe 1

Les dispositifs d'aide à l'innovation de la DGA

Pour préparer le futur des systèmes de Défense et équiper les forces Armées, et animer la sphère économique et civile notamment du Cyber et du Geoint français, développer les solutions innovantes et stimuler la recherche nationale, la DGA dispose de plusieurs **outils financiers :**

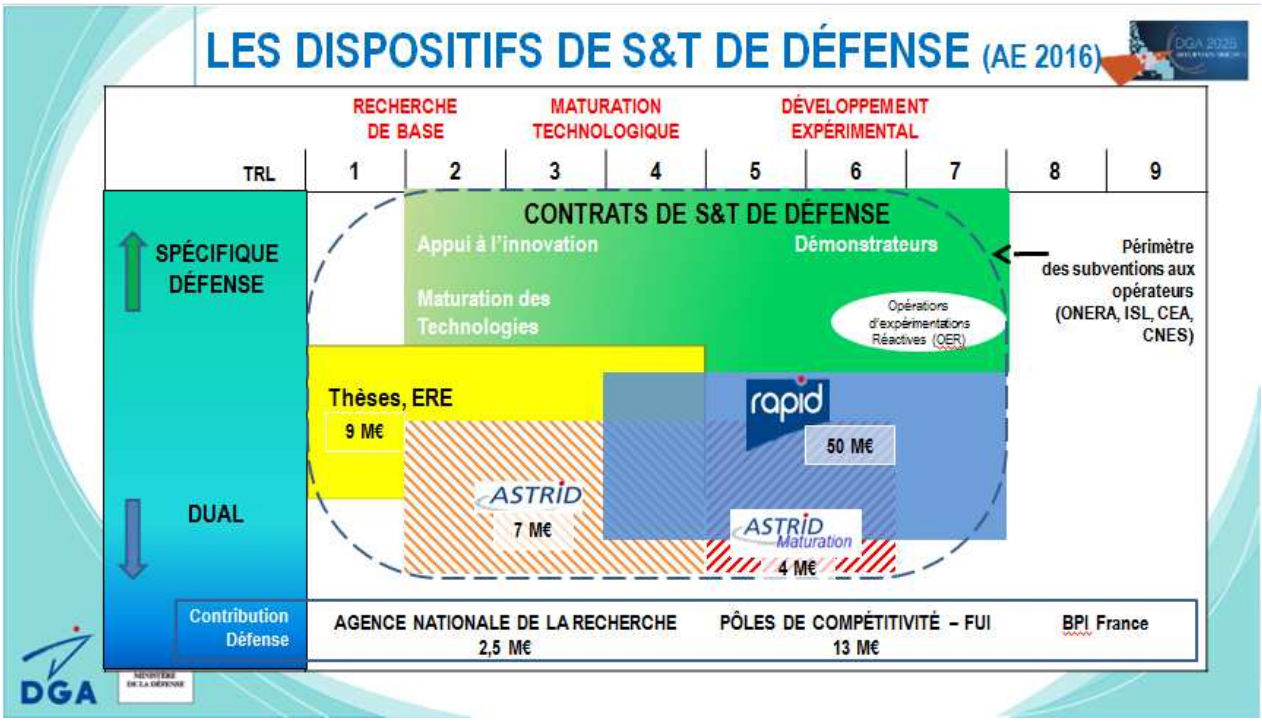


Figure 4: Orientation de la S&T de défense - Les outils de l'innovation.

Source : Conférence à l'Ecole de Guerre de l'Ingénieur Général Hors Classe N. FARGERE, Chef de l'Inspection de l'Armement, 07/02/2017, Paris.

- le dispositif Rapid (Régime d'Appui à l'Innovation Duale) finance les idées françaises détectées comme innovantes au sein de laboratoires universitaires, et appuie ainsi l'innovation duale des PME et ETI[158] (thèses[159], recherches, publications). Doté de 40M€ en 2013, de 45M€ en 2014, il atteint depuis 2015 une dotation annuelle de 50M€, permettant de soutenir 62 projets en 2015.
- le dispositif Astrid (Accompagnement Spécifique des Travaux d'Innovation de Défense) favorise le transfert de technologies des laboratoires de recherches vers les PME. Ce dispositif a financé depuis 2013 pas moins de 25 projets par an.

[158] PME/ETI : petites et moyennes entreprises, entreprise de taille intermédiaire.
[159] DGA a financé environ 137 nouvelles thèses de doctorat dans 10 domaines scientifiques, avec un taux de sélection de global de 29% (source : DGA, 2017).

- un fond d'investissements complémentaire, doté de plusieurs millions d'euros est en cours de création par le MINDEF et la DGA pour protéger les PME innovantes nationales des investissements étrangers, dans une logique de préservation des « pépites » industrielles françaises et stratégiques et d'identification des capacités industrielles souveraines[160].
- Enfin, le pacte défense-PME renforce également le rôle des PME innovantes en leur facilitant notamment l'accès au marché difficile et codifié de la Défense.

[160] Voir à ce sujet le rapport d'information n° 634 (2011-2012) de MM. Daniel REINER, Yves POZZO di BORGO, Jacques GAUTIER, Alain GOURNAC, Gérard LARCHER, Rachel MAZUIR, Jean-Claude PEYRONNET et Gilbert ROGER, fait au nom de la commission des affaires étrangères et de la défense, déposé le 4 juillet 2012.

Annexe 2

L'USCYBERCOMMAND

1. Missions

USCYBERCOM (ou USCYBERCOMMAND) planifie, conduit et coordonne les activités Cyber pour sécuriser, mettre en œuvre et défendre les réseaux du DoD et garantir sa liberté d'action dans le cyberespace. Il s'agit comme en France du volet LID. Ses missions sont aussi d'interdire cette même liberté d'action aux adversaires, et sur ordre, de conduire un large spectre d'actions offensives pour dissuader ou détruire toute menace stratégique contre les intérêts américains et ses infrastructures. Il s'agit alors du volet offensif (LIO).

Figure 5:Missions USCYBERCOM. Source : USCYBERCOM (unclassified)

2. Organisation

Véritable Etat-major militaire dédié à l'objet Cyber, l'USCYBERCOM, commandé actuellement par l'Amiral Michael S.Rogers (*USN*), intègre toutes les fonctions d'un EM (J1 à J8), une réserve opérationnelle dédiée et surtout un CO en charge du suivi des opérations Cyber.

L'interconnexion avec la NSA (capacités techniques, équivalentes de la Direction Technique de la DGSE française) sont très fortes. De plus, les liens opérationnels Cyber sont également très étroits avec le DOJ (*Department of Justice*)/FBI, le DHS (*US Department of Homeland Security – le CERT américain*) et le DoD.

Figure 6: Organisation USCYBERCOM. Source : USCYBERCOM (unclassified)

3. Pour l'anecdote : le logo…

Figure 7 : logo d'USCYBERCOMMAND

Le logo d'USCYBERCOMMAND comporte une série de chiffres dans sa couronne dorée intérieure : 9ec4c12949a4f31474f299058ce2b22a..

En y appliquant la fonction informatique md5sum[161], voici le résultat :

~> echo -n "USCYBERCOM plans, coordinates, integrates, \ synchronizes and conducts activities to: direct the \ operations and defense of specified Department of \ Defense information networks and; prepare to, and when \ directed, conduct full spectrum military cyberspace \ operations in order to enable actions in all domains, \ ensure US/Allied \ freedom of action in cyberspace and \ deny the same to our adversaries." | md5 9ec4c12949a4f31474f299058ce2b22a[162]. Il s'agit d'un des libellés de la mission du CYBERCOMMAND (cf §1.)

[161] Md5sum est une commande Unix standard qui calcule une "empreinte digitale" de 128 bits d'une chaîne de caractères quelqu'en soit sa longueur.. C'est une fonction de hachage dont le principal usage est le contrôle d'intégrité de fichiers numériques (par comparaison du hash md5, celui-ci étant par définition unique). Cette propriété est également très utile dans ses nombreuses applications en cryptographie.

[162] Anonyme, *USCYBERCOM Secret revealed*, UMBC ebiquity, 8 juillet 2010, http://ebiquity.umbc.edu/blogger/2010/07/08/uscybercom-secret-revealed/, consulté le 10 octobre 2016.

Annexe 3

Organisation de la Direction du Renseignement Militaire

1. Organisation générale

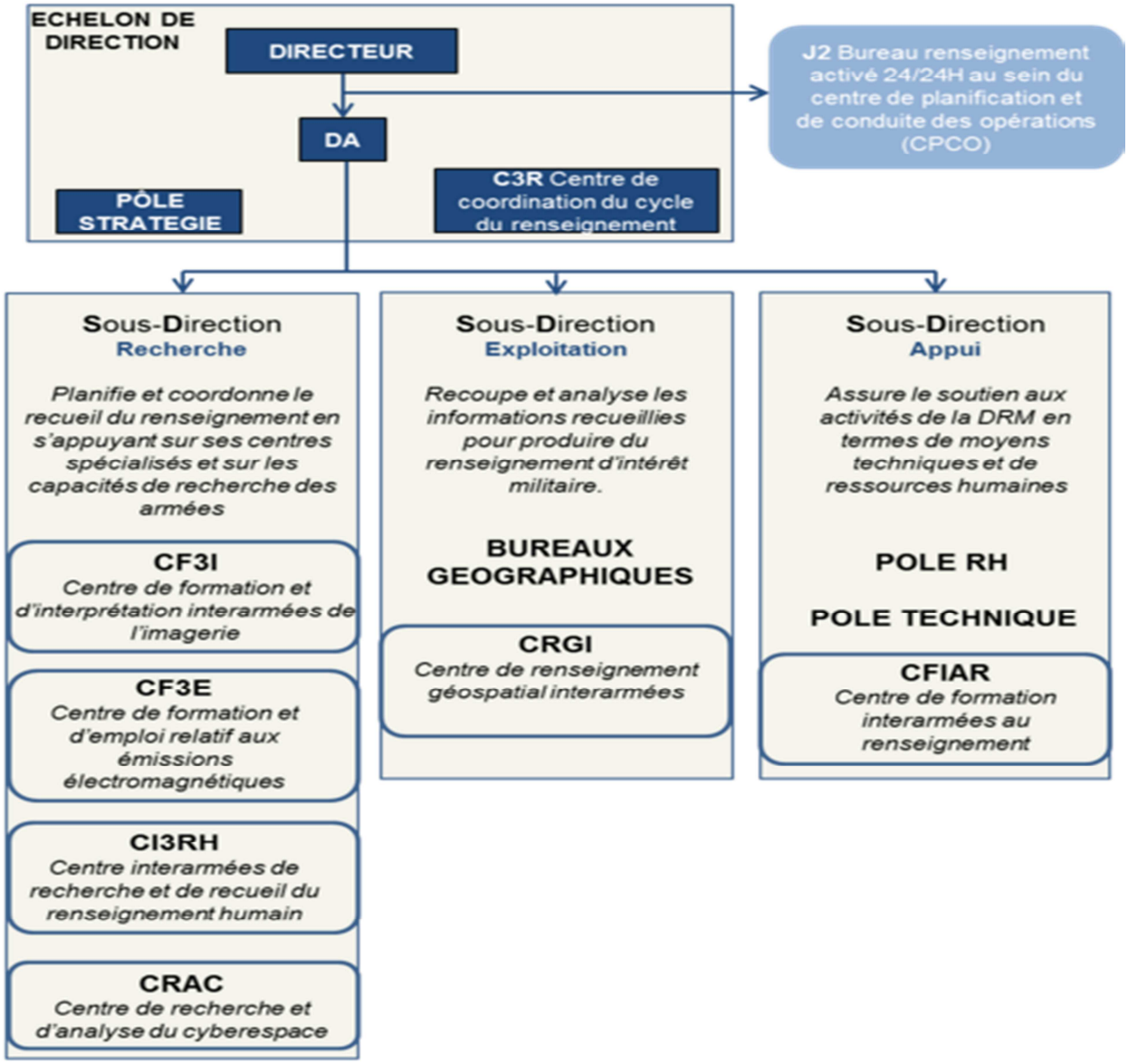


Figure 8 : source : EMA. Disponible sur http://www.defense.gouv.fr/ema/interarmees/la-direction-du-renseignement-militaire/la-drm/organisation/organisation, consulté le 20/12/2016

2. Les 6 centres de la DRM

CF3I : Centre de formation et d'interprétation interarmées de l'imagerie.

- **Recueille de l'information** d'origine image
- **Forme** les interprètes images des armées françaises et de l'OTAN
- **Définit des besoins** et le maintien à niveau des capacités

Organisme spécialisé créé le 1er septembre 1993 par la fusion d'unités de trois armées, le CF3I est une référence nationale dans le domaine du renseignement

d'origine image (ROIM).

CF3E : Centre de formation et d'emploi relatif aux émissions électromagnétiques

- **Oriente** les capteurs d'écoute
- **Forme** les personnels des armées dans le domaine électromagnétique
- **Analyse et exploite** la production en renseignement d'origine électromagnétique (ROEM)
- **Met à jour** le référentiel technique national militaire

Les interceptions ROEM peuvent être réalisées par des capteurs spatiaux ou des moyens spécialisés mis en œuvre par les armées. Elles nécessitent la maîtrise de techniques de haut niveau dans le domaine des télécommunications, de l'informatique, de l'électronique, du traitement du signal, de la cryptologie et de la traduction.

CI3RH : Centre interarmées de recherche et de recueil du renseignement humain

- **Recueille et analyse** le renseignement d'origine humaine (ROHUM).
- **Forme** les spécialistes en renseignement humain des armées avant leur envoi en mission
- **Déploie des spécialistes** de haut niveau sur les théâtres d'opération

Le CR3RH est en outre chargé de la gestion centralisée des sources humaines.

CRAC : Centre de recherche et d'analyse du Cyberespace

- Mène une **recherche numérique** spécialisée
- Recherche sur les **réseaux sociaux**
- **Evalue la menace** et les systèmes d'armes adverses

CRGI : Centre de renseignement géo-localisé interarmées

- Fusionne le renseignement issu des **différents capteurs**

CFIAR : Centre de formation interarmées au renseignement

- Assure la **formation au renseignement d'intérêt militaire**, dans un cadre national ou multinational, et l'apprentissage des langues nécessaires au renseignement

Annexe 4

Exemples de productions Geoint civils

1. Imagerie radar SAR :

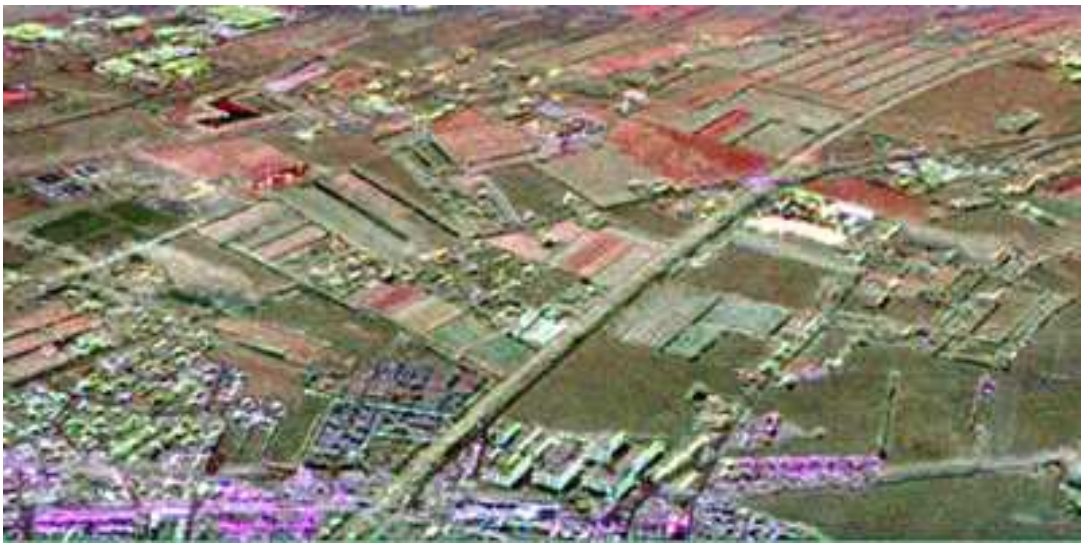


Figure 9: imagrie SAR. Source : ONERA, http://www.onera.fr/fr/imagedumois/image-radar-sar

En technique radar, la résolution angulaire d'une antenne est inversement proportionnelle à sa taille. La technique SAR (*Synthetic Aperture Radar*) ou radar à synthèse d'ouverture, exploite donc le déplacement de l'antenne pour former une antenne "de synthèse" de dimension plus importante, et donc d'une résolution angulaire plus élevée que la même antenne, immobile. La grande antenne est reconstituée par traitement du signal.

Dans cet exemple, les antennes émettrice et réceptrice sont embarquées à bord d'un même avion. Leur dimension est de l'ordre de la dizaine de centimètres. La grande antenne "virtuelle", qui permet d'obtenir les images de cette page a pour longueur environ soixante mètres.

Sur l'image SAR reconstituée ici, chacune des trois couleurs correspond à une polarisation de l'onde émise et une polarisation de l'antenne de réception particulière choisies pour mettre en évidence le type d'interaction entre l'onde radar incidente et la surface rétrodiffusante. Ainsi **les zones apparaissant en marron sont plutôt des zones de sols nus, alors que les zones vertes correspondent à des surfaces de végétation. Les points bleus indiquent la présence de bâtiments ou de structures artificielles.**

L'utilisation d'ondes radar rend l'observation possible quelle que soit le temps et même de nuit.

2. Produits LIDAR

L'imagerie laser, ou LIDAR, permet de reconstituer une image thématique grâce aux propriétés optiques du faisceau et l'étude de ses modifications par réflexion (concentration de végétation, nature des sols, hydrométrie, relief précis, sous-sol…).

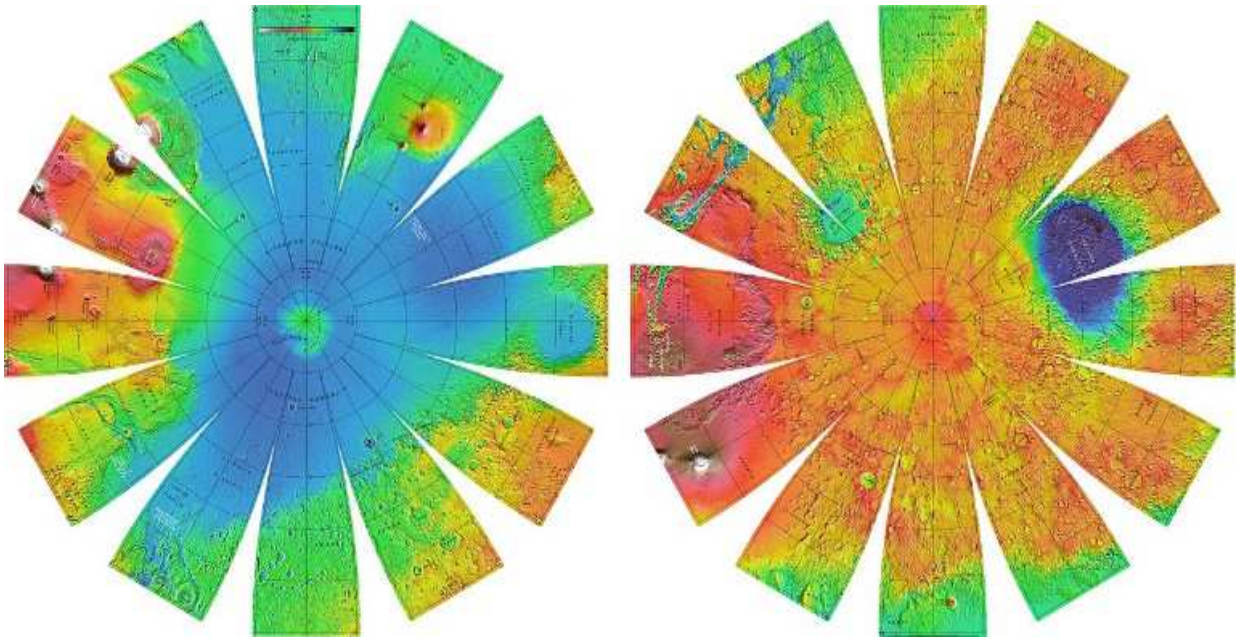


Figure 10: Cartographie de Mars par le lidar MOLA de la sonde MGS. Source : http://photojournal.jpl.nasa.gov/catalog/PIA02993

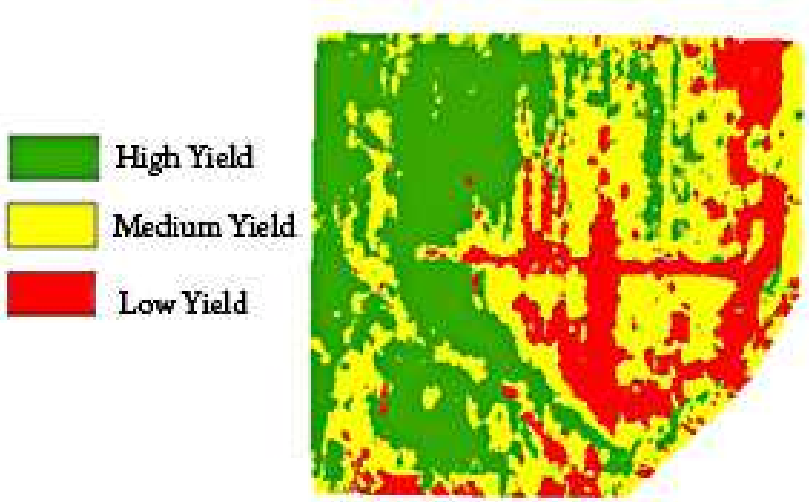


Figure 11: Carte de rendement agricole. Source : https://www.ars.usda.gov

3. Produits Geoint élaborés

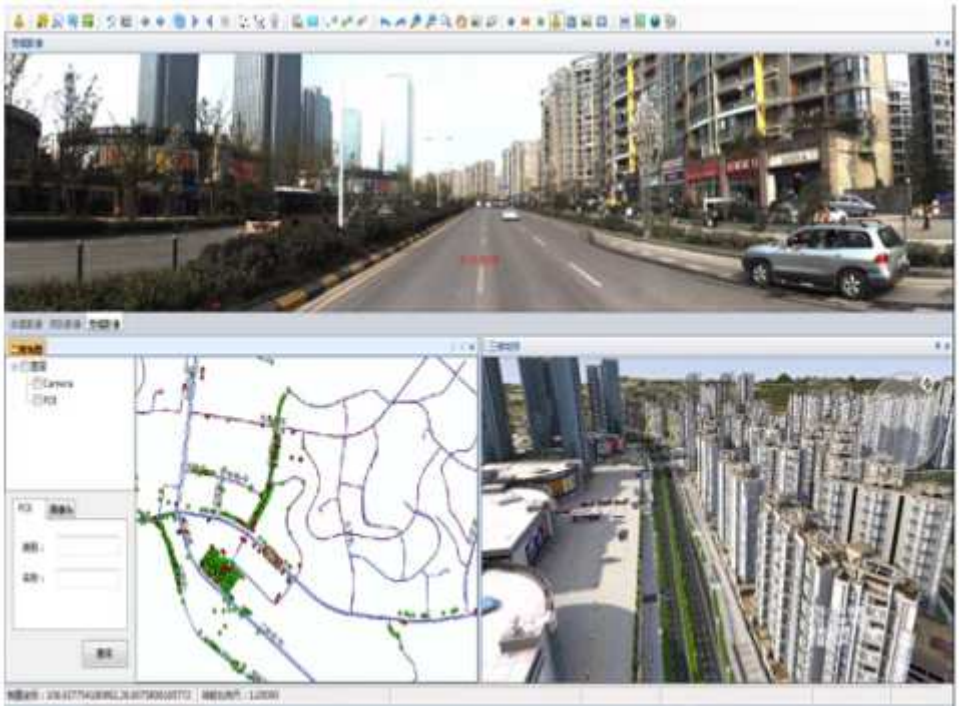


Figure 12: Solution TRUEMAP. Source: L. Ming P.Y Fang, Visualization Emergency Research Based on Mobile Mapping Technology. Cybernetics and Information Technologies, Journal of Institute of Information and Communication Technologies of Bulgarian Academy of Sciences - Special Issue on Logistics, Informatics and Service Science, 2015, vol. 15, no 6, 239p.

Figure 13: exemple d'application du Geoscoring. Source : http://www.ens-lyon.fr/recherche/lokeo-de-pablo-jensen-laureat-du-trophee-reseau-curie-2011-du-ministere-de-la-recherche-124331.kjsp

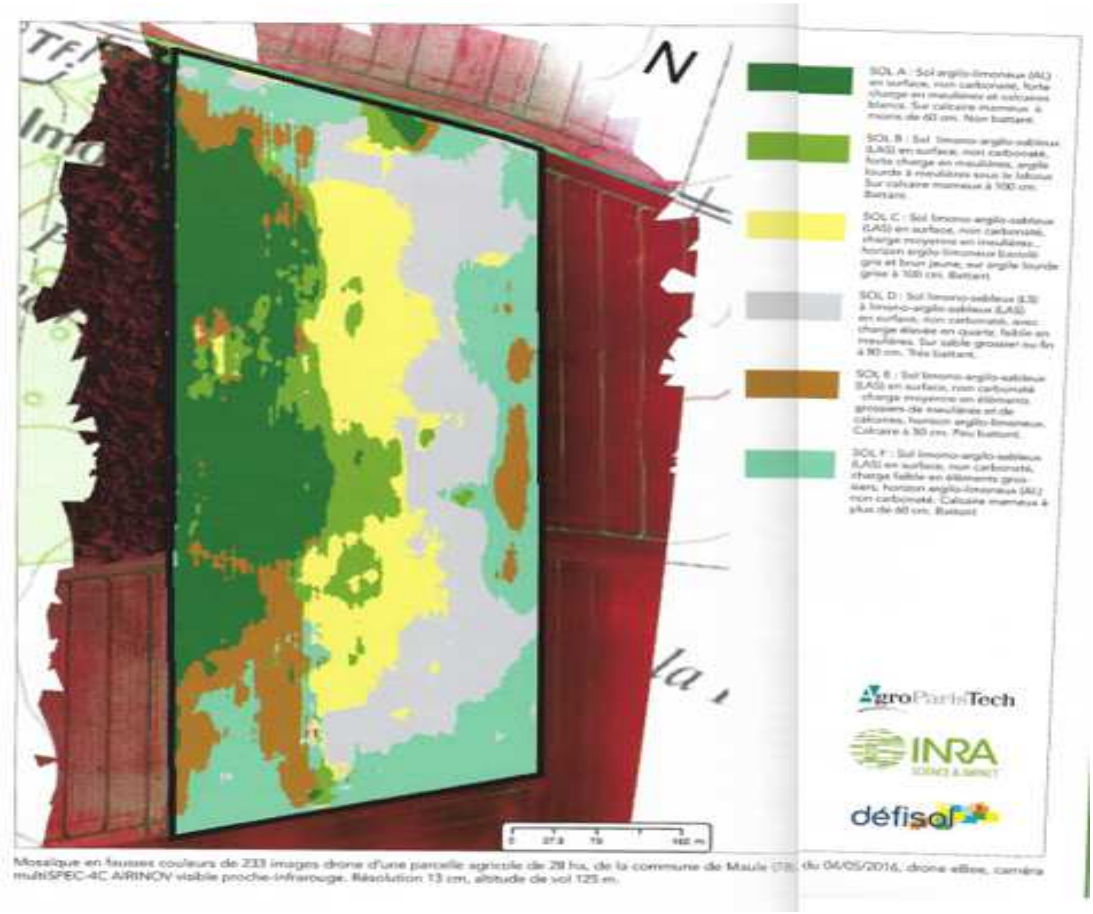


Figure 14 : Cartographie des types de sol d'une parcelle agricole par imagerie drone. Source : ESRI-France, les SIG à la carte, Vol.13, 2016.

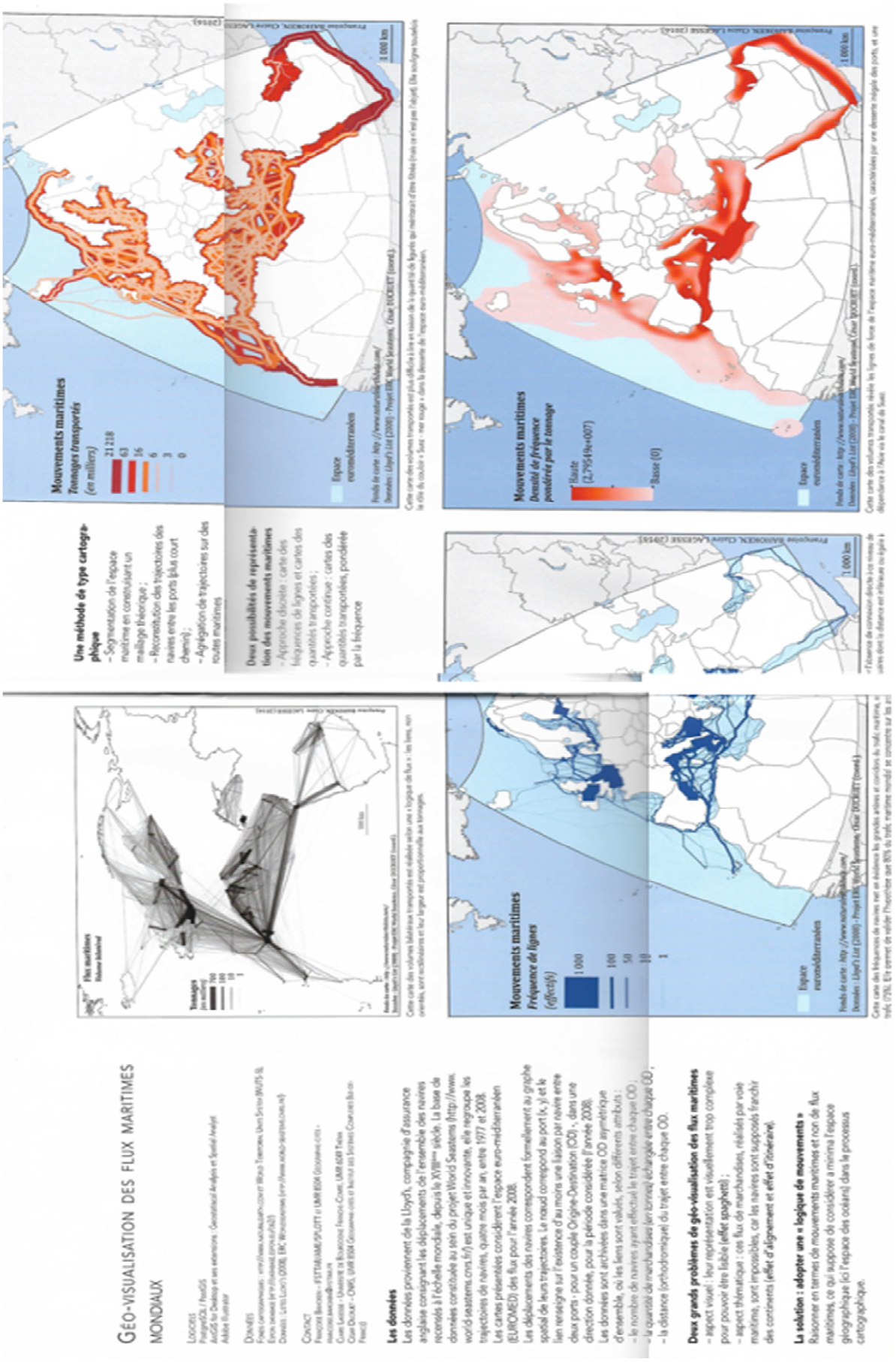


Figure 15: Geo-visualisation des flux maritimes mondiaux. Source : ESRI-France, ibid.

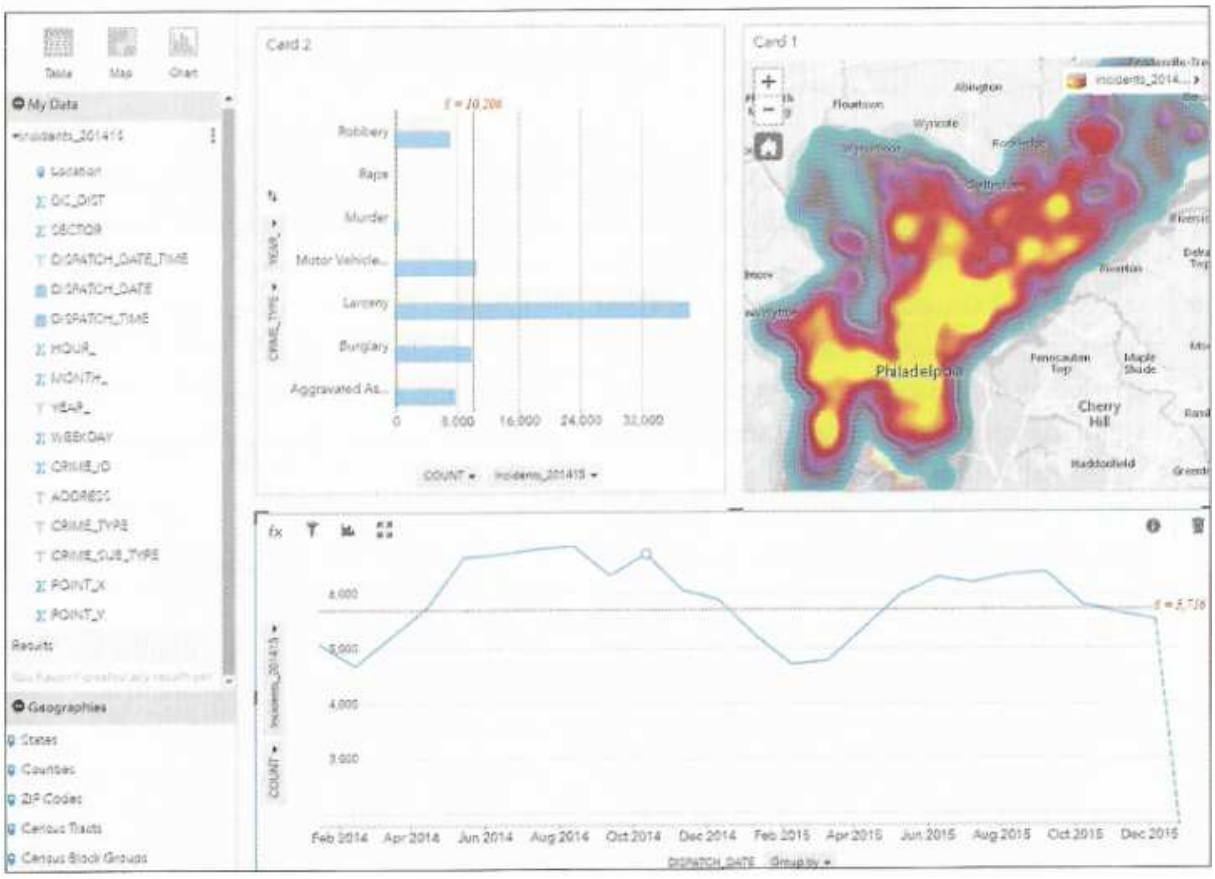


Figure 16: Capture du logiciel Insights for ArcGIS*, où les opérateurs peuvent déposer tous types de données brutes directement sur l'écran du SIG, qui les représentera sous toutes les formes possibles (tableau, cartes, diagrammes...) en vue d'une hypothétique mise en relation à développer ensuite (ici étude géographique type Police su les type de crimes commis en 2016 sur les environs de Philadelphie)*

Source : ArcGIS, ESRI, ArcNew Summer 2016, 39 pages, p5

Annexe 5

L'*United States Intelligence Community*

L'*United States Intelligence Community* (US-IC, ou IC) est un regroupement de 16 agences gouvernementales américaines, de renseignement (civils et militaires), et d'analyses (en charge de la fusion des données), autonomes dans leurs travaux sur leurs domaines de compétences, mais échangeant et se regroupant pour mener des actions de renseignement au titre de la sécurité nationale.

Son directeur, le DNI (*Director of National Intelligence)*, directement en relation avec le président des Etats-Unis, n'est autre que James R.CLAPPER, très influent directeur de 2001 à 2006 du NGA (connu jusqu'en 2003 sous l'acronyme NIMA, *National Imagery and Mapping Agency*).

Les 16+1 agences composantes l'USIC sont :

- l'ODNI (Office of the Director of National Intelligence), en charge de la coordination d'ensemble au profit des 16 agences ci-dessous ;

- les 6 agences de renseignement suivantes : la CIA (*Central Intelligence Agency*), la DIA (*Defense Intelligence Agency*), le FBI (*Federal Bureau of Investigation*), le NGA, le NRO (*National Reconnaissance Office*) et la NSA *(National Security Agency*) ;

- Les 5 agences thématiques suivantes : le DE (*Department of Energy*), le DHS (*Department of Homeland Security*), le DS *(Department of States*), le DT *(Department of Treasury*), et le DEA (*Drug Enforcement Administration*) ;

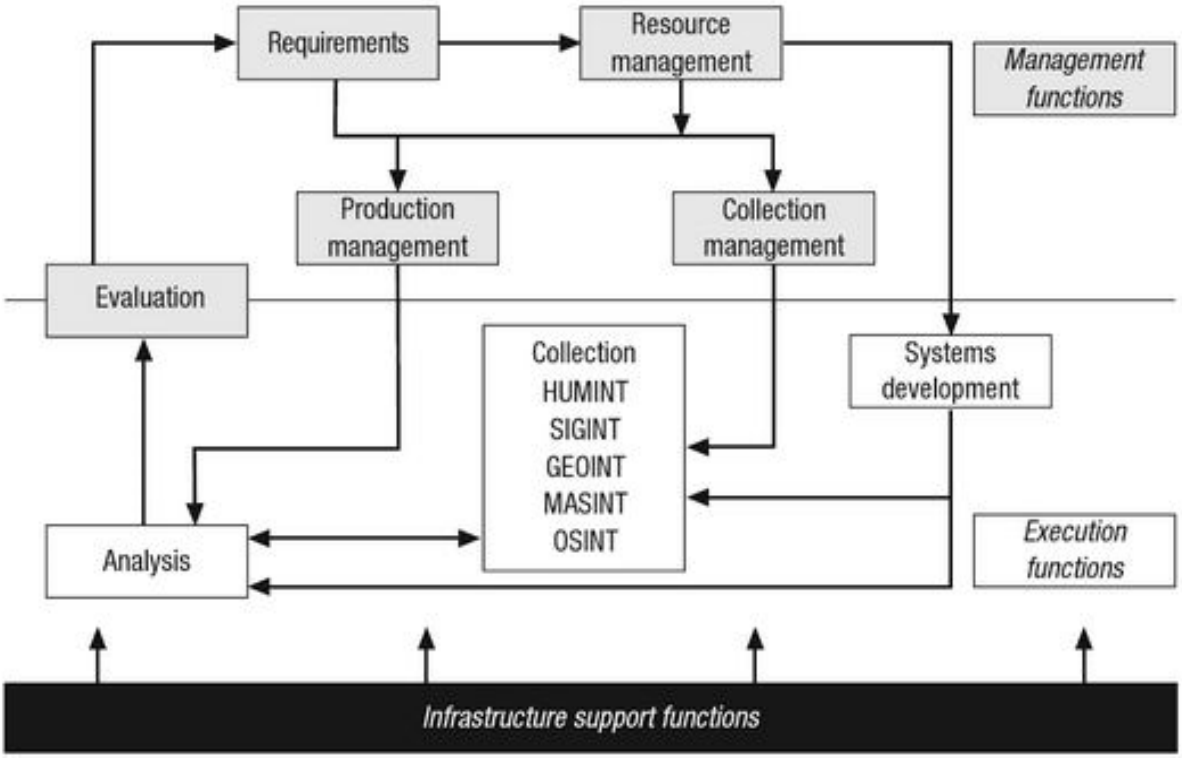
- et les 5 Armées : l'USAF (*US-Air Force*), l'US *Army*, les US *Coast Guard*, l'US *Marine Corps* et l'US *Navy*.

Figure 17: Source : https://www.intelligencecareers.gov/icmembers.html

Une autre possibilité de voir le fonctionnement de l'USCI est présentée ci-dessous. Il est intéressant d noter, et sans doute surprenant, de voir ici le Geoint positionné sur la partie

capteur (*collection*).

Figure 3-2 **Alternative Ways of Looking at the Intelligence Community: A Functional Flow View**



Source: U.S. House Permanent Select Committee on Intelligence, IC21: The Intelligence Community in the 21st Century, 104th Congress, 2d session, 1966.

Note: HUMINT = human intelligence; GEOINT = geospatial intelligence; MASINT = measurement and signatures intelligence; OSINT = open source intelligence; SIGINT = signals intelligence.

Annexe 6

Le pouvoir normatif du NSG : *Standards and the NSG Architecture*

Standards support the NSG enterprise architecture and are the basis for systems interoperability and operational efficiency.

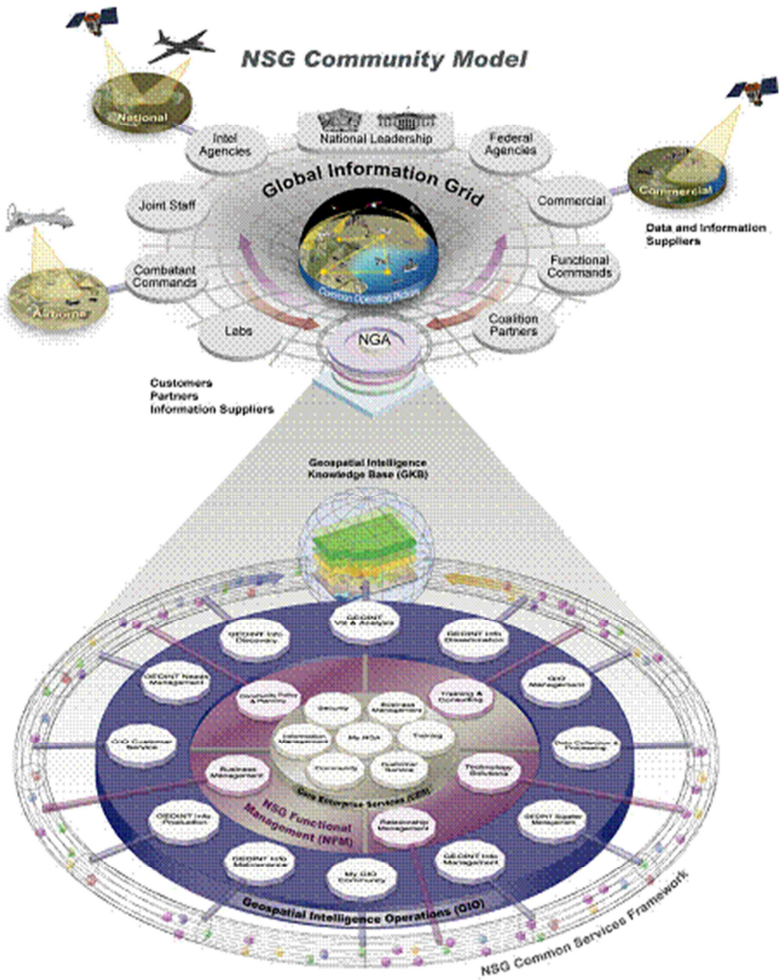


Figure 18: The use of standardized web services enables distributed dissemination of GEOINT products.

The NSG architecture defines, at varying levels, the operations and systems that are needed, from data collection to dissemination and storage, to produce the GEOINT required by the NSG community. This architecture is, in essence, a "blueprint" that functionally describes the NSG enterprise and the interconnectivity of its components.

The high-level operational architecture depicted here shows the key operational components of the NSG enterprise. Each of these components is realized through a number of technical objectives and capability goals. These objectives and capabilities, in turn, drive the need for standards that support them.

A key characteristic of the NSG architecture is that it is being defined within a service-oriented framework. A Service-Oriented Architecture (SOA) is defined in many ways, but, in general, it is an approach to finding business solutions through the use of interfaces that manage service requests and replies in a standardized way. Web services provide one technology for implementing SOAs, and they are critical components of the NSG architecture.

Source : Part 2: Overview of GEOINT Standards - On-line training modules of Geoint Standards – The Basics – GWG. Disponible sur https://fr.slideshare.net/Zubin67/part-2-overview-of-geoint-standards, slide 3. Consulté le 10 novembre 2016

Annexe 7

Les standards GEOINT du NSG

Les standards	
• Geoint metadata • Still/motion imagery content/format • Sensor modeling • Geographic feature encoding • Feature data dictionaries/catalogs • Geographic portrayal	• Geospatial referencing • Information transfer • Data compression • GEOINT reporting • GEOINT product specifications • GEOINT web services

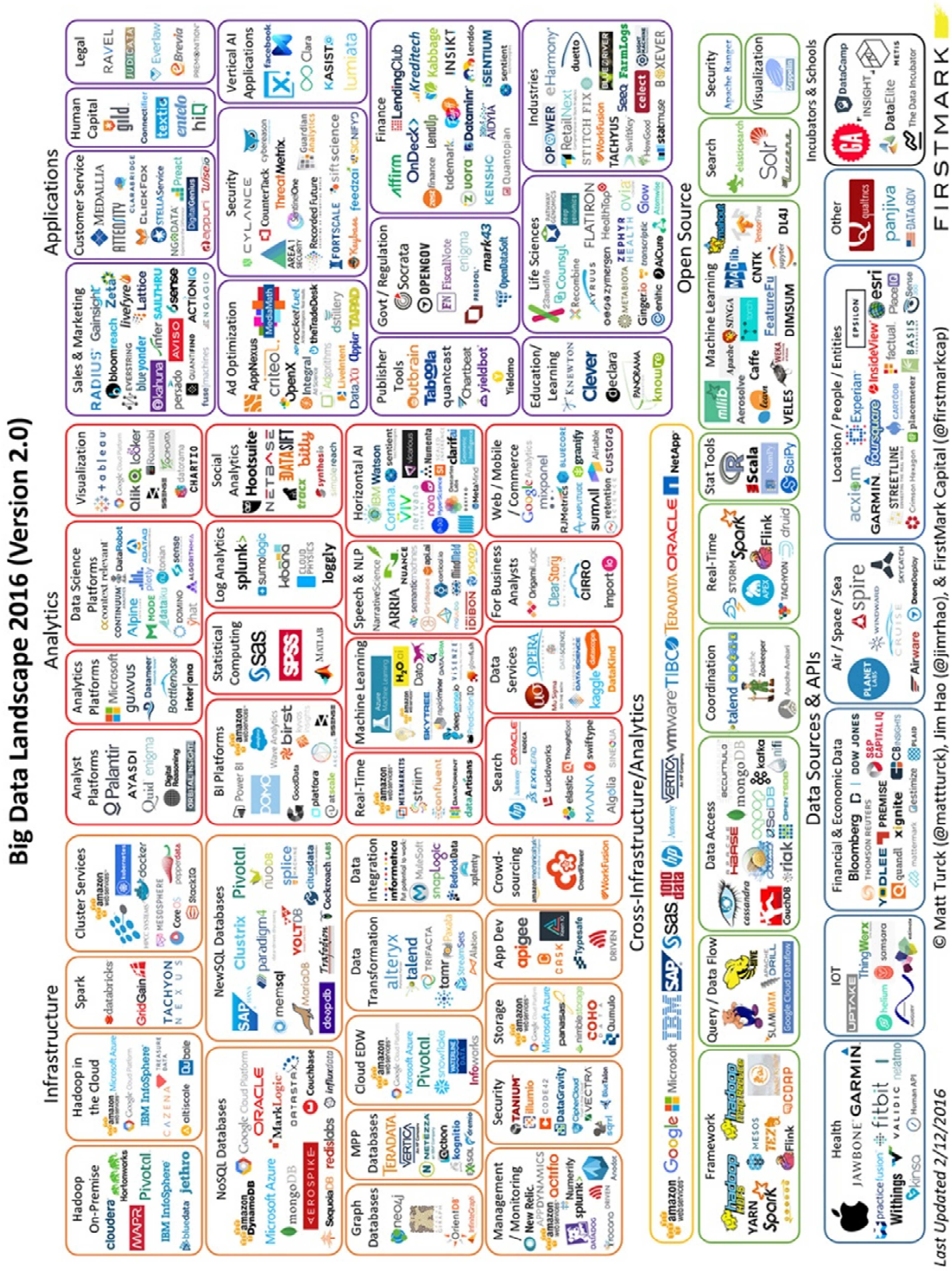
Les principales normes de référence Geoint du NSG	
OGC® Standards • Web Features Service (WFS) • Web Map Service (WMS) • Web Map Context (WMC) • Web Coverage Service (WCS) • Geography Markup language (GML) • Styled Layer Descriptor (SLD) • Catalog Services (CS-W) • Filter Encoding Specification (FE)	Other Standards • ISO 19115 Geographic Information – Metadata • ISO 19119 Geographic Information – Services • ISO/IEC 15444-1:2004 Information Technology -- JPEG 2000 image coding system: Core coding system • NSG Feature Data Dictionary (NFDD) • NSG Entity Catalog (NEC)

Figure 19 : Principaux acteurs stratégiques liés à l'activité de normes GeoInt.

Source : http://www.gwg.nga.mil/guide.php#3

Annexe 8

BigData Landscape 2016



Last Updated 2/12/2016

© Matt Turck (@mattturck), Jim Hao (@jimrhao), & FirstMark Capital (@firstmarkcap)

FIRSTMARK