Observatoire de la politique de défense américaine

JUIN 2019

Rapport n° 2/FRS/OBSUSA
de juin 2019

Marché n° 2018 1050 118 198
EJ court 180 005 17 10
notifié le 18 octobre 2018
réunion de lancement : 14 novembre 2018

Bon de commande SPAC n° 1 du 8 avril 2019
Référence CHORUS : 1404618822

La compétition dans les technologies de rupture entre les États-Unis, la Chine et la Russie

PHILIPPE GROS – NICOLE VILBOUX – FRÉDÉRIC COSTE – STÉPHANE DELORY
AVEC LA COLLABORATION D'ANTOINE BONDAZ

FONDATION pour la RECHERCHE STRATÉGIQUE

WWW.FRSTRATEGIE.ORG | 4 BIS RUE DES PATURES 75016 PARIS | TEL : 01.43.13.77.77 | MAIL : CONTACT@FRSTRATEGIE.FR

SIRET 39409553300052 TVA FR74 394 095 533 CODE APE 7220Z FONDATION RECONNUE D'UTILITÉ PUBLIQUE DÉCRET DU 26 FÉVRIER 1993

SOMMAIRE

LISTE DES ABRÉVIATIONS

ABM	*Anti Ballistic Missile*
AED	Arme à énergie dirigée
AFRL	*Air Force Research Laboratory*
APL	Armée Populaire de Libération
ARL	*Army Research Laboratory*
ASAT	Anti-satellite
ATR	*Automated Target Recognition*
A2/AD	*Anti-Access/Area Denial*
BITD	Base industrielle et technologique de défense
C4ISR	Command, Control, Communications, Computer, Intelligence Surveillance and Reconnaissance
CPGS	*Conventional Prompt Global Strike*
DARPA	*Defense Advanced Research Project Agency*
DA-ASAT	*Direct ascent ASAT*
DIU	*Defense Innovation Unit*
DMO	*Distributed Maritime Operations*
EM	Électromagnétique
GAFAM	*Google, Amazon, Facebook, Apple, Microsoft*
GBI	*Ground Based Interceptor*
GE	Guerre électronique
GEO	*Geosynchronous orbit*
HCSW	*Hypersonic Conventional Strike Weapon*
HEO	*High Elliptical Orbit*
HPM	*High Power Microwaves*
HVT	*High Value Target*
IA	Intelligence artificielle
IADS	*Integrated Air Defense System*
ICM	Intégration civilo-militaire
IRBM	*Intermediate Range Ballistic Missile*
IRCPS	*Intermediate Range Conventional Prompt Strike*
LEO	*Low Earth Orbit*
LIO	Lutte informatique offensive
LRHW	*Long Range Hypersonic Weapon*
LRPF	*Long Range Precision Fires*
MdC	Missile de croisière
MDO	*Multi Domain Operations*
NDAA	*National Defense Authorization Act*
NIFC-CA	*Naval Integrated Fires Capability - Counterair*
PNT	*Positionnement, Navigation, Timing*
ROEM	Renseignement d'origine électromagnétique
SATCOM	Satellite de communication
SCO	*Strategic Capabilities Office*
SSA	*Space Situational Awareness*
SWAP-C	*Size Weight and Power - Cooling*
TEL	Transporteur-Erecteur-Lanceur
THAAD-ER	Terminal High Altitude Area Defense, Extended Range
TRL	*Technological Readiness Level*
TST	*Time Sensitive Targeting*
USD R&E	*Under Secretary of Defense Research & Engineering*

RÉSUMÉ

L'érosion de la supériorité des États-Unis dans le domaine technologique, qui sous-tend celle de leur leadership stratégique à moyen-long terme, surtout face à la Chine, est sur toutes les lèvres outre-Atlantique. La compétition est particulièrement vive dans les dix domaines technologiques critiques identifiés par le Dr Griffin, *Under Secretary of Defense for Research and Engineering*.

Parmi ces dix domaines, les missiles hypersoniques représentent la priorité numéro 1 du Pentagone. Sur ce plan, les Russes, suivis des Chinois, sont en avance dans le domaine des missiles de croisière antinavires et des missiles quasi-balistiques aérolargués, alors que les trois compétiteurs restent au coude à coude pour parvenir à des missiles à planeur opérationnels au début des années 2020, avec des ambitions moindres pour Pékin. Les ruptures principales apportées par ces armes ont trait au contre-IADS pour les Américains et à la lutte antinavire du côté russe et chinois. Ce dernier point est probablement le plus critique car il remet en cause la supériorité navale américaine. Cependant, si aucune solution n'existe à court terme pour se défendre contre ces armements, ce sont les Américains qui sont de loin les mieux placés, tant en matière d'architecture que de missiles d'interception, pour disposer de parades efficaces à moyen/long terme, tirant partie de leurs 40 ans d'investissement massif dans la défense antimissile.

Les armes à énergie dirigée (AED) représentent un domaine technologique très particulier. Il est probable que les Chinois ne soient guère éloignés des Américains en ce qui concerne tant les armes laser que les armes électromagnétiques (EM). Dans ce dernier domaine, ils sont peut-être même en avance en ce qui concerne la protection des plateformes navales alors que les Américains semblent disposer de capacités opérationnels air-sol offensives. Cependant, en ce qui concerne les armes laser, la vulnérabilité des trois camps apparaît encore réduite. En effet, la première génération d'armes laser en cours de maturation, si son déploiement se confirme dans les 5 ans, sera destinée à la lutte anti-drones courte portée, certainement pas à stopper les vagues de missiles du compétiteur stratégique. Quant aux lasers de contre-mesure optronique, à visée antisatellite (ASAT) par exemple, ils ne constituent pas une solution miracle, un élément clé de l'arsenal anti-ISR. Il est donc possible, de prime abord, que l'impact des armes EM soit beaucoup plus important que celui des lasers dans l'environnement haute intensité qui caractérise la présente compétition.

Ces AED font partie des capacités auxquelles les compétiteurs pourraient recourir en *counterspace*. Dans ce domaine, les trois puissances disposent déjà des instruments en mesure de menacer les constellations de l'adversaire : missiles capables d'intercepter

des satellites en orbite basse, guerre électronique contre les segments de liaison voire les satellites eux-mêmes en co-orbital, maîtrise des rendez-vous orbitaux et des technologies duales de capture d'une plateforme, etc. Cette évolution constitue une rupture majeure par rapport à l'ère de l'exploitation de l'espace en toute impunité dont ont joui les Américains ces dernières décennies. Ces derniers ont cependant plusieurs avantages : une meilleure *situational awareness* du milieu spatial et surtout une résilience allant croissant : « désagrégation » des architectures fonctionnelles, redondance des communications avec le milieu aérien (*Aerial Layer Network*), exploitation des nouvelles constellations commerciales de SATCOM et de télédétection en orbite basse ou médiane, réactivité des lancements, recherche effrénée de solutions de positionnement, navigation, timing (PNT) de complément puis de substitution au GPS. Comme la Chine suit peu ou prou la même logique, il apparaît de plus en plus douteux que les deux grands puissent mutuellement s'interdire l'ensemble de leurs capacités d'ISR et de SATCOM en cas de confrontation.

Enfin, les Américains continuent de devancer largement leurs compétiteurs dans le domaine sous-marin ou en matière d'intégration des architectures C4I, que les concepts de synergie « multidomaine », mantra de leur stratégie capacitaire depuis 10 ans, entendent étendre à l'ensemble des 5 domaines de lutte et diffuser aux plus bas échelons tactiques. Compte tenu de ces paramètres, si les avancées chinoises et russes renforcent considérablement leurs aptitudes de déni d'accès aux forces américaines dans leurs atterrages, elles sont encore loin d'espérer priver Washington de sa supériorité dans le domaine conventionnel. Cependant, la modernisation continue de leur C4I, certes gage d'une efficacité opérationnelle accrue et d'une résilience renforcée par la distribution des éléments, expose toujours plus les Américains à la menace cyber-électronique.

Or, la Chine cherche clairement le « *leapfrog* », le saut de grenouille, en investissant massivement dans les technologies de l'information notamment dans les « mégaprojets » susceptibles de refaçonner cette compétition militaire, au premier rang desquels figurent l'intelligence artificielle et les technologies quantiques. Si Xi Jinping a demandé à l'Armée populaire de libération (APL) de devenir une « armée de classe mondiale » (世界一流军队) d'ici 2050, l'objectif est de devenir la première puissance mondiale en matière d'IA d'ici 2030. Dans ce domaine, les écosystèmes américains privés restent encore les plus puissants du monde. Le Pentagone poursuit pour sa part plus de 500 initiatives dans des domaines aussi variés que le renseignement, la maintenance, l'aide à la décision, la guerre électronique (etc.). Cependant, l'administration n'a que récemment accéléré ses efforts d'orientation stratégique en la matière. Face aux États-Unis, les écosystèmes chinois se développent très rapidement, se diversifient avec l'apport de nombreuses PME et innovent sur plusieurs aspects. La Russie, à beaucoup plus petite échelle, poursuit le développement de solutions d'IA principalement conçues pour l'emploi militaire.

Dans le domaine des technologies quantiques, dont il convient peut-être de relativiser le caractère de rupture, les acteurs américains conservent une marge d'avance dans le

domaine du calcul, de « l'ordinateur quantique ». La Chine les talonne dans le domaine des capteurs et elle est passée à l'avant-scène mondiale dans la R&D sur les télécommunications. Là encore, les pouvoirs exécutif et législatif américains n'entendent orienter l'écosystème national que depuis ces dernières années.

Parmi les facteurs influençant cette compétition, intervient le niveau de ressource. Si les États-Unis restent largement en tête des financements de R&D, c'est surtout la courbe de progression des investissements chinois qui inquiète les hiérarques du Pentagone. Pékin pourrait dépasser Washington dans la prochaine décennie. Sur ce plan, là encore, la Russie est nettement en retrait. Sur le plan organisationnel, la R&D chinoise est bien orientée, a su mettre sur pied des écosystèmes assez cohérents dans l'ensemble de ces domaines des technologies de l'information et procède d'une forte « intégration civilo-militaire » combinant planification et mécanismes de marché, à laquelle contribuent de plus en plus les entreprises et *start-up* les plus innovantes. En revanche, elle pâtit toujours d'un déficit de ressources humaines dans le domaine scientifique, d'un niveau élevé de corruption et de favoritisme, d'une concurrence des provinces dans l'obtention des faveurs de Pékin créant des bulles d'investissement inefficaces. Sa BITD, encore très fractionnée et redondante, peine à concevoir des systèmes complexes indigènes. Cependant, les lacunes d'innovation scientifique découlant de ces facteurs sont compensées par une forte innovation dans l'ingénierie tirée de solutions technologiques étrangères. La guerre commerciale en cours ainsi que le changement de perception des Occidentaux auront donc probablement un impact sur les capacités d'innovation de la Chine. Cette dernière peut-elle seule arriver à être innovante ? C'est la vraie question. Quant à la Russie, si sa BITD conserve des segments d'excellence en matière de systèmes d'arme et tente de s'organiser dans le domaine de l'IA, ses énormes lacunes en matière d'investissements, de ressources humaines, d'apports du secteur privé rendent peu probable qu'elle puisse se mêler à la compétition sur le moyen-long terme entre les deux grands.

Face aux progrès fulgurants de la Chine et aux développements russes, les États-Unis ont considérablement accentué leurs efforts. À cet égard, si la notion de *Third Offset Strategy* n'a pas survécu au changement d'administration, les dynamiques qu'elle entendait promouvoir restent virtuellement identiques, voire se renforcent. Tout d'abord, le Congrès et le Pentagone ont accéléré et flexibilisé la stratégie capacitaire. Par exemple, un quart des financements de RDT&E concerne maintenant des programmes de *Rapid Prototyping* permis par la NDAA de la FY16. Témoigne aussi de cette mobilisation américaine la volonté de constituer ces écosystèmes « stratégiques » sur l'IA et le quantique. Cependant, à la différence de la Chine, elle se heurte à des divergences d'intérêts mais aussi de culture entre les acteurs du numériques et l'administration. Il n'en reste pas moins que le Pentagone semble être parvenu à « embrayer » avec l'industrie de la *high tech* au travers de ses *Defense Innovation Unit*. Au final, il est donc encore trop tôt pour savoir lequel, du lièvre américain ou de la grenouille chinoise, prendra le pas sur l'autre.

INTRODUCTION

La compétition stratégique contre la Chine et la Russie est devenue l'unique horizon de la défense américaine même si cette dernière reste engagée dans la lutte contre les djihadistes. Le général Dunford, *Chairman of the Joint Chiefs of Staff* (CJCS) sortant, a ainsi remis à jour la formule mathématique résumant ces dernières années les menaces principales et défis auxquels font face les États-Unis : 2 + 3 : Chine, Russie + Iran, Corée du Nord et organisations extrémistes violentes. La dynamique de l'érosion de la supériorité américaine face à ces compétiteurs est répétée *ad nauseam*, par tous les responsables, de l'Administration au Congrès, et les *think tanks* depuis des années. Voici l'une des dernières formulations en date de ce paradigme, par le général Dunford :

« *We have a competitive advantage against any adversary across all domains—air, sea, land, space, and cyber—and we can project power to advance the interests of the United States anywhere around the globe […] But* ***that competitive advantage has eroded. This is the result of seventeen years of continuous combat against transregional violent extremism and the damaging effects of funding instability***. ***China and Russia have capitalized on our distraction and our constraints***. *They have invested in capabilities specifically designed to challenge our traditional sources of strength and have sought to undermine the rules-based international order that brought prosperity and relative peace for the last seven decades.* »

La compétition stratégique se fonde sur la compétition technologique, tant militaire que commerciale, notamment avec la Chine. Le Dr. Griffin, le premier à réincarner la fonction de *Under Secretary of Defense for Research and Engineering* (USD R&E) rétablie en 2018 pour réinsuffler l'innovation au sein du DoD, comme au temps de la guerre froide, a identifié 10 domaines clés liés à une technologie ou à une mission spécifique structurant cette compétition pour l'appareil militaire américain : les armes hypersoniques ; les armes à énergie dirigée ; le C3 ; l'offensive et la défensive spatiale, la cyber-sécurité, l'intelligence artificielle et le *machine learning* ; la défense antimissile ; le calcul et les sciences quantiques, enfin la modernisation nucléaire.

Ce rapport propose donc un bilan d'étape de cette compétition. Il ne détaillera cependant pas la totalité de ces dix thèmes, ce qui serait un objectif par trop ambitieux et contraint par le volume du présent exercice. Il est divisé en trois parties :

- La première est consacrée à trois domaines de systèmes d'armes : les armes hypersoniques et la défense antimissile contre ces armements, le *counterspace* et les armes à énergie dirigée. Dans cette partie, la logique de compétition implique de traiter non seulement le développement et la concrétisation capacitaire des technologies mentionnées mais aussi la vulnérabilité de l'opposant à la technologie évoquée ;

- La seconde est consacrée à deux domaines relevant du champ nettement plus large des technologies de l'information : l'intelligence artificielle et les technologies quantiques, en « *enablers* » futurs d'une large part des capacités des compétiteurs. L'approche doit ici obligatoirement prendre en compte également les développements non-militaires qui mènent l'innovation ;
- La troisième propose un essai de « *scorecards* » et revient sur les facteurs de force et de faiblesse des États-Unis dans cette compétition.

Cet observatoire étant consacré à la politique de défense des États-Unis, il n'a pas vocation à traiter dans le détail des développements technologiques chinois et russes. Dans la mesure du possible, les contributeurs livrent cependant leur évaluation propre en la matière, en sus de la perception américaine de ces menaces.

PARTIE 1 – LES SYSTÈMES D'ARMES

1. Les missiles hypersoniques

1.1 Apport de la technologie

Le missile hypersonique représente la priorité n°1 du Dr Griffin. Les armes évoquées pointent en réalité des systèmes de trois types :

- Les missiles de croisière propulsés par super-statoréacteurs ;
- Les planeurs hypersoniques, tirés depuis la surface par un lanceur spatial léger, un missile balistique ou possiblement un propulseur de missile ;
- Les missiles balistiques aérolargués, qui poursuivent une trajectoire quasi-balistique ou balistique suivie d'une phase de manœuvre.

Le contour de la technologie de rupture est en fait moins net qu'il n'y paraît. Les technologies de manœuvrabilité sont connues depuis les années 1960 et plus ou moins exploitées depuis les années 1980 (Pershing II, SS-21, SS-23). La notion d'hypersonique, qui consiste à obtenir des vitesses supérieures à Mach 5 (1,5 km/s) sur des trajectoires non balistiques est plus neuve. Elle dérive néanmoins directement des études poursuivies de longue date sur les corps manœuvrants (appliquée aux planeurs hypersoniques) et des études sur la stato-réaction (appliquées aux missiles de croisière propulsés par super statoréacteurs). L'exploitation de la manœuvrabilité, qui caractérise les programmes hypersoniques actuels, n'est pas non plus particulièrement neuve, puisque développée dès les années 1980 sur les têtes manœuvrantes, les systèmes actuels offrant une capacité de manœuvre suffisante pour leurrer les systèmes existants (manœuvre de 100 à 300 km pour des systèmes portés par IRBM). Ainsi, la rupture apparaît essentiellement dans la recherche de l'extension de portée du vol en atmosphère ; de la précision (lorsque l'hypersonique est associé à un emploi conventionnel), mais aussi de la durée de propulsion (super-statoréacteurs). Toutefois, si les approches technologiques sont connues, cette recherche de manœuvre en atmosphère sur des portées longues induit des contraintes lourdes sur les matériaux, la navigation et le guidage. Elle suppose des ruptures non négligeables, que les technologies de manœuvrabilité actuelles ne permettent pas d'atteindre :

- La navigation et le guidage de ce type de vecteur restant très dépendants des GPS, un important travail reste à réaliser dans le développement de PNT précis et fiable.

- Sur les technologies de super-statoréacteur, qui offrent un potentiel majeur de développement pour les engins hypersoniques légers, la compréhension des phénomènes d'écoulement d'air, de combustion, d'échauffement des matériaux et la conception de matériaux mécaniquement et thermiquement résistants reste un enjeu technologique majeur ;
- L'exploitation des avantages offerts par les systèmes hypersoniques, notamment la promptitude et la fulgurance n'est possible que par le déploiement d'un C4ISR très performant.

Quoi qu'il en soit, l'apport opérationnel de ces armements est évident. Il permet de :

- Surclasser et pénétrer, par la vitesse et/ou la manœuvre, des défenses antiaériennes et antimissiles adverses de plus en plus étoffées, conférant un avantage déterminant à l'attaquant. Ainsi, en réduisant ou annulant la trajectoire balistique, ces systèmes réduisent leur vulnérabilité à la défense antimissile exo-atmosphérique. La vitesse de transit de ces armes est trop rapide pour les radars d'acquisition et leur manœuvrabilité (pour les planeurs) permet de déjouer bon nombre de procédés d'interception ;
- Et/ou permettre des frappes fulgurantes de *Time-Sensitive Targeting* (TST) à l'échelle d'un théâtre.

Cette problématique n'est cependant pas la même selon que l'on se place du point de vue américain ou de celui de la Chine et de la Russie.

1.2 Développements américains

1.2.1 Historique

Le développement des programmes hypersoniques américains est fortement lié à l'identification, dès les années 1990, et à la recherche de solution permettant une frappe rapide, selon une logique de TST, de cibles militaires de haute valeur ajoutée (TEL, radars, C2) puis des problématiques de déni d'accès. Menés par l'*Air Force*, les programmes initiés ont essentiellement porté sur le développement d'un missile de croisière propulsé par super-statoréacteur, incarné actuellement par le programme *Hypersonic Air-breathing Weapon Concept* (HAWC). Développés dans une logique très opérationnelle, ces programmes sont à distinguer des programmes lancés dans le cadre du *Prompt Global Strike* et du *Conventional Prompt Global Strike* (CPGS), à visée plus stratégique et pour lesquels les technologies hypersoniques sont initialement développées à un horizon lointain. L'abandon du Trident Conventionnel en 2008 recentre les programmes CPGS autour du développement de planeurs stratégiques (HTV-2), logique progressivement abandonnée après 2012 au profit de programmes moins ambitieux, visant à donner une première capacité de frappe dans la grande profondeur du théâtre. La dimension non nucléaire de ces programmes reste essentielle, expliquant la recherche systématique d'une précision

très élevée (inférieure à 10 mètres) pour permettre à ces systèmes d'engager des cibles fortement durcies[1].

1.2.2 Les cinq programmes actuels

Actuellement, les armées américaines développent cinq programmes, tous étant des armes à planeur sauf le dernier :

- Le *Long Range Hypersonic Weapon* (LRHW) de l'*Army*, dont la portée affichée sera de 2200 km, une de ses deux solutions de feux stratégiques, priorité des opérations multidomaines. Le LRHW sera mis en œuvre par un bataillon de feux stratégiques au sein des *Multidomain Operations Task Force,* nouvelles unités polyvalentes de projection des feux cinétiques et non-cinétiques (GE, cyber) en contre-déni d'accès[2] ;
- L'*Intermediate Range Conventional Prompt Strike* (IRCPS) de la *Navy*, devant être mis en œuvre par les SNA classe Virginia. Le programme repose sur un lanceur de portée intermédiaire non identifié, qui pose la question de l'intégration dans les nouveaux modules dévolus à l'emport des missiles croisière sur les sous-marins d'attaque Virginia ;
- Trois programmes de missiles aéroportés de l'*Air Force* :
  - L'*Hypersonic Conventional Strike Weapon* (HCSW) destiné à aboutir à une solution opérationnelle rapidement, à la fin de 2021 après une année de tests, espère l'USAF[3]. Le lanceur pourrait être dérivé d'un propulseur de type MGM-140, répliquant le Sparrow israélien ou le Kh-47 russe ;
  - L'AGM-183A *Air-Launched Rapid Response Weapon* (ARRW), plus performant théoriquement mais plus risqué, continuant le programme de R&D de *Tactical Boost Glide* (TBG) mené avec la DARPA. Les tests en vol viennent de commencer ;

---

[1] Voir Stéphane Delory, et alii, *Le concept américain de « Conventional Prompt Global Strike »*, 19 juillet 2017, réalisé au profit du CICDE, document en diffusion restreinte

[2] Sydney J. Freedberg Jr. « *Army* Wants Hypersonic Missile Unit by 2023: Lt. Gen. Thurgood », *Breaking Defense*, June 04, 2019, https://breakingdefense.com/2019/06/*Army*-wants-hypersonic-missile-unit-by-2023-lt-gen-thurgood/

[3] Vivienne Machi, « *Air Force* Two Years Away From Initial Hypersonics Capability, Official Says », *Defense Daily*, 02/08/2019, https://www.defensedaily.com/air-force-two-years-away-initial-hypersonics-capability-official-says/air-force/

Figure n° 1 : TEST EN VOL DE L'AGM-183A

- Enfin le missile de croisière *Hypersonic Air-breathing Weapon Concept* (HAWC) lui aussi réalisé avec la DARPA. Propulsé par un super-statoréacteur dérivé du X-51 Waverider, ce programme semble souffrir de retards importants.

Pour accélérer le développement de ces systèmes, les *services* recherchent des solutions communes. Ainsi, le LRHW, l'IRPCS et l'HCSW partagent le même planeur, le *Common Hypersonic Glide Body* (C-HGB). Son développement échoit à la *Navy* dont les contraintes d'emport sont les plus sévères[4]. Il reprend et miniaturise l'*Alternate Re-Entry System* (ARES) développé par l'*Army* dans le cadre de son propre programme AHW, jugé plus mature que le planeur développé pour le *Tactical Boost Glide* de l'*Air Force*. L'ARES est en effet dérivée du *Sandia Winged Energetic Reentry Vehicle Experiment* (SWERVE), expérimenté avec succès dès les années 1980, combiné peut-être à des éléments de l'*Advanced Maneuvering Reentry Vehicule* (AMaRV), tête manœuvrante des missiles Minutenam et MX.[5]. C'est d'ailleurs le laboratoire Sandia qui est chargé de travailler sur ce C-HGB[6]. Le SWERVE présente un corps de rentrée conique non propulsé, plus simple que les autres planeurs de formes planes développés ces deux dernières décennies mais qui se traduit par une portée plus courte[7]. La *Navy* fournira également à l'US *Army* le lanceur de portée intermédiaire qui nécessite de concevoir un nouveau TEL. Les charges utiles légères de ces systèmes (de quelques centaines de kg en général) destinent ces armes à la neutralisation de cibles de haute valeur non ou peu durcies (radars, sites C2 non

[4] Sydney J. Freedberg Jr, « *Army* Building 1,000-Mile Supergun », *Breaking Defense*, October 11, 2018, https://breakingdefense.com/2018/10/*Army*-builds-1000-mile-supergun/

[5] Stéphane Delory et alii, « Le concept américain de « *Conventional Prompt Global Strike* » », étude FRS au profit du CICDE, juillet 2017.

[6] Joseph Trevithick, « USAF, *Army*, and *Navy* Join Forces To Field America's First Operational Hypersonic Weapon », *The War Zone*, October 11, 2018, http://www.thedrive.com/the-war-zone/24181/usaf-*Army*-and-*Navy*-join-forces-to-field-americas-first-operational-hypersonic-weapon

[7] Steve Trimble & Guy Norris, « Sandia's Swerve Could Lead To First-gen Hypersonic Production Line », *Aviation Week & Space Technology*, October 11, 2018.

enterrés, TEL, navires, etc.). Cette légèreté de la charge utile, qui plus est unitaire, doit être compensée par la très grande précision terminale du système d'arme.

Par ailleurs, les États-Unis semblent envisager le développement de systèmes balistiques à tête manœuvrante pouvant opérer sur les portées intermédiaires (programme TSV), probablement dérivés d'anciens programmes du Trident Conventionnel (CTM).

1.2.3 La question de l'architecture de ciblage

Les Américains disposent de l'architecture de ciblage nécessaire à la mise en œuvre de ces systèmes, avec le mix de capteurs aériens, spatiaux, ROIM comme ROEM, et leurs multiples réseaux de C4I. Cette dernière souffre cependant de limites non négligeables. Tout d'abord, les Américains manquent peut-être encore de capacités ISR aéroportées pénétrantes à long rayon d'action, même s'il est possible qu'ils disposent de programmes de drones classifiés comme le RQ-180. Ils doivent néanmoins s'en remettre aux moyens ISR spatiaux. Or dans ce domaine, leurs constellations souveraines, bien qu'impressionnantes, ne fournissent qu'une capacité de reconnaissance. Réaliser de la surveillance ne peut passer que par l'exploitation des constellations commerciales en orbite médiane ou basse en cours de développement. Cet éventuel gap est cependant progressivement comblé par le déploiement des chasseurs de 5ème génération que viendront renforcer dans la prochaine décennie les bombardiers B-21. En second lieu, les architectures C4I garantissent l'interopérabilité des éléments au sein d'un domaine de lutte (opérations aériennes, aéronavales, aéroterrestres, etc.) mais elles ne sont pas encore « multidomaines », par exemple ce que constituerait une chaîne composée d'un capteur aéroporté de l'USAF confirmant une perception ROEM d'un sous-marin de la *Navy* et en mesure de désigner directement, sur ordre du PC de la *Joint Task Force*, un objectif à une batterie de missiles hypersoniques de l'*Army*. Le développement de ce type de capacité reste tout l'enjeu des concepts actuels de *Multi-Domain Operations* (MDO) ou de *Cross-Domain synergy*.

En attendant, ces limitations confineront probablement les premières générations de missiles hypersoniques au ciblage d'objectifs de haute valeur (*High Value Targets*, HVT) fixes ou relocalisables en quelques heures, peu durcis, tels que les sites C2 non enterrés, ou encore les radars de veille. Une approche plus dynamique peut cependant être envisagée pour le HAWC, dans une configuration antinavire. Ainsi, les missiles hypersoniques américains pourraient fort bien constituer les « Tomahawk nouvelle génération », destinés à affaiblir la cohérence des systèmes de défense intégrée (IADS) adverses en ouverture de campagne, permettant aux autres moyens d'entreprendre leur dislocation, ou à la frappe de décapitation sur les capacités de commandement tactique adverse tout au long d'une campagne.

1.3 Développements chinois et russes

1.3.1 Russie

La principale problématique russe est de crédibiliser sa dissuasion nucléaire face aux évolutions futures de la défense antimissile américaine, problématique anticipée dès la terminaison du traité ABM et explorée avant celle-ci dans un contexte de recherche précision par la manœuvrabilité (logique de frappe antiforce, que les systèmes russes ne permettent alors que par des frappes avec armes très puissantes). Cette conjonction des problématiques de frappe nucléaire antiforce et de défense antimissile stratégique pousse les Russes à axer leur développement sur le concept de manœuvrabilité des corps de rentrée, avec cependant une demande de précision très inférieure à celle des systèmes conventionnels américains.

Leur principal programme de planeur hypersonique stratégique est Yu71 Avanguard, beaucoup plus imposant que les systèmes américains (long de 5 m), destiné à être délivré par l'ICBM SS-18 puis par le Sarmat avec une vitesse moyenne estimée supérieure à 5 km/s (Mach 15) pour des missions nucléaires.

Figure n° 2 : PREMIER ESSAIS PUBLIQUEMENT RAPPORTÉS D'UN SYSTÈME D'ARME DE TYPE PLANEUR[8]

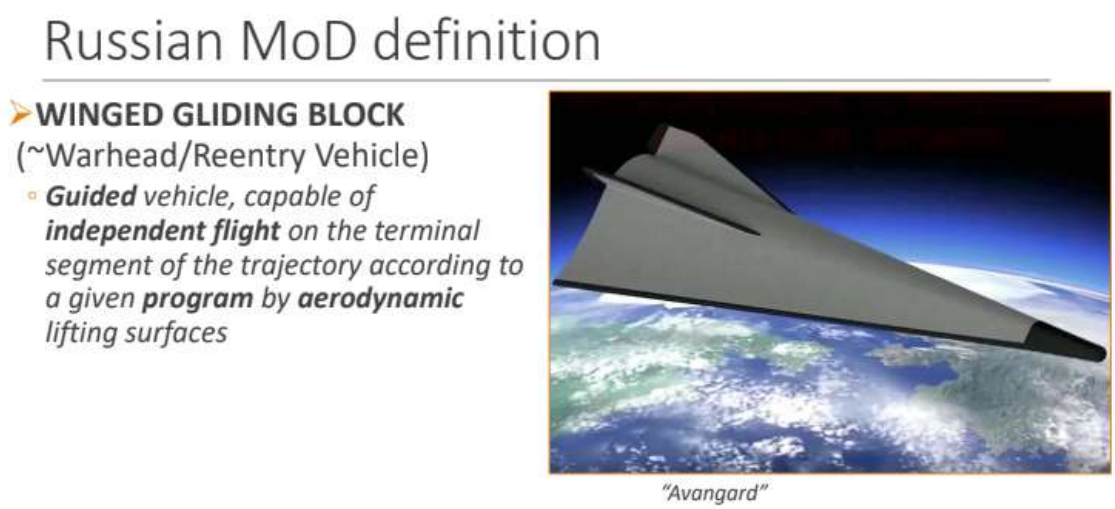
Igla Trajectory

Les chercheurs russes ont systématiquement cherché à exploiter la formation de plasma, inhérente au vol en atmosphères d'engin volant à plus de Mach 10, ceci afin de compliquer la détection radar américaine. Cet avantage se paie cependant par une incapacité probable du missile d'être recalé par une liaison de données, sauf lors du vol terminal, lorsque le planeur a ralenti. Il est donc assez probable qu'une part non négligeable de la navigation du missile soit assurée par des systèmes inertiels et stellaires et non par GPS – en tout état de cause incompatible avec la mission stratégique – conduisant assez probablement à une certaine imprécision et à des trajectoires simplifiées. Il est donc difficile

[8] Nicolai Sokov, « Military Exercises in Russia: Naval Deterrence Failures Compensated by Strategic Rocket Success », *Jame's Martin Center for Nonproliferation Studies*, 24 février 2004.

d'évaluer si le déploiement d'un tel système s'inscrit dans une logique de renforcement des capacités antiforces ou s'il elle viserait avant tout à garantir la capacité de représailles. Il faut néanmoins anticiper que le planeur puisse également être utilisé comme une tête manœuvrante (plané court, réduisant la problématique de la navigation et du positionnement de la tête par rapport à la cible, mais qui semble peu cohérent avec les images fournies par les Russes sur ce que serait le système), mais aussi que des travaux robustes soient effectués sur le guidage inertiel, réduisant l'imprécision de la navigation du planeur et permettant une transition efficace aux systèmes de guidage terminaux.

Figure n° 3 : ILLUSTRATION DE L'AVANGARD[9]



La Russie s'est également engagée dans la solution techniquement éprouvée du missile balistique aérolargué (*Air-Launched Ballistic Missile*, ALBM), dit Kinjal, un dérivé air-mer du missile quasi-balistique courte portée 9K720 Iskander-M, largué depuis un MiG-31 et possiblement d'un Tu-22M3 (ou variation). Le choix d'aérolarguer un missile de type SS-26 offre de nombreux avantages. Il permet d'étendre la portée du missile bien au-delà des 500 à 700 km du SS-26 mais aussi d'optimiser les trajectoires en fonction des défenses. En théorie, le Kinjal devrait permettre d'opter pour une trajectoire quasi balistique sur des portées courtes mais aussi d'opter pour des trajectoires balistiques suivies d'une manœuvre pour les portées longues. Dans les deux cas de figure, l'interception exo-atmosphérique pourrait être quasi impossible, alors que le missile pourrait opérer sur des portées supérieures à 2000 km (combinaison de portée du vecteur et de sa plateforme).

[9] Dmitry Stefanovich (Russian International Affairs Council), document non daté, lieu de présentation non précisé (https://drive.google.com/file/d/1yUDOi1S3YeRomJ40-HH805rUXJyXDywc/view)

Il ne s'agit donc pas ici d'une technologie de rupture mais d'une application opérationnelle de rupture de technologies assez matures.

Cependant, le domaine dans lequel les Russes sont engagés depuis le plus longtemps est celui des missiles de croisière (MdC) antinavires avec les programmes 3M22 Zyrkon et BrahMos II, dont les spécialistes pensent qu'ils partagent les mêmes technologies. Les Russes utiliseraient une propulsion à super-statoréacteur (probablement à hydrogène) permettant d'atteindre des vitesses hypersoniques (donnée à Mach 8 par les Russes) sur des distances courtes de quelques centaines de km de portée (600 à 800 selon les sources russes). Ces missiles ont vocation à être mis en œuvre depuis les navires de surface (Kirov), bombardiers (Tu-22M Backfire) et sous-marins (Oscar II).

Il est très probable que les Russes utilisent les technologies de super statoréaction dans une logique très différente de celle des Américains, ne cherchant pas à développer un système de longue portée pouvant opérer sur plus de 1000 km mais avant tout pour obtenir une brève augmentation de vitesse afin de générer un effet tactique optimal. Les Russes semblent donc dans une logique de développement opérationnel du super-statoréacteur pour des munitions de « courte portée » visant à les rendre non interceptables. A l'inverse, la manœuvrabilité de l'engin est sans doute faible, l'essentiel de l'effet devant être obtenu par la vitesse.

Il est enfin à noter que des vitesses assez proches de Mach 5 seront obtenues sur des engins à propulsion liquide classique de type Kh-32 (dérivé du Kh-22).

1.3.2 Chine

La problématique chinoise reste celle de la « défense active » pour entraver le déploiement de force américain en cas de conflit dans la sous-région. Dans ce contexte, il s'agit de s'assurer des capacités de frappe d'interdiction antinavire et anti-terre en mesure de surclasser les défenses antimissiles de théâtre américaine et japonaise voire de contribuer à leur annihilation. En effet, l'imposante force de missiles balistiques chinois peut être en partie neutralisée par les capacités nippo-américaines, les plus sophistiquées du monde. L'intérêt majeur que constitueraient les armes hypersoniques pour la Chine serait ainsi, outre le renforcement de leur capacité antinavire, de disposer de moyens de frappe difficile à intercepter et en mesure de neutraliser des éléments fixes de cette défense antimissile, comme par exemple les destroyers antimissiles japonais et américains à leurs ports d'attache nippons.

Dans le domaine des MdC à super-statoréacteur, la Chine a commencé à faire connaître ses programmes. En mai 2018, les premières images d'un système dénommé Lingyun-1 ont été révélées, montrant un système qui semble fortement inspiré des technologies du HyFire testées par les États-Unis dans les années 2000. La mise à poste du Lingyun-1 est assurée par un booster spécialement développé à cet effet. L'engin est donc proba-

blement un démonstrateur. D'autres expérimentations ont été rendues publiques, autour d'un système désigné comme MF-1 qui semble plus être lié au comportement d'un corps de rentrée de type hypersonique qu'à la propulsion proprement dite.

Figure n° 4 : LINGYUN-1

L'APL a procédé également en juin 2018 au tir d'un nouveau démonstrateur, le Xing Kong-2, un *Waverider* comme le X-51. Lors du test, l'engin aurait volé 400 secondes, affichant une vitesse de Mach 5,5 à 6, donc une portée de près de 700 km. Son porteur pourrait être un missile balistique DF-11 ou BP-12 d'exportation[10].

Les Chinois développeraient également le CH-AS-X-13, un missile balistique aérolargué, un équivalent du Kinjal russe, d'une portée de 3000 km. L'engin serait testé depuis la fin de 2016[11].

La Chine dispose enfin de plusieurs programmes expérimentaux de planeurs :

[10] Henri Kenhmann, « Mach 6, 400 secondes… Essai réussi d'un Waverider hypersonique chinois », *East Pendulum*, 2018-08-06, http://www.eastpendulum.com/mach-6-400-secondes-essai-reussi-dun-waverider-hypersonique-chinois

[11] Henri Kenhmann, « La Chine développe deux nouveaux systèmes de missile balistique aéroporté », *East Pendulum*, 2018-06-20, http://www.eastpendulum.com/la-chine-developpe-deux-nouveaux-systemes-de-missile-balistique-aeroporte

- Le programme le plus ambitieux est celui du DF-ZF/Wu-14, testé sept fois de 2014 à 2016, dont 5 avec succès semble-t-il, à des vitesses situées entre Mach 5 et Mach 10 sur des portées totales allant de 1250 à 2100 km[12] ;
- Les renseignements américains ont révélé le test en novembre 2017 d'un missile balistique DF-17 doté d'un planeur, qui a parcouru en 11 minutes une distance de 1400 km mais on ignore s'il s'agit du plané de l'engin ou de la distance totale parcourue par le missile puis son planeur, la vitesse de ce dernier s'établissant entre Mach 4 et 6[13] ;

Selon l'expert James Acton, les Chinois se heurteraient à de multiples défis (modélisation informatique du régime aérodynamique, matériaux résistants à la friction, zones de tests, guidage, etc.) s'ils souhaitaient développer des engins de portée supérieure.

Si le développement d'un engin comme le CH-AS-X-13 apparaîtrait cohérent avec les intentions capacitaires antinavires chinoises, on ne peut tirer grand-chose des autres programmes quant aux éventuelles capacités opérationnelles recherchées, notamment pour les planeurs, dont les portées estimées, très incertaines, ne correspondent pas à un emploi quelconque.

On peut faire l'hypothèse que l'architecture de ciblage de ces missiles serait la même que celle devant être utilisée pour les missiles DF-21D et DF-26, à base de nombreux satellites de ROIM et d'ELINT RORSAT Yaogan, de radars transhorizon et de capteurs navals et aériens, de la constellation PNT Beidou et de SATCOM divers[14].

1.4 Evaluation des capacités réciproques à l'interception de ces systèmes

1.4.1 L'interception des vecteurs hypersoniques

La vulnérabilité perçue à l'égard des systèmes hypersoniques est évidemment liée aux caractéristiques des systèmes, qui, dans leurs trajectoires, tendent à différer des engins balistiques classiques ou des engins quasi-balistiques sol-sol.

Les engins balistiques de courte portée peuvent être interceptés en phase terminale, leur vélocité étant suffisamment basse pour que des systèmes de défense aérienne élargie (DAE) puissent les engager, l'absence de contre-mesure favorisant l'interception. Les engins quasi-balistiques sont plus complexes à engager, du fait de leur manœuvre dans l'atmosphère, mais leur lenteur en phase finale permet également leur interception, généralement par une adaptation des algorithmes de guidage des intercepteurs.

---

[12] James M. Acton, *China's Advanced Weapons*, Carnegie Endowment for International Peace,Testimony before the U.S.-China Economic and Security Review Commission, February 23, 2017, https://carnegieendowment.org/files/Acton_Testimony_2_23_17.pdf

[13] Henry Kenhmann, « DF-17, première arme à planeur hypersonique au monde », *East Pendulum*, 30 décembre 2017. http://www.eastpendulum.com/df-17-premiere-arme-a-planeur-hypersonique-au-monde

[14] Andrew S. Erickson, Chinese Anti-Ship Ballistic Missile (ASBM) Development:: Drivers, Trajectories and Strategic Implications, Jamestown Foundation, May 2013, http://www.andrewerickson.com/wp-content/uploads/2018/03/Chinese-Anti-Ship-Ballistic-Missile-Development_Book_Jamestown_2013.pdf

Les engins de portée moyenne peuvent également être interceptés par les systèmes de défense antiaérienne élargie, mais aussi par des engins de type THAAD, contre lesquels ils sont relativement vulnérables. Sur les segments supérieurs (portée intermédiaire et stratégique), l'interception exo-atmosphérique est rendue très complexe du fait de la combinaison de la vitesse de la tête et de l'emploi de contre-mesures et d'aides à la pénétration. Toutefois, l'interception exo-atmosphérique se situe sur un segment de la trajectoire où la vulnérabilité de la tête est maximale, celle-ci suivant une trajectoire balistique prévisible sur une durée relativement longue.

L'interception des têtes manœuvrantes, dont la trajectoire se rapproche de celle des véhicules hypersoniques reste très complexe. Toutefois, la phase balistique reste un élément de vulnérabilité pour les engins longue portée, alors que la forte décroissance de la vélocité de la tête, lors de la manœuvre en atmosphère, tend systématiquement à générer des vulnérabilités à l'interception, plus particulièrement pour les systèmes courte et moyenne portée.

L'interception d'un planeur stratégique, qui effectuerait son plané sur plusieurs milliers de kilomètres à des vélocités élevées (supérieures à 3 voire 4 km/s) **pose actuellement un problème insurmontable**. Volant à des altitudes très élevées (plus de 60 km) sur une trajectoire non prédictive (variation d'altitude et possiblement d'azimut), ce type d'engin ne peut être engagé par la définition d'un point d'interception prévu, qui reste le mode d'action classique de tout intercepteur antimissile. Un intercepteur exo-atmosphérique classique ne pourra probablement pas engager le lanceur, la mise à poste du planeur se faisant à des distances trop éloignées, plus particulièrement face à système chinois ou russe. D'autre part, un intercepteur sol-air endo-atmosphérique ne pourra engager ce type de cible durant la phase de transit, faute de segment radar adéquat pour situer la position du planeur avec suffisamment d'exactitude mais aussi du fait de l'insuffisance des capteurs terminaux pour corréler la position de l'intercepteur et de sa cible, dans l'hypothèse improbable où les deux voisineraient. Les vélocités relatives des deux engins seraient en effet actuellement trop élevées pour que les capteurs puissent orienter le véhicule intercepteur. La propulsion du lanceur de l'intercepteur est également très problématique, tout comme la manœuvre du véhicule intercepteur dans les hautes couches de l'atmosphère.

En théorie, l'interception terminale pourrait être considérée, notamment si le planeur a une vocation conventionnelle. Dans ce cas de figure, il doit en effet fortement décélérer pour permettre l'activation de ses capteurs terminaux mais aussi pour arriver à une vitesse au sol inférieure à 1,5 km/s (limite de résistance mécanique d'un pénétrateur). La très haute vitesse d'arrivée sur cible, avant la ressource terminale, rend cependant l'activation des défenses très hypothétique. L'utilisation d'une charge nucléaire, détonée en altitude, qui atténue la nécessité de décélération du véhicule et de précision rendrait probablement toute tentative d'interception terminale illusoire.

Les solutions possibles reposent sur le déploiement d'une architecture spatiale (en l'état associée à des détecteurs infrarouges) permettant une première trajectographie du planeur et d'intercepteurs spatiaux engageant la cible lorsque sa capacité de manœuvre est faible, c'est-à-dire dans les couches hautes de l'atmosphère. L'adaptation des capteurs et des effecteurs reste à résoudre, un engin spatial opérant à des vélocités très élevées.

Un second axe de réflexion se situe sur l'interception en phase propulsée et ascendante, c'est-à-dire avant la mise à poste du planeur. Le principal problème repose cependant, pour un planeur stratégique, sur l'altitude d'interception et sur la vitesse de l'engin à intercepter, qui, en quelques minutes atteindra une vitesse de 5 à 7 km/s, à des altitudes qui dépasseront probablement 200 à 300 km. Cette problématique, qui n'est pas liée spécifiquement aux planeurs, a été largement étudiée aux États-Unis et reste au centre des recherches.

L'interception d'un planeur de théâtre, opérant sur quelques milliers de kilomètres, volant plus bas dans l'atmosphère à des vélocités moins élevées (2 à 3 km/s) **peut en revanche être considérée**, plus particulièrement dans la phase finale du vol, lorsque le planeur se situe à des altitudes basses et manœuvre vers sa cible. A ces altitudes, le segment radar sol peut être utilisé, probablement appuyé par le segment spatial, et il possible de concevoir un intercepteur qui, en termes de propulsion, serait capable d'engager la cible, soit autour des technologies solides de type THAAD (le programme THAAD ER vise désormais à pouvoir engager ce type de cible), soit autour de statoréacteur à haute performance. L'utilisation de ces super-statoréacteurs semble peu probable à courte/moyenne échéance.

Trois difficultés majeures demeurent :

- Du fait de la capacité de manœuvre du planeur, l'intercepteur doit être propulsé sur une phase longue ou, alternativement, disposer d'une vélocité encore élevée avant l'interception. Une architecture distribuée, constituée d'intercepteurs multiples engagés en mode *Engage on Remote* (EOR, c'est-à-dire quand la plate-forme de tir n'a pas acquis l'objectif sur ses propres capteurs) et adossé à une architecture radar très robuste, disposant d'une forte capacité de fusion de données représente très certainement un élément de solution pour l'interception terminale de ce type de vecteurs ;
- La question des capteurs terminaux reste à résoudre ;
- La question de l'alerte avancée reste importante. Le développement d'une architecture de détection spatiale reste probablement impératif.

L'interception d'un MdC à statoréacteurs pose un problème encore différent. On exclut ici les MdC à super-statoréacteurs « stratégiques », qui restent actuellement hors de portée des technologies et qui ne représentent pas une menace immédiate. Les super-statoréacteurs tactiques posent déjà un problème difficile à résoudre. En effet, bien que volant à des vitesses plus basses (1,5 km/s pour le X-51, 1,8 km/s évoqués pour

le Zyrkon, mais probablement en vitesse de pointe), à des altitudes de l'ordre de 20 à 25 km, et que leur capacité de manœuvre soit, à altitude égale, probablement plus faible que celle d'un planeur, les systèmes actuellement en développement ne sont pas forcément aisés à intercepter. Le modèle du Zyrkon russe semble montrer que l'un des axes de développement s'oriente sur de la munition courte portée, utilisant le statoréacteur pour obtenir un pic de vélocité après une première phase de propulsion chimique. Sur des distances « courtes », considérant la vitesse de pointe (1,5 à 1,8 km/s) et la vitesse d'arrivée sur cible (1 à 1,5 km/s), ce type d'engin laisse un temps de réaction très court aux défenses. Il est assez probable que sur la phase finale du vol, la vitesse résiduelle autorise des manœuvres violentes, les capteurs terminaux étant d'autre part parfaitement fonctionnels et autorisant un ciblage précis. Très typiquement, ce type d'engin ne peut que très difficilement être intercepté par les défenses actuelles, sauf à systématiser les architectures NIFC-CA, afin d'être en mesure d'engager la cible à la distance la plus élevée de l'intercepteur. Dans le cas du SM-6 cependant, il reste à examiner si la vélocité du missile est encore suffisante.

1.4.2 Les défenses antimissiles américaines restent les plus à même d'intercepter ces armes tactiques

Ces différents paramètres montrent que dans le développement des technologies d'interception, les États-Unis restent les mieux placés. Ils sont les seuls à maitriser les architectures distribuées qui permettent d'optimiser la trajectographie et l'engagement, sans disposer en l'état des équipements nécessaires pour intercepter un engin quelconque.

Ils disposent ou finalisent le développement déjà d'architectures en mesure d'évoluer vers des solutions futures d'interception : celle de défense collaborative antiaérienne de la *Navy*, le *Naval Integrated Fire Control – Counter-Air* (NIFC-CA) et l'*Integrated Air and Missile Defense Battle Command System* (IBCS) de l'*Army* qui doit être opérationnelle au début de la décennie. Ces éléments seront complétés par des programmes en développement, précisément anti-planeur hypersonique de théâtre : intercepteur *Terminal High Altitude Area Defense, Extended Range* (THAAD-ER) attendu pour la fin de la prochaine décennie, *Space Sensor Layer* en orbite basse, décidée par la *Missile Defense Review* et qu'informera la démonstration Blackjack de 20 minisatellites commerciaux de la DARPA vers 2022, enfin à nettement plus long terme, interception depuis l'espace (objet du récent programme *Glide Breaker* de la DARPA).

La principale vulnérabilité américaine réside donc dans le domaine naval. L'introduction du Zyrkon peut cependant appeler à retravailler sur le SM-6, notamment autour de la propulsion. Le Kh-47 pose également un problème actuellement quasi insoluble, la vitesse et la manœuvrabilité du système restant élevées pour les défenses actuelles. Il est cependant à souligner que les deux systèmes dépendant de capteurs terminaux, l'interception ne doit pas être considérée comme la solution unique : le brouillage, les leurres ou éventuellement les armes électromagnétiques peuvent être envisagés.

Parallèlement, le Yu-71 permet à la Russie de considérer un système de seconde frappe peu exposé aux évolutions de la défense antimissile, sauf à évaluer le déploiement avancé de vecteurs très véloces (GBI deux étages), couplés à un KV endo-atmosphérique. Se positionner officiellement pour le développement de tels vecteurs, dont l'efficacité devrait par ailleurs être démontrée, consisterait à faire de la défense antimissile un élément constitutif de la dissuasion, ce que les États-Unis se sont jusqu'à présent refusés à faire. Se pose également la question de l'interception de planeurs non stratégiques, notamment si ceux-ci sont associés à des charges nucléaires, ces systèmes pouvant parfaitement s'intégrer dans des logiques de frappes limitées, visant essentiellement le théâtre.

1.4.3 Des capacités russes et chinoises pour l'instant inadaptées

Du côté russe et chinois, l'émergence de l'hypersonique pose évidemment un problème d'interception, les engins de type S-400 étant inadaptés contre les planeurs alors que les systèmes défensifs de la flotte (5V55 et 9M96 en version navale) ne permettant pas l'interception et que les architectures radars sont totalement inadaptées. L'interception d'engins manœuvrants reposant sur le développement de radars multifaisceaux, qui permettent un guidage plus précis du missile, il est probable que les intercepteurs terminaux devront attendre le développement de nouvelles générations de radar pour être pleinement efficaces contre les cibles les plus lentes. L'introduction par les États-Unis de têtes manœuvrantes sur des missiles stratégiques ou sur des missiles à portée intermédiaire soulèverait le même problème pour les intercepteurs et pourrait conduire les Russes à reconsidérer leur posture vers le développement de technologies *hit to kill* pour le S-500, gardant l'option nucléaire ouverte. L'état de la défense antimissile chinoise ne permet pas d'envisager d'interception, quel que soit le modèle d'intercepteur retenu.

Russes et Chinois ne peuvent envisager le développement d'architectures distribuées au niveau de la flotte mais un examen plus attentif doit être réalisé sur le segment sol, le radar à basse fréquence Nebo M (Russe) montrant une capacité de développement avancée pour les engins multistatiques, ouvrant la possibilité d'une plus grande distribution des architectures. Comme pour les États-Unis, le segment doit cependant être reconfiguré pour prendre en compte les cibles très véloces de haute altitude, que les configurations actuelles ne permettent pas de détecter ou de trajectographier.

1.5 Conclusion

En conclusion, il apparaît que les armements hypersoniques poseront, lors de leur mise en service à court-moyen terme, des problèmes initialement insurmontables aux trois compétiteurs. Pour les États-Unis, ils sont l'une des clés du contre-déni d'accès face aux IADS et IFS adverses. Pour les Russes et les Chinois, ils représentent surtout l'un des outils de la remise en cause de la supériorité navale américaine. Les Américains bénéficient cependant de deux avantages. Sur le plan offensif, leur architecture C4ISR, plus complète et mieux intégrée même si elle reste imparfaite, leur garantit une meilleure

exploitation du potentiel offert par ces armes. Dans le domaine défensif, les 30 ans d'investissement massif dans la défense antimissile, pourtant brocardés comme l'exemple type de « désavantage compétitif » en raison du rapport coût/bénéfice de l'entreprise, les mettent en position de développer le plus rapidement les parades nécessaires à ces armements, à tout le moins à une partie d'entre eux.

2. Les armes à énergie dirigée

Les armes à énergie dirigée (AED) seront traitées plus succinctement que les deux autres volets de cette partie dans la mesure où l'on sait trop peu de choses sur l'avancement des compétiteurs russe et chinois pour réaliser une analyse comparative.

2.1 Apport de la technologie

Les AED incluent principalement deux types de technologies : les lasers et les armes électromagnétiques (ou armes à radiofréquences, RF, ou micro-ondes de forte puissance, HPM).

Les armes laser sont, rappelons-le, des dispositifs d'émission stimulée d'un faisceau lumineux destiné à in-capaciter, endommager voire détruire une cible par effet thermique ou de percement. Ces armes laser sont principalement de deux types :

- Les lasers reposant sur un matériau chimique, dont la technologie est déjà ancienne. Ces armes, très puissantes mais très encombrantes et polluantes, ont été abandonnées ;
- Les lasers reposant sur un matériau solide (*Solid-State Laser* – SSL), généralement la fibre optique. Elles sont incomparablement plus pratiques. La puissance unitaire de la source laser est limitée mais les faisceaux sont combinés pour obtenir des puissances opérationnelles nécessaires[15].

Les lasers ont pour principale plus-value leur extrême précision, surtout leur énorme puissance de feu pour un coût d'emploi ridiculement faible, la discrétion des effets et la variabilité des effets en fonction de leur puissance. En revanche, ce sont des armes à tir directe, dont l'efficacité reste sensible aux conditions atmosphériques. Leur principale contrainte reste cependant le facteur *Size, Weight and Power-Cooling* (SWAP-C), c'est-à-dire l'encombrement et le refroidissement qui rendent extrêmement problématique toute intégration opérationnelle d'une arme suffisamment puissante dans une plateforme. Les progrès en la matière ont cependant été constants ces dernières années et permettent d'envisager à moyen terme de premières armes opérationnelles de quelques kW à dizaines de kW, sur les bâtiments de combat et sur les véhicules terrestres. Ces

[15] Synthèse de notre note, Philippe Gros, Les armes à énergie dirigée, Observatoire des conflits futurs, note n°2, juin 2018, à consulter sur le site FRS

armes seront dédiées à la lutte anti-drone et anti-embarcations légères à courte portée (quelques km). Les armes permettant la destruction de cibles plus durcies et/ou plus véloces nécessitant des puissances beaucoup plus élevées (plusieurs centaines de kW), ainsi que les armes embarquées sur aéronefs en raison de leur SWAP-C, restent en revanche des perspectives de beaucoup plus long terme.

Les armes électromagnétiques (EM) visent quant à elles la perturbation, le dérangement (*upset*) voire le dommage pérenne des circuits électroniques d'une cible. Elles procèdent par impulsions électriques générant un effet de couplage sur les circuits de la cible, selon différents procédés : soit en passant par les récepteurs de la cible (antenne radar par exemple) soit par les anfractuosités de sa structure. Elles peuvent théoriquement être utilisées en mode défensif par exemple pour protéger un site ou une plateforme contre des essaims de drones ou des missiles, ou en mode offensif pour neutraliser des dispositifs peu protégés de détection ou de C2 adverses. Leur plus-value réside dans la variété des volumes envisageables (avec la possibilité d'en faire la charge utile de missiles ou bombes) ; la discrétion de leurs effets ; le caractère zonal de leur effet ; le fait que ce soit une arme non létale et leur puissance de feu pour certaines d'entre elles. En revanche, ce sont des armes de portée extrêmement limitée et beaucoup de projets auraient un facteur SWAP dirimant. Le développement de ces armes EM, extrêmement sensibles, recueille moins de publicité que les lasers mais il semble que les premières de ces armes soient cependant désormais opérationnelles.

2.2 Développements américains et vulnérabilités chinoises et russes

2.2.1 Les armes laser : une avancée circonspecte vers de premiers programmes opérationnels

La R&D américaine travaille depuis des décennies sur les armes lasers. Actuellement, tous les centres de recherche des *services* ainsi que ceux de l'USSOCOM et de la *Missile Defense Agency* disposent de feuille de route visant à développer de telles armes[16]. Cependant, la défiance dominait encore il y a quelques années, après la longue succession de déclarations ambitieuses par les communautés R&D et les industriels. Le développement de capacité mature à court terme était devenu le *joke* du « *Five Years away* ». Depuis deux à trois ans, compte tenu d'un premier palier de réelle maturation technologique, au niveau du SWAP des lasers à fibre optique, les communautés opérationnelles au sein de la *Navy* et de l'*Army*, se disent prêtes à franchir le pas vers des programmes d'acquisition. Il convient cependant encore de rester prudent.

[16] Pour un point de situation des différents programmes, voir les vidéos du Directed Energy Summit organisé par le CSBA et Booz Allen Hamilton, https://www.boozallen.com/d/event/directed-energy-summit-2018.html ,

Figure n° 5 : PRINCIPAUX PROGRAMMES D'ARMES LASER DES FORCES AMÉRICAINES

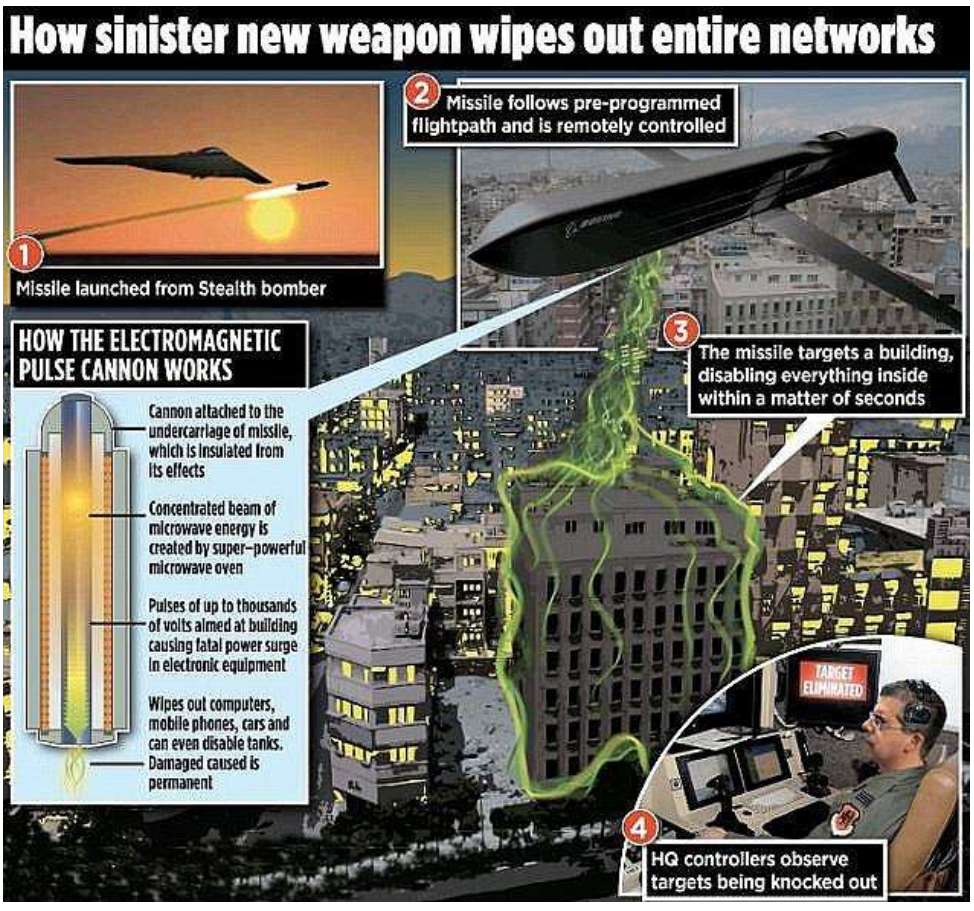
	Court terme (< 5ans)	Moyen - long terme
US *Air Force*	• ***Self-protect High-Energy Laser Demonstrator* (SHiELD)** d'autodéfense aéroporté sur nacelle appuyé par la DARPA. Test sur F-15 prévu en 2021 • Démonstrateur de laser sol-air de protection des bases aériennes	Les lasers doivent compter parmi les outils de l'*Air Dominance* et de l'interdiction post-2030
***Air Force* Special Operations Command**	Démonstration d'un **HEL de 60 kW sur les canonnières AC-130 Ghostrider** pour frappes air-sol surprise et discrètes. Test en 2022.	
US *Navy*	Famille de *Surface Navy Laser Weapon System* (SNLWS) offrant une capacité de protection des bâtiments anti-drones, anti-fast craft, à plus long terme de défense antiaérienne et antimissile limitée • Installation en 2021 d'un premier ***High Energy Laser and Integrated Optical-dazzler with Surveillance (HELIOS)*** sur destroyer DDG-51, d'une puissance comprise entre 60 et 150 kW. • Poursuite du programme de R&D de ***Solid State Laser Technology Demonstration* (SSL-TM).** Test d'un laser de 150 kW	Eventuel déploiement de plusieurs HELIOS à moyen terme. Eventuelle intégration à plus long terme des armes démontrées dans **SSL-TM .**
US Marine Corps	Prototypage rapide de ***Compact Laser Weapons System*** de 5-10 kW pour éventuelle incorporation rapide dans le programme de ***Ground-Based Air Defense Directed* (GBAD) Counter-Unmanned Aerial System (C-UAS)** de protection SATCP des unités tactiques.	
US *Army*	Intégration des lasers dans les solutions de recréation de la défense SACP vs. capteurs ISR, drones et, dans le futur, missiles de croisière et projectiles d'artillerie • ***Mobile Expeditionary High Energy Laser* (MEHEL) *demonstrator*** sur blindé Stryker en cours. MEHEL 3.0 atteint 10 kW • ***High Energy Laser Tactical Vehicle Demonstrator* (HEL TVD)** de 100 kW à tester en 2022.	• Eventuelle intégration MEHEL à 50 kW dans le *Maneuver-Short Range Air Defense capability* • Eventuelle intégration HEL TVD dans l'architecture de défense de site fixe *Indirect Fire Protection Capability Increment 2*

	Suite du démonstrateur HLMTT ayant atteint 60 kW en 2017
Missile Defense Agency	***Next Gen ABL,*** relance d'un *Airborne Laser* destiné à la destruction des missiles balistiques adverses en phase propulsée. Concept de laser en nacelle embarquée sur drone HALE. Mené pour partie avec la DARPA, il constitue le programme HEL américain le plus ambitieux – et sans doute le plus irréaliste – sur le plan technique

Pour le très long terme, le Dr Griffin a répété à plusieurs reprises qu'il pensait crédible le développement d'armes laser spatiales, bien qu'il pose des défis technologiques énormes.

2.2.2 Les armes électromagnétiques progressent sous l'horizon radar

Figure n° 6 : FONCTIONNEMENT DU *COUNTER-ELECTRONICS HIGH POWER MICROWAVE ADVANCED MISSILE PROJECT* (CHAMP)[17]



[17] Ronald Kessler, « EXCLUSIVE: U.S. *Air Force* has deployed 20 missiles that could zap the military electronics of North Korea or Iran with super powerful microwaves, rendering their military capabilities virtually useless with NO COLLATERAL DAMAGE », *Daily Mail*, 16 May 2019, https://www.dailymail.co.uk/news/article-7037549/Air-Force-deployed-20-missiles-fry-military-electronics-North-Korea-Iran.html

La première AED américaine pleinement opérationnelle ne serait pas un laser mais une arme EM. L'USAF aurait déployé sur le théâtre coréen 20 missiles de croisière équipés d'une charge EM, ce qui signifie que ce programme, le *Counter-Electronics High Power Microwave Advanced Missile Project* (CHAMP), a atteint le stade de la production opérationnelle comme l'a admis l'*Air Force Research Laboratory* au *Daily Mail*[18]. Une seconde version est développée en lien avec la *Navy*, le *High-power Joint Electromagnetic Non-Kinetic Strike* (HiJENKS).

Les centres américains, notamment la *Joint Non-Lethal Weapons Directorate* développent d'autres pistes d'armes HPM destinées plus particulièrement à la lutte non létale anti-personnel et anti-véhicule dans un contexte de contre-insurrection et de lutte anti-terroriste[19]. L'un de ces projets est l'*Active Denial Technologies* développé depuis 15 ans. L'arme HPM vise le « contrôle des foules » en provoquant une sensation de brulure chez les émeutiers. Leurs caractéristiques SWAP totalement inadaptées, de même que la sensibilité politique d'une telle arme ont amené les commandeurs en Irak et en Afghanistan à refuser l'emploi des premières versions de ces armes[20]. Leur développement continue néanmoins et inclut des équipements permettant de stopper les véhicules.

2.3 Développements chinois et russes et vulnérabilités américaines

2.3.1 L'incertitude chinoise

La Chine mène des recherches sur tous les types de laser (chimiques, solides, à électron libre) depuis les années 1960 avec un niveau scientifique excellent. Elle était par exemple créditée de l'une des meilleures technologies en matière d'optique adaptatives dans les années 1990. On sait cependant peu de chose sur les avancées actuelles de ses programmes. Certaines annonces, comme celle du fusil laser, apparaissent peu crédibles[21]. En revanche, selon le Dr Fischer, les Chinois travaillent comme les Américains sur des solutions SACP anti-drones terrestres, fondées sur le « Silent Hunter » présenté par le groupe Poly à Abou Dhabi en 2017, avec une puissance affichée entre 30 et 100 kW. Une version navalisée serait également en cours de développement[22]. Récemment un

[18] Idem

[19] DoD Non-Lethal Weapons Program, « Active Denial Technology » https://jnlwp.defense.gov/Future-Non-Lethal-Weapons/Active-Denial-Technology/ & Mr. David B. Law, *Joint Non-Lethal Weapons Program (JNLWP) Next-Generation Non-Lethal Directed Energy Weapons and Enabling Technology Portfolios*, présentation, National Defense Industrial Association (NDIA) 2016 Armament Systems Forum, 25-28 April 2016, https://ndiastorage.blob.core.usgovcloudapi.net/ndia/2016/armament/Law_JNLWDPdirectedenergy.pdf

[20] Sharon Weinberger, « High-Power Microwave Weapons Start to Look Like Dead-End », *Scientific American*, September 12, 2012, https://www.scientificamerican.com/article/high-power-microwave-weapons-start-to-look-like-dead-end/?print=true

[21] Joseph Trevithick, « No, China Hasn't Built A Laser Assault Rifle That Can 'Carbonize' People », blog *The War Zone*, The Drive, July 3, 2018, http://www.thedrive.com/the-war-zone/21925/no-china-probably-hasnt-built-a-laser-assault-rifle-that-can-carbonize-people

[22] U.S.-China Economic and Security Review Commission, Hearing on China's Advanced Weapons, written testimony of Richard D. Fisher, Jr., February 23, 2017, https://www.uscc.gov/sites/default/files/transcripts/China%27s%20Advanced%20Weapons.pdf

reportage de la China Central Television (CCTV) a montré ce qui semble être un prototype d'arme embarquée sur un navire, sans que l'on puisse savoir s'il s'agit du même type d'arme[23]. Selon la DIA, la Chine travaillerait également au développement d'arme laser ASAT (voir partie suivante).

Quant aux armes EM, l'incertitude est aussi de mise. Le professeur Huang Wenhua de l'Institut de technologie nucléaire du Nord-ouest a été récompensé du *National Science and Technology Progress Award* en 2017, pour ses travaux sur les HPM, notamment le test d'une arme antimissile embarquée sur navire. En réponse à la *Third Offset Strategy* américaine, la Chine aurait accéléré le développement de ces armes[24].

2.3.2 Les quelques développements russes

Les programmes russes actuels ne seraient que l'ombre de ceux de l'époque soviétique où ils avaient atteint la parité avec les Américains dans tous les domaines, voire les dépassaient dans certains. L'URSS avait par exemple mis au point une station spatiale équipée d'un laser, détruite lors de l'explosion de la fusée Energia qui devait la déployer. Au niveau tactique, leurs unités de défense sol-air avaient commencé à prendre en compte plusieurs armes SACP. Actuellement, les Russes ont développé au moins deux systèmes : le Peresvet, embarqué sur véhicule, prétendument de lutte antimissile et ASAT mais sans doute plus prosaïquement dédié à la défense sol-air, et l'A-60 Sokol-Eshelon, que nous évoquons dans la section suivante. Les deux systèmes visent probablement les contre-mesures optroniques plus que la destruction.

Dans le domaine des armes EM, l'industriel russe UIC a annoncé avoir développé une arme sol-air d'une portée de 10 km[25]. Elle rappelle le programme de R&D RANETS-E, dévoilé et testé en 2001, qui pouvait disposer, selon l'expert australien Carlo Kopp, d'une portée réelle de 7 à 13 km contre les composants électroniques civils[26]. Plusieurs experts russes, comme le général Gorkov, ancien commandant des forces de missiles de défense antiaérienne russe, ont fait part de leur scepticisme devant cette revendication. Si ces doutes sont tout à fait crédibles compte tenu des incertitudes régulièrement nourries quant aux effets réels de ce type d'armes, on ne peut pas non plus exclure, *a contrario* de la communication classique russe surévaluant l'efficacité de nombreux équipements, que les déclarations du général minorent à dessein les performances d'un équipement des plus sensibles.

---

[23] Andrew Tate, « Chinese *Navy* trials laser weapon », *Jane's Defence Weekly*, 10 April 2019

[24] Elsa B. Kania, « The PLA's Potential Breakthrough in High-Power Microwave Weapons, » *Diplomat*, March 11, 2017; Jeffrey Lin and P.W. Singer, "China's New Microwave Weapon » Can Disable Missiles and Paralyze Tanks," Popular Science, January 26, 2016.

[25] Tatyana Rusakova, « Russia's new microwave gun to target drones », *Russia Beyond*, July 23, 2015, https://www.rbth.com/defence/2015/07/23/russias_new_microwave_gun_to_target_drones_47953.html

[26] Carlo Kopp, « Russian / Soviet Point Defence Weapons », Technical Report APA-TR-2008-0502, *Air Power Australia*, May, 2008, Updated April, 2012, http://www.ausairpower.net/APA-Rus-PLA-PD-SAM.html

2.4 Conclusion

En conclusion, il apparaît probable que les Chinois ne soient guère éloignés des Américains en ce qui concerne tant les armes laser que les armes EM. Dans ce dernier domaine, ils sont peut-être même en avance en ce qui concerne la protection des plateformes navales.

Cependant, en ce qui concerne les armes laser, la vulnérabilité des deux camps apparaît encore réduite, pour deux raisons. Tout d'abord, la première génération de SSL en cours de maturation sera destinée à la lutte anti-drones courte portée, certainement pas à stopper les vagues de missiles du compétiteur stratégique. Quant aux lasers de contre-mesure optronique, à visée ASAT par exemple, ils ne constituent pas une solution miracle, un élément clé de l'arsenal anti-ISR adverse : aveugler entièrement un capteur optronique récent nécessite de détruire des millions de pixels, ce qui nécessite des techniques de balayage laser dont la précision excède les systèmes de pointage envisageable.

Il est donc possible, de prime abord, que l'impact des armes EM soit beaucoup plus important que celui des lasers dans l'environnement haute intensité qui caractérise la présente compétition. Cependant, les incertitudes quant aux performances réelles de ces armes, aux types de systèmes pouvant être affectés par chacune préviennent toute formulation de conclusions significatives.

3. Le « *counterspace* »

Les capacités « *counterspace* » offensives ne sont que rarement des moyens spécifiquement et explicitement conçus pour des opérations contre les systèmes spatiaux : soit elles emploient des technologies appliquées dans d'autres domaines de confrontation (défense anti-missile, guerre électronique, AED, cyber) ; soit elles reposent sur des systèmes ayant officiellement un usage civil (satellites de maintenance, radars de suivi), potentiellement utilisables à des fins hostiles.

Comme le relevait une étude récente de la FRS, « *officiellement, aucune des trois grandes puissances spatiales n'annonce avoir de programme antisatellite opérationnel. Seules sont connues des capacités technologiques expérimentales ou des programmes passés et leur utilisation future est hypothétique en l'absence de doctrine déclarée* »[27].

3.1 Technologies impliquées

Les attaques contre les capacités spatiales peuvent viser les systèmes déployés dans l'espace, mais aussi les installations terrestres de suivi (segment contrôle) ou de réception

[27] Florence Gaillard-Sborowski, Isabelle Facon, Xavier Pasco, Isabelle Sourbès Verger, Philippe Achilleas, *Sécuriser l'espace extra-atmosphérique : éléments pour une diplomatie spatiale à l'horizon 2030*, Paris, FRS, Février 2016, p. 64.

et traitement des signaux (segment utilisateurs). Les menaces cinétiques (frappe, opérations conventionnelles) contre les installations à terre, n'ayant pas de spécificité, ne sont pas abordées ici.

Cinq types de menaces « anti-spatiales » sont généralement répertoriés, en fonction des technologies employées[28] :

- Les attaques cinétiques en tir direct visant à détruire des satellites (*Direct-ascent ASAT*, DA-ASAT), soit depuis la surface (intercepteur anti-missile basé à terre ou en mer), soit depuis les airs (missile tiré d'avion) ;
- Les attaques contre des satellites menées par des engins en orbite (*co-orbital ASAT*), utilisant des armes cinétiques (satellites « kamikazes » ou dotés de systèmes de capture) ou non (brouillage électronique) ;
- Les attaques électroniques visant la transmission des données entre les satellites et le sol ;
- Les attaques contre satellites menées depuis le sol par des armes à énergie dirigée (laser) ;
- Les attaques cyber, visant les données échangées et susceptibles d'être menées contre toutes les composantes d'un système spatial (stations au sol[29] et satellites).

Tableau récapitulatif des capacités de *counterspace*

Figure n° 7 : TABLEAU DES CAPACITÉS DE *COUNTERSPACE*

Capacités requises	Effets réalisables	Limites
▶ Attaque cinétique depuis la Terre		
Intercepteur balistique de moyenne portée, doté d'un véhicule « tueur » exo-atmosphérique avec dispositifs terminaux de détection (infrarouge ou radar) et de manœuvre[30]. Missile lancé d'avion.	Possibilité d'endommager/détruire : - un satellite en orbite basse en quelques minutes (5 à 15 minutes) depuis le sol ; - un satellite en orbite géosynchrone en plusieurs heures (4 heures). (Caractéristiques des orbites en annexe) ▶Atteinte structurelle	Un système basé au sol devrait attendre le passage du satellite visé[31] : ⇒ Nécessité de placer des intercepteurs sur différents sites ; ⇒ Ou utilisation de missiles embarqués sur avions.

[28] C'est notamment le cas dans le rapport publié par la DIA : Defense Intelligence Agency, *Challenges to Security in Space*, Washington (D.C.), January 2019.

[29] En 2014, des *hackers* se sont introduits dans le réseau informatique de l'Agence américaine d'observation océanique et atmosphérique (NOAA). Suite à cette attaque, la NOAA a arrêté de fournir des images satellite au service météorologique américain pendant deux jours.

[30] Florence Gaillard-Sborowski, Isabelle Facon, Xavier Pasco, Isabelle Sourbès-Verger, Philippe Achilleas, *Sécuriser l'espace extra-atmosphérique : éléments pour une diplomatie spatiale à l'horizon 2030*, *op. cit.*, p. 37 et p. 67.

[31] David Wright, Laura Grego, Lisbeth Gronlund, *The Physics of Space Security*, American Academy of Arts and Sciences, 2005, p. 156.

	▶Dommages permanents	La destruction de satellites produit des débris dangereux pour toutes les puissances spatiales[32].
▶ Attaque non cinétique depuis la Terre		
Laser de haute puissance (chimique/solide)[33] ; + système de contrôle précis du faisceau ; + optiques *to counteract atmospheric turbulence* pour les lasers basés au sol. Les systèmes de suivi *Satellite Laser Ranging (SLR)* seraient suffisamment puissants pour aveugler des capteurs optiques.	- Eblouissement (*dazzling*) des capteurs optiques (par saturation des pixels) des satellites de télédétection (reconnaissance) en orbite basse. ⇒ un laser de 10 W pourrait aveugler une zone de 1 km de rayon ; un laser de plusieurs kilowatts, une zone d'environ 10 km[34]. - Aveuglement des senseurs par destruction du plan focal. - Dommages physiques par échauffement prolongé des surfaces. ▶ Atteinte fonctionnelle réversible ▶ Possibilité de dommages structurels permanents.	Nécessité de connaitre précisément l'attitude du satellite visé. Nécessité pour l'attaquant d'être placé en ligne de visée directe. Les satellites en GEO sont hors de portée de lasers au sol ou en orbite basse.
▶ Attaque en orbite		
Systèmes capables de manœuvrer en orbite (réserve de carburant) pour se positionner à proximité de leur cible : - Satellites de service / Engins d'élimination des débris (*Active debris removal*, ADR), dotés de bras / de harpon / de filet ; - Satellites équipés de systèmes de guerre électronique.	Possibilité d'endommager un satellite mais aussi de le détruire par collision ou en l'entraînant hors de son orbite. Menace pour les satellites en LEO ; possibilité de manœuvre d'un engin en LEO vers les orbites plus hautes. ▶Dommages structurels permanents ▶Possibilité d'atteinte fonctionnelle	Multiples satellites ADR nécessaires pour neutraliser effectivement une constellation[35]. Manœuvres lentes et limitées, laissant du temps de réaction à la cible visée.
Satellites embarquant des AED Laser : option douteuse compte tenu de la quantité d'énergie nécessaire. HPM :	Onde EM générant un champ électrique suffisamment puissant pour créer un survoltage dans les circuits électriques de la cible. ▶ Atteinte fonctionnelle.	Technologie HPM encore en développement : problème de conception d'un émetteur puissant de taille[36].

[32] L'essai effectué par la Chine en 2007 a produit plus de 2.300 débris détectables par les systèmes de surveillance et environ 150.000 morceaux de plus de 1 cm.

[33] Brian Weeden, Victoria Samson, *Global Counterspace Capabilities: An Open Source Assessment,* Secure World Foundation, April 2019, p. 1-18.

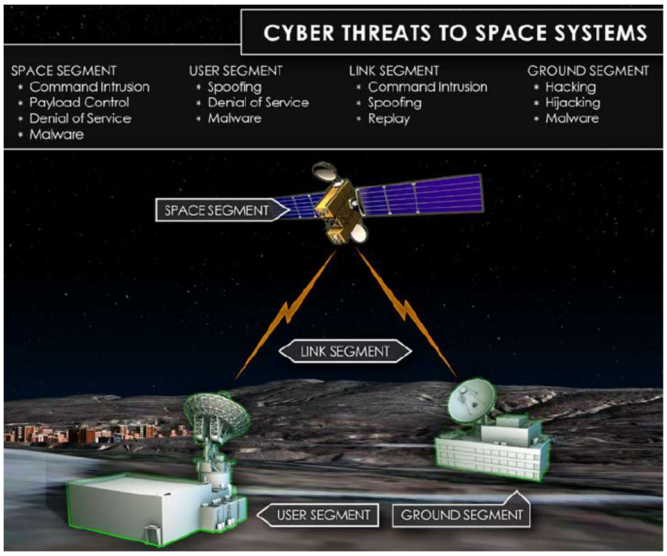
[34] David Wright, Laura Grego, Lisbeth Gronlund, *The Physics of Space Security*, *op. cit.*, p. 127.

[35] Bohumil Dobos, Jakub Prazak, "To Clear or to Eliminate ? Active Debris Removal Systems as Antisatellite Weapons", *Space Policy*, n°47, February 2019, p. 221.

[36] David Wright, Laura Grego, Lisbeth Gronlund, *The Physics of Space Security*, *op. cit.*, p. 132.

- à bande étroite, visant les récepteurs, antennes de communications ou radars ; - ou à large bande, affectant les composants électroniques non durcis.		La prédictibilité de l'effet d'une arme HPM est limitée. Effets indiscriminés sur tous les systèmes proches.
▶ **Guerre électronique**		
Disponibilité dans le commerce de systèmes de brouillage peu coûteux, efficaces contre le segment utilisateur[37].	Brouillage ou leurrage des faisceaux ascendants / descendants. ▶ Atteinte fonctionnelle. ▶ Effets temporaires et réversibles	Bonne résistance des systèmes militaires de navigation et options de limitation des effets d'une attaque[38].
▶ **Cyber attaque**		
	Compromission des données. Prise de contrôle logicielle d'un satellite. ▶ Atteinte fonctionnelle.	

Figure n° 8 : TYPES DE MENACES CYBER[39]



Dans la plupart des cas, l'attaque contre les systèmes spatiaux repose en outre sur un système de détection et surveillance (à terre ou en orbite), permettant d'identifier et localiser précisément les satellites (*Space situational awareness*, SSA).

[37] *Ibid.*, p. 119.

[38] Brian Weeden, Victoria Samson, *Global Counterspace Capabilities: An Open Source Assessment,* [2019], p. 1-17.

[39] National Air and Space Intelligence Center, *Competing in Space*, Wright-Patterson AFB, Public Affairs Office, December 2018, p. 19.

La surveillance de l'espace demande d'accomplir trois fonctions principales[40] :

- La détection des objets en orbite sans disposer de connaissance a priori (existence, position…) ;
- La détermination des paramètres orbitaux (trajectographie) de l'objet observé avec une précision demandée variable en fonction de l'exploitation envisagée et mises à jour régulières ;
- L'identification.

Un réseau de surveillance repose donc sur une combinaison de moyens radars et optiques (télescope) auxquels sont adjoints des capacités de transmission et de traitement adaptées pour détecter les objets en orbite, déterminer leur trajectoire et préciser leur forme et leur taille.

3.2 Développements chinois et russes et vulnérabilités américaines

L'importance de l'espace dans la sécurité nationale et la stratégie de défense des États-Unis s'est affirmée de manière croissante à partir des années 1990, jusqu'à constituer un « intérêt vital » dans la *National Space Policy* de 2006. Dès lors, la protection des systèmes spatiaux devient un enjeu majeur et l'attention portée aux menaces potentielles se développe.

Deux arguments structurent le discours américain sur les menaces dans le domaine spatial :

- Il s'agit d'une part de la reconnaissance d'une vulnérabilité particulière des États-Unis , liée à leur dépendance à l'égard des systèmes spatiaux ;
- D'autre part, les adversaires ayant analysé cette vulnérabilité, s'emploient à développer leurs capacités contre-spatiales pour priver les États-Unis d'un avantage majeur en cas de conflit.

Le thème de la « dépendance à l'espace » est mis en exergue dès 2001 dans le rapport de la *Commission to Assess National Security Space Management and Organization* (dite « Commission Rumsfeld »). Les systèmes spatiaux étant de plus en plus indispensables au fonctionnement de l'économie comme à la stratégie militaire, ils apparaissent comme des « *cibles potentielles attractives* », qu'il faut pouvoir défendre[41].

Selon la base de données de l'UCS, au 31 décembre 2018, près de 850 satellites américains sont en orbite, dont 170 sont des satellites gouvernementaux, presque tous militaires[42].

---

[40] Florence Gaillard-Sborowski, Isabelle Facon, Xavier Pasco, Isabelle Sourbès-Verger, Philippe Achilleas, *Sécuriser l'espace extra-atmosphérique : éléments pour une diplomatie spatiale à l'horizon 2030*, *op. cit.*, p. 86.

[41] Donald Rumsfeld (Chairman), *Report of the Commission to Assess United States National Security Space Management and Organization*, Executive Summary, January 2001, p. 9.

[42] *UCS Satellite Database*, Union of Concerned Scientists. https://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database

La perception américaine des menaces est alimentée :

- En partie par le développement ou la démonstration de capacités spatiales susceptibles de contester la suprématie américaine, tel que le lancement par la Chine en mai 2013 d'un missile capable d'approcher l'orbite géosynchrone (36.000 km) ;
- Mais surtout, par l'évolution des relations globales avec les autres puissances, dont la nature détermine largement le sens donné aux activités spatiales[43] : le retour de la confrontation avec la Russie et l'affirmation de la compétition avec la Chine depuis 2014 renforcent considérablement l'inquiétude quant à leurs capacités[44], même lorsque celles-ci sont ambiguës.

Aujourd'hui, les deux pays sont officiellement présentés dans les rapports et les discours officiels comme poursuivant des programmes offensifs destinés à dégrader ou interdire l'utilisation des systèmes spatiaux américains. Lors d'une conférence au CSIS en avril 2019, le *DASD for Space policy* explique que « *les menaces contre les systèmes spatiaux sont réelles, graves et en augmentation* »[45]. Il est communément admis dans la communauté stratégique américaine que « *la Chine et la Russie pourraient considérer l'aptitude à interdire l'utilisation de l'espace aux* États-Unis *comme un moyen important de dissuader des opérations militaires classiques* » ; et en cas de conflit, ce serait *« un multiplicateur de force »*[46].

Les discours stratégiques chinois et russes semblent effectivement accorder une importance considérable à la dimension spatiale des conflits futurs. Dans les deux pays, la réflexion doctrinale insiste sur la nécessité d'obtenir la supériorité aérospatiale (en Russie) / spatiale (en Chine) dès le début d'une confrontation, pour avoir la possibilité d'atteindre ses objectifs. Il s'agit, selon l'Armée Populaire de Libération (APL) de « *s'assurer de la possibilité d'utiliser l'espace sans restriction tout en limitant, réduisant ou détruisant les forces spatiales d'un adversaire* »[47].

Le développement de systèmes « *counterspace* » serait ainsi une priorité pour la Chine, à la fois :

---

[43] Comme en témoigne la réaction mesurée des Etats-Unis à l'expérimentation indienne de destruction d'un satellite, réalisée en mars 2019.

[44] En 2008, une Commission indépendante estimait encore que « *ni la Russie ni la Chine ne représente une menace majeure* » dans le domaine spatial. A. Thomas Young (Chairman), *Leadership, Management, and Organization for National Security Space*, Report to Congress of the Independent Assessment Panel on the Organization and Management of National Security Space, Institute for Defense Analyses, July 2008, p. 9.

[45] Steve Kitay, Evaluating the Global Counterspace Landscape, Washington (D.C.), CSIS, April 23, 2019. https://www.csis.org/events/evaluating-global-counterspace-landscape?utm_source=CSIS+All&utm_campaign=024a8907ed-EMAIL_CAMPAIGN_2017_12_31_COPY_01&utm_medium=email&utm_term=0_f326fc46b6-024a8907ed-221741637

[46] National Academies of Sciences, Engineering, and Medicine, *National Security Space Defense and Protection: Public Repor*t, Washington (DC), The National Academies Press, 2016, p. 42.

[47] Jiang Lianju, Wang Liwen, eds., *Textbook for the Study of Space Operations,* Beijing, Military Science Publishing House, 2013. Cité par Zaeem Shabbir, Ali Sarosh, "Counterspace Operations and Nascent Space Powers", *Astropolitics*, June 2018, p. 7.

- Dans une logique de dissuasion d'une intervention américaine « dans sa sphère d'influence »[48] ;
- Et, en cas de confrontation, comme facteur « *égalisateur* » de puissance (*game-leveler*)[49].

L'attaque des satellites américains serait notamment un facteur de renforcement de la stratégie d'interdiction, en menaçant les capacités C4ISR sur lesquelles reposent les opérations de projection[50]. Certains analystes chinois considèrent même que l'interdiction de l'usage de l'espace aux armées américaines causerait leur défaite[51].

Du côté russe également, l'espace est devenu un domaine de combat dont la maîtrise sera décisive pour gagner une future guerre[52]. Selon la DIA, « *la Russie développe par conséquent des systèmes contre-spatiaux pour neutraliser ou interdire aux* États-Unis *l'utilisation des services spatiaux, militaires et commerciaux ».* Cela participe à la recherche de méthodes asymétriques de « compensation » *(offsetting)* de l'avantage militaire américain.

3.2.1 L'organisation des forces spatiales

L'importance accordée à la dimension spatiale s'est traduite, en Russie puis en Chine, par des réorganisations visant à mieux intégrer la contribution des moyens spatiaux aux opérations.

La Russie avait créé en 1992 la première Force militaire spatiale, en charge des activités de lancement, de la défense spatiale et de la surveillance radar à longue portée. En 2011, elle a été combinée avec les Forces de défense aérienne, puis l'ensemble est intégré depuis aout 2015 avec les Forces aériennes pour former les Forces aérospatiales (Воздушно-космическиесилы,*Vozdushno-Kosmicheskiye Sily*, VKS), reflétant la conception russe d'une intégration des opérations aériennes et spatiales[53]. Les VKS assurent le commandement des forces aériennes de combat et de transport, des réseaux de défense anti-aérienne et anti-missile, ainsi que des Forces spatiales, qui sont plus spécifiquement responsables de[54] :

- La surveillance des objets spatiaux, l'identification des menaces potentielles dans l'espace et la prévention d'éventuelles attaques ;

---

[48] Brian Weeden, Victoria Samson, *Global Counterspace Capabilities: An Open Source Assessment,* Secure World Foundation, April 2018, p. 1-1.

[49] Tate Nurkin, *China's Advanced Weapon Systems*, Report prepared for the US China Economic and Security Commission, Jane's IHS Markit, May 2018, p. 139.

[50] Malcolm Davis, "China's space mission (part 1): dominating a contested domain", ASPI, *The Strategist*, April 15, 2019.

[51] Brian Weeden, Victoria Samson, *Global Counterspace Capabilities: An Open Source Assessment,* [2018], *op. cit.,* p. 1-21.

[52] Defense Intelligence Agency, *Challenges to Security in Space*, *op. cit.,* p. 23.

[53] Nicole J. Jackson, *Outer Space in Russia's Security Strategy*, Simons Papers in Security and Development, No. 64/2018, School for International Studies, Simon Fraser University, Vancouver, August 2018, p. 7.

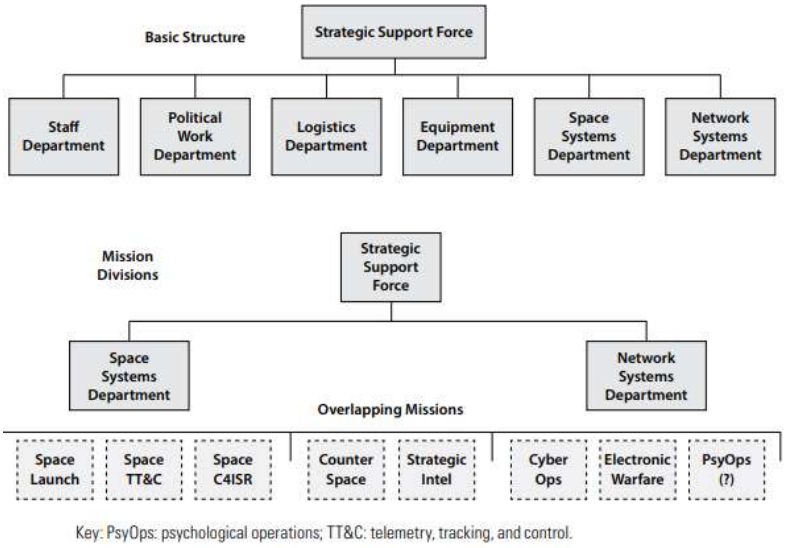
[54] Jeffrey L. Caton, *Impacts of Anti-Access/Area Denial Measures on Space Systems: Issues and Implications for Army and Joint Forces*, Carlisles Barracks, US *Army* War College, SSI, September 2018, p. 21.

- Le lancement, le suivi et la maintenance des satellites militaires et à « double-usage », en particulier du réseau d'alerte stratégique avancée.

Les réformes de la défense menées en Chine ont conduit à la création en décembre 2015, d'une Force de Soutien Stratégique (FSS - 战略支援部), regroupant les activités spatiales, cyber, de guerre électronique et psychologique sous un commandement unifié, afin de mieux les intégrer aux opérations. Ces différentes capacités sont jugées essentielles à la conduite des guerres *« informatisées »* (信息化)[55]. La FSS est divisée en deux branches[56] :

- Le Département des systèmes de réseaux, qui a la responsabilité des opérations d'information ;
- Et le Département des systèmes spatiaux, qui chapeaute pratiquement toutes les activités spatiales auparavant dispersées entre plusieurs entités, à savoir : la surveillance et le contrôle des systèmes spatiaux ; le lancement ; l'exploitation de l'information spatiale ; les missions d'attaque et de défense[57].

Figure n° 9 : STRUCTURE DE LA FSS[58]



Key: PsyOps: psychological operations; TT&C: telemetry, tracking, and control.

Toutefois, le rôle de la FSS dans le développement des moyens et la conduite des opérations ASAT n'est pas clair. Un essai de missile DN-3 effectué en août 2017, depuis le site de lancement de Jiuquan, peut laisser penser que les Forces spatiales sont respon-

[55] Elsa B. Kania, "China Has a 'Space Force.' What Are Its Lessons for the Pentagon?", *Defense One*, September 29, 2018.

[56] John Costello, Joe McReynolds, "China's Strategic Support Force. A Force for a New Era", in Phillip C. Saunders, Arthur S. Ding, Andrew Scobell, Andrew N.D. Yang, Joel Wuthnow (Eds.), *Chairman Xi Remakes the PLA*, Washington (D.C), National Defense University Press, 2019, p. 450.

[57] *Ibid.*, p. 455.

[58] *Ibid.*, p. 442.

sables du déploiement de ces systèmes potentiellement ASAT. Mais selon certains auteurs, le contrôle des systèmes contre-spatiaux relève toujours de l'Armée des lanceurs (火箭军)[59].

3.2.2 Les capacités anti-spatiales identifiées par les États-Unis

Dans sa présentation annuelle des menaces au Congrès, en mars 2018, le Directeur du Renseignement expliquait que « *la Russie et la Chine continuent à développer des armes anti-satellites pour réduire l'efficacité militaire des* États-Unis ». Ils cherchent à se doter de moyens anti-spatiaux « *destructeurs et non-destructeurs* » en prévision d'un conflit possible. Les documents institutionnels sont rarement plus détaillés, mais les analyses des experts identifient un certain nombre de programmes présentés comme constituant des capacités anti-spatiales et couvrant toute la gamme des options offensives.

➧ Capacités d'attaque cinétique depuis la Terre

La Russie poursuit trois programmes de véhicules d'interception cinétique susceptibles de constituer une capacité anti-satellite en tir direct (DA-ASAT) :

- Le **PL-19 / Nudol** (désignation russe : 14Ts033) : intercepteur de défense anti-missile sol-air (intégré au complexe A-235) dont la portée lui permettrait d'atteindre les satellites en orbite basse. Monté sur tracteur-érecteur-lanceur, il pourrait être déplacé pour menacer plusieurs satellites successivement[60]. En développement depuis 2011, la date de son déploiement n'est pas encore définie. Il a été testé 6 fois entre 2014 et mai 2018, puis en décembre 2018 : il a alors volé 17 minutes et parcouru 3000 km.
- Le **S-500 Prometeï** : intercepteur anti-missile sol-air, mobile, d'une portée de 600 km, ce qui devrait lui permettre d'atteindre une orbite à 300 km d'altitude. Il doit pouvoir détruire un ICBM en vol exo-atmosphérique avant la séparation des têtes et éventuellement des satellites[61]. Il serait entré en production en mars 2018 et pourrait être opérationnel fin 2020.
- Le **78M-6 Kontakt** : intercepteur air-air, qui pourrait atteindre les satellites en orbite basse. Il s'agit de la reprise depuis 2009 d'un projet des années 1980, visant à embarquer un missile ASAT, cette fois sur un MiG-31BM. Un essai de vol aurait été effectué en septembre 2018[62] et le système est supposé être opérationnel d'ici 2022.

---

[59] Malcolm Davis, "China's space mission (part 1): dominating a contested domain", *op. cit.*

[60] Sean O'Connor, "Russia's ASAT development takes aim at LEO assets", *Jane's Intelligence Review*, 2018. https://www.janes.com/images/assets/591/81591/Russias_ASAT_development_takes_aim_at_LEO_assets_v2.pdf

[61] Déclaration du Lieutenant General Vladimir Lyaporov, Chief of the Zhukov Air and Space Defence Academy, cité in "S-500 Missile System Crews Already Being Trained by Russian Air Defence Forces; A Look at the Game Changing Platform's Capabilities", *Military Watch Magazine*, March 6, 2019. https://militarywatchmagazine.com/article/s-500-missile-system-crews-already-being-trained-by-russian-air-defence-forces-a-look-at-the-game-changing-platform-s-capabilities

[62] Amanda Macias, "A never-before-seen Russian missile is identified as an anti-satellite weapon and will be ready for warfare by 2022", CNBC, October 25, 2018. https://www.cnbc.com/2018/10/25/russian-missile-identified-as-anti-satellite-weapon-ready-by-2022.html

Du côté de la Chine, la DIA estime en 2019 que « *l'APL dispose d'un missile ASAT basé à terre opérationnel »,* capable de menacer les satellites en orbite basse[63]. Il s'agit probablement du **SC-19 (ou DN-1),** dérivé du missile de moyenne portée DF-21C[64], qui aurait une portée ascendante de 1250 km. Testé pour la première fois en 2005, il a suscité une grande émotion lors de l'essai de janvier 2007, en détruisant un satellite météo à 865 km d'altitude et à une vitesse de 8km/s, provoquant des milliers de débris. Le système serait probablement opérationnel en 2019[65].

Figure n° 10 : DF-21C

Deux autres systèmes, également présentés par la Chine comme des intercepteurs de défense anti-missile, sont potentiellement des systèmes contre-spatiaux :

- Le **DN-2**[66], dérivé d'un missile balistique mobile, testé en mai 2013 et dont la portée ascendante aurait atteint l'orbite géostationnaire (36.000 km) selon les observations américaines ;
- Le **DN-3** (ou KO-9), testé à trois reprises en 2015 et 2018 et dont les capacités ASAT ne sont pas confirmées.

Pour les experts de la *Secure World Foundation*, il est probable que « *la série des systèmes DN soit en réalité un système de défense anti-missile, comparable au SM-3 américain, ayant des capacités ASAT latentes* »[67]. L'Administration américaine tend cependant à interpréter presque systématiquement l'ensemble des interceptions antimissiles chinoises comme des interceptions de type ASAT, se fondant notamment sur l'analyse des cibles et des modes d'interception.

---

[63] Defense Intelligence Agency, *Challenges to Security in Space*, *op. cit.*, p. 21.

[64] Tate Nurkin, *China's Advanced Weapon Systems*, *op. cit.*, p. 140.

[65] Brian Weeden, Victoria Samson, *Global Counterspace Capabilities: An Open Source Assessment,* [2019] *op. cit.*, p. 1-13.

[66] Cette désignation américaine n'a pas été officiellement confirmée.

[67] Brian Weeden, Victoria Samson, *Global Counterspace Capabilities: An Open Source Assessment,* [2019] *op. cit.,* p. 1-13.

➧ Capacités ASAT non-cinétiques depuis la Terre

Les États-Unis s'inquiètent de l'utilisation possible de lasers terrestres contre leurs satellites.

L'URSS avait commencé à développer des programmes d'armes lasers dans les années 1970 et 1980 et des travaux ont vraisemblablement repris depuis la décennie 2010. Cela concerne principalement le ***Sokol-Eshelon*** (1LK222, Сокол-Эшелон), laser chimique de contre-mesure optronique embarqué sur l'extrados d'un IL-76 modifié, l'A-60. Il aurait été testé en 2009, permettant d'illuminer un satellite orbitant à 1.500 km. Le développement du système, entamé à la fin de la guerre froide, a été repris, par à-coup, depuis 2003 par Almaz-Antey qui l'aurait achevé en 2018[68].

Figure n° 11 : SYSTÈME SOKOL-ESHELON

En juillet 2018, le ministère russe de la défense a par ailleurs annoncé l'entrée en service dans les VKS d'un système laser mobile, le ***Peresvet*** (Пересвет). Dévoilé en mars 2018, il est officiellement présenté comme destiné à l'interception de missiles balistiques en phase de vol exo-atmosphérique. Cependant, le niveau général de maturation technologique de laser solide d'une telle puissance rend très improbable sinon impossible cette capacité. Vu les dimensions de l'appareil présenté sur les images, il est possible qu'il soit destiné à la contre-mesure optronique[69].

---

[68] « ASAT : quel est l'état de la menace ? », DSI, n°28, février-mars 2013. https://www.defense24.news/2018/02/23/asats-letat-de-menace/ & Arun Mathew, « Russia Completes Development of Airborne Anti-satellite Laser Weapon », Defpost, February 26, 2018, https://defpost.com/russia-completes-development-airborne-anti-satellite-laser-weapon/

[69] Voir vidéo « Russian military Laser Gun/Cannon for Anti-missile System 01.03.18 », https://www.youtube.com/watch?v=LwwafKqjgG4, Kirill Ryabov « Новости от президента: боевой лазерный комплекс », topwar.ru, 9 марта 2018, http://*Army*-news.ru/2018/03/rossijskij-boevoj-lazernyj-kompleks/ ; « "Peresvet" Combat Laser Complex », Globalsecurity, 2018, non daté https://www.globalsecurity.org/military/world/russia/vlk.htm

Figure n° 12 : SYSTÈME PERESVET

Le danger peut aussi venir de l'adaptation des lasers de surveillance spatiale qui pourraient être utilisés pour aveugler ou endommager des satellites. En juin 2018, les médias russes ont annoncé que des chercheurs d'une division de Roscosmos (*Scientific and Industrial Corporation 'Precision Instrument Systems', NPK SPP),* travaillent sur une nouvelle technologie qui permettrait de *« vaporiser des débris spatiaux potentiellement dangereux grâce à un faisceau laser »*[70]. Il s'agirait de coupler le télescope du centre d'Altay[71] avec un laser pour en faire un *« canon laser »*. En septembre, c'est un article de *Jane's Intelligence Review* qui évoque la possible transformation du système de surveillance laser (*"laser optical locator"*, 30Zh6, image ci-dessous)[72] du Complexe de Krona en arme anti-satellite[73].

[70] "High-Tech Firepower: Russia Develops New Space Laser Cannon", *Sputnik International*, 06.10.2018. https://sputniknews.com/science/201806101065288031-laser-cannon-space-debris/

[71] Situé près de la frontière avec le Kazakhstan.

[72] Bart Hendrickx, *NASA SpaceFlight.com*, 2018. https://forum.nasaspaceflight.com/index.php?topic=46485.0

[73] Todd Harrison, Kaitlyn Johnson, Thomas G. Roberts, *Space Threat Assessment 2019*, *op. cit.*, p. 22.

En ce qui concerne la Chine, la DIA affirme qu'elle « *pourra probablement déployer une arme laser terrestre capable de contrer les capteurs spatiaux en orbite basse d'ici 2020* » et qu'elle pourrait avoir des systèmes « *plus puissants* » à la fin de la prochaine décennie[74]. Mais aucune précision n'est donnée sur les systèmes en question, dont il n'est pas fait état dans les études de la *Secure World Foundation*. Le seul élément factuel est une déclaration du Directeur du NRO en 2006, indiquant que des satellites de reconnaissance américains avaient été éblouis lors de leur survol de la Chine[75].

➧ Capacités ASAT en orbite

Les seuls systèmes offensifs spécifiques au domaine spatial sont les engins d'attaque « co-orbitale ». Mais tous les programmes menés actuellement sont officiellement conçus à des fins pacifiques, de maintenance ou d'élimination des débris. Comme le reconnaissait en 2018 une responsable du DoS, « *it is difficult to determine an object's true purpose simply by observing it on orbit*"[76].

Durant la Guerre froide, l'URSS avait développé une arme co-orbitale et démontré des capacités d'interception de satellites en orbite basse à la fin des années 1970[77]. Le système pouvait manœuvrer sur une ou deux orbites, guidé depuis le sol, pour approcher à une dizaine de mètres d'un satellite et l'endommager en explosant[78]. Il a été retiré du service en 1993.

---

[74] Defense Intelligence Agency, *Challenges to Security in Space*, *op. cit.,* p. 20.

[75] Todd Harrison, Kaitlyn Johnson, Thomas G. Roberts, *Space Threat Assessment 2019*, *op. cit.,* p. 14.

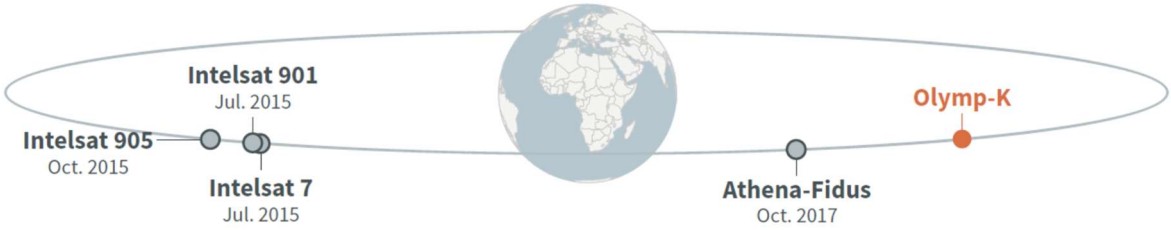
[76] Yleem D.S. Poblete, Assistant Secretary, Bureau of Arms Control, Verification and Compliance, Remarks on Recent Russian Space Activities of Concern, Conference on Disarmament, Geneva, August 14, 2018. https://www.state.gov/t/avc/rls/285128.htm

[77] Bart Hendrickx, "Self-defense in space: protecting Russian spacecraft from ASAT attacks", *The Space Review*, July 16, 2018. http://www.thespacereview.com/article/3536/1

[78] Laura Grego, *A History of Anti-Satellite Programs*, Union of Concerned Scientists, January 2012, p. 3.

Depuis 2010, une succession de manœuvres d'approche (*Rendezvous and Proximity Operations*, RPO) ont été effectuées par différents satellites russes, en orbites basse et géosynchrone, laissant envisager des essais d'action hostile[79] :

- Manœuvres du satellite Kosmos 2499, entre juin 2014 et mars 2016 ;
- Du Kosmos 2504, entre avril 2015 et avril 2017 ;
- Du Kosmos 2521, séparé du Kosmos 2519 en août 2017, ayant effectué plusieurs manœuvres avant de revenir s'y amarrer en octobre 2018. Il pourrait aussi avoir largué un autre satellite en octobre 2017, dont le comportement a été jugé « *très anormal* » par le Département d'Etat, sans plus de précision[80] ;
- Du Kosmos 2501 (Olymp-K), entre octobre 2014 et août 2017, qui s'est approché jusqu'à 10 km d'autres satellites (notamment des Intelsat) en orbite géosynchrone, probablement « *pour une mission de surveillance ou de renseignement* »[81] (schéma ci-dessous).



Les manœuvres réalisées laissent penser que ces satellites peuvent être destinés à l'inspection et à l'amélioration de la SSA, mais aussi à l'interception de communications.

Par ailleurs, un spécialiste des programmes spatiaux russes, repris dans les rapports américains[82], estime qu'un programme ASAT co-orbital (Burevestnik-KA), éventuellement susceptible d'opérer en orbite géosynchrone, est peut-être en cours de développement depuis mai 2014[83].

Les activités chinoises sont jugées tout aussi inquiétantes aux États-Unis. Un rapport de novembre 2015 de la *US-China Commission* affirme qu'elles « *indiquent que* [la Chine] *dé-*

---

[79] Brian Weeden, Victoria Samson, *Global Counterspace Capabilities: An Open Source Assessment,* [2018] *op. cit.,* p. 2-1.

[80] Mike Wall, "'Very Abnormal' Russian Satellite Doesn't Seem So Threatening, Experts Say", *Space.com*, August 16, 2018. https://www.space.com/41511-weird-russian-satellite-not-so-abnormal.html

[81] Brian Weeden, Victoria Samson, *Global Counterspace Capabilities: An Open Source Assessment,* [2018] *op. cit.*, p. 2-11.

[82] Le rapport du CSIS reprend la source originale, sans mentionner les nombreuses incertitudes qui y figurent, et en évoquant le programme, vraisemblablement expérimental, comme « *le nouveau système co-orbital* » russe. Todd Harrison, Kaitlyn Johnson, Thomas G. Roberts, *Space Threat Assessment 2019*, *op. cit.,* p. 21.

[83] Bart Hendrickx, "Burevestnik : a new Russian ASAT ?", *NASA SpaceFlight.com*. https://forum.nasaspaceflight.com/index.php?topic=45734.0

veloppe des systèmes antisatellites co-orbitaux pour cibler » les satellites américains. Un article de 2017 prétend que « *depuis 2008, la Chine travaille sur une arme antisatellite co-orbitale* » qui « *pourrait attaquer simultanément plusieurs satellites essentiels, de si près que les* États-Unis *n'auraient pas le temps d'empêcher les dommages* »[84]. Une analyse publiée en 2018 par *Jane's* décrit encore plus abruptement les satellites chinois de manœuvre co-orbitale comme des « *satellites kamikazes et assassins* »[85].

Selon les derniers rapports de la *Secure World Foundation*, la Chine a effectivement « *mené de multiples essais de technologies d'approche à la fois en orbite basse et géosynchrone qui pourraient conduire à une capacité ASAT co-orbitale* »[86]. Mais les auteurs admettent qu'il n'existe « *aucune preuve que ces technologies RPO soient irréfutablement développées pour un usage anti-spatial* ».

Les premières manœuvres suspectes identifiées datent de 2010, impliquant les satellites Shi Jian-12 (SJ-12) et SJ-06F. Plusieurs autres activités ont été observées, les plus récentes début 2019 (voir tableau ci-dessous)[87].

Table 1-2 - Recent Chinese Rendezvous and Proximity Operations

Date(s)	System(s)	Orbital Parameters	Notes
June – Aug. 2010	SJ-06F, SJ-12	570-600 km; 97.6°	SJ-12 maneuvered to rendezvous with SJ-06F. Satellites may have bumped into each other.
July 2013 – May 2016	SY-7, CX-3, SJ-15	Approx. 670 km; 98°	SY-7 released an additional object that it performed maneuvers with and may have had a telerobotic arm. CX-3 performed optical surveillance of other in-space objects. SJ-15 Demonstrated altitude and inclination changes to approach other satellites.
Nov. 2016 – Feb. 2018	SJ-17, YZ-2 upper stage	35,600 km; 0°	YZ-2 upper stage failed to burn to the graveyard orbit and stayed near GEO. SJ-17 demonstrated maneuverability around the GEO belt and circumnavigated Chinasat 5A.
Jan. 2019	TKS-3, TKS-3 AGM	35,600 km; 0°	TkS-3 AKM separated from the TKS-3 in the GEO belt and both performed small maneuvers to maintain relatively close orbital slots.

Au-delà des manœuvres effectuées par ces satellites, les inquiétudes américaines sont alimentées par la nature même des systèmes :

- Le **Shi Jian-7** serait un satellite de service, doté d'un bras robotisé, ce qui lui donne une aptitude à endommager ou déplacer un système en orbite ;
- Le **Shi Jian-17** dispose d'équipements électro-optiques, officiellement destinés à la surveillance des débris, mais qui pourraient avoir une fonction d'espionnage.

---

84 Brian G. Chow, "Stalkers in Space: Defeating the Threat", *Strategic Studies Quarterly*, Summer 2017, p. 82.

85 Tate Nurkin, *China's Advanced Weapon Systems*, *op. cit.*, p. 137.

86 Brian Weeden, Victoria Samson, *Global Counterspace Capabilities: An Open Source Assessment,* [2018] *op. cit.*, p. x.

87 Brian Weeden, Victoria Samson, *Global Counterspace Capabilities: An Open Source Assessment,* [2019] *op. cit.*, p. 1-7.

Un autre système, le **Aolong-1** (« *Roaming dragon* ») lancé en juin 2016, est doté d'un bras robotisé afin de récupérer des débris spatiaux et les faire brûler dans l'atmosphère[88].

Par ailleurs, d'autres éléments peuvent servir à développer des capacités offensives dans l'espace, comme le satellite relais, Queqiao placé en mai 2018 « *sur une position stratégiquement importante au-dessus de la face cachée de la lune* ». Officiellement, il doit y effectuer des missions d'étude des ondes gravitationnelles mais selon un expert du NASIC, « *Queqiao pourrait potentiellement servir de relais à un vaisseau ou arme orbitant autour de la lune* [afin de] *frapper les satellites militaires américains en orbite géosynchrone* »[89].

➧ Guerre électronique

Les moyens de guerre électronique peuvent être intégrés au domaine *counterspace* dans la mesure où ils permettent de dégrader certaines fonctions opérées par les satellites :

- Brouillage des communications ;
- Interférence avec les systèmes de PNT ;
- Brouillage des systèmes de détection radar.

Selon la DIA, « *la Russie a mis en service une large gamme de systèmes terrestres de guerre électronique pour brouiller le GPS, les communications tactiques, les satellites de communication et les radars* »[90].

Figure n° 13 : SYSTÈMES RUSSES DE GUERRE ÉLECTRONIQUE À CAPACITÉ ANTI-SPATIALE

	Caractéristiques	Aptitudes counterspace
Systèmes visant les satellites		
Krasukha-4S	Brouilleur de puissance antiradar aéroporté opérant en bande X/Ku. Portée jusqu'à 300 km. Peut-être dix systèmes en service dans les brigades de GE de district, délivré sur la période 2013-2015.[91]	Permettrait de neutraliser ; les satellites radar en LEO[92].
Systèmes visant le segment utilisateur		
R-330Zh - Zhitel	Brouilleur de puissance UHF dotant les compagnies de guerre électronique de brigade de manœuvre	Dédié au brouillage des réceptions SATCOM bande étroite des forces tactiques et signaux GPS

[88] Tate Nurkin, *China's Advanced Weapon Systems*, *op. cit.*, p. 144.

[89] Patrick Tucker, "China's Moon Missions Could Threaten U.S. Satellites: Pentagon," *Nextgov*, October 17, 2018. https://www.nextgov.com/emerging-tech/2018/10/chinas-moon-missions-could-threaten-us-satellites-pentagon/152096/

[90] Defense Intelligence Agency, *Challenges to Security in Space*, *op. cit.*, p. 28.

[91] Jonas Kjellén, *Russian Electronic Warfare*, FOI / Swedish Defence Research Agency, September 2018, p. 54. https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--4625--SE

[92] *Ibid.*, p. 53.

Tirada-2S	Brouilleur SATCOM. Peu d'information. Système opérationnel uniquement depuis 2019. Détecté en Ukraine par l'OSCE conjointement avec un R-330Zh[93].	Présenté comme un système de « destruction » de satellite[94]. Peut-être dédié à la neutralisation du segment de liaisons SATCOM des drones

Alors que « *la Russie dispose d'une multitude de systèmes capables de brouiller les récepteurs GPS localement* », elle « *n'a pas de capacité connue d'interférer avec les satellites eux-mêmes par brouillage radio* (EM) »[95].

3.3 Développements américains et vulnérabilités chinoises et russes

Face à la multiplication des risques (naturels ou accidentels) et menaces, les États-Unis cherchent à préserver leur *« liberté d'opérer dans l'espace »* (selon la *National Space Strategy* de 2017) et plus particulièrement la sécurité de leurs activités spatiales (ce que la doctrine interarmées qualifie de « *space mission assurance* »). Cela implique de maintenir une « supériorité spatiale » (*Space superiority)*, définie comme :

> *« the degree of control in space of one force over any others that permits the conduct of its operations at a given time and place without prohibitive interference from terrestrial and space-based threats"*[96].

Ainsi, même si la stratégie spatiale globale est défensive, elle combine des éléments visant à la préservation des capacités et des éléments offensifs, comparables à ceux des puissances rivales.

3.3.1 Les mesures défensives américaines

Apparu en 2014 dans la *Strategic Portfolio Review*, l'objectif de garantir la continuité des opérations spatiales (*Assured Space Operations*) a été précisé en 2015, dans le *DoD Space Mission Assurance Framework*[97], puis inscrit dans la doctrine interarmées. Elle en décrit les trois composantes principales[98] :

- Les opérations défensives, qui incluent des mesures de protection passive et active (détection et alerte, aptitude à la manœuvre évasive), mais aussi des actions visant à « neutraliser » les menaces « imminentes » ;

---

[93] « Как опознать новейшую российскую систему орбитального подавления "Тирада-2" на Донбассе », Inform Napalm, 01.05.2019, https://informnapalm.org/46754-kak-opoznat-novejshuyu-rossijskuyu-sis/

[94] Yaroslav Pravdolyubov, « Complex EW "Triad 2C" », Anna News, 10.29.2018, http://anna-news.info/kompleks-reb-triada-2s/?fbclid=IwAR1JvUQwQl_kPtpeWdROF6dUvXSGh0ykaK86K5pEkM28UByBEEz-0XJMvJA

[95] Brian Weeden, Victoria Samson, *Global Counterspace Capabilities: An Open Source Assessment,* [2018] *op. cit.,* p. 2-21.

[96] Joint Publication 3-14, *Space Operations*, Joint Chiefs of Staff, US Department of Defense, April 2018, p. I-3.

[97] Theresa Hitchens, Joan Johnson-Freese, *Toward a New National Security Space Strategy: Time for a Strategic Rebalancing*, *op. cit.,* p. 38.

[98] Joint Publication 3-14, *Space Operations*, *op. cit*., pp. I-7, I-8.

- L'aptitude à la reconstitution des capacités, qui vise à restaurer une fonction après un acte de dégradation ;
- La résilience des systèmes, passant par la désagrégation, la distribution, la diversification, la protection, la redondance et la déception.

De nombreux programmes ont été lancés pour mettre en œuvre ces différentes mesures.

Figure n° 14 : EXEMPLES DE MESURES DE RÉSILIENCE AMÉRICAINE

Reconstitution des capacités	
Aptitude au lancement rapide	En 2018 la DARPA a lancé le "*Launch Challenge*"[99], pour expérimenter les possibilités de lancement sur court préavis de petits satellites en orbite basse. Trois concurrents ont été sélectionnés en avril 2019 pour un essai en 2020. La DARPA poursuit également avec Boeing le programme *Experimental Spaceplane*, véhicule hypersonique capable de placer une charge en orbite basse, avec quelques heures de préavis.
Développement de micro-satellites (moins de 300 kg) qui peuvent être lancés rapidement et à moindre coût pour remplacer des systèmes neutralisés	L'*Army* a expérimenté en 2017-2018 un démonstrateur de satellite d'imagerie de 50kg (*"Kestrel Eye"*), dans l'optique de constituer une constellation[100]. Dans le domaine des SATCOM : programme de Nanosatellites (SNaP, 5,5 kg) de l'*Army Space and Missile Defense Command* (2013).
Désagrégation	
Répartition des différentes fonctions sur différentes plateformes	La nouvelle génération de SATCOM sépare les fonctions : - AEHF stratégiques : programme *Evolved Strategic SATCOM* (ESS) ; - AEHF tactiques : *Protected Tactical SATCOM* (PTS)
Diversification	
Multiplication des moyens différents pour accomplir une mission.	Programme DARPA Micro-PNT, de capteurs inertiels miniaturisés pour compenser la perte de signal GPS. SATCOM : l'*Army* développe des systèmes terrestres : *High-band Networking Waveform* (HNW) ; *Mid-tier Networking Vehicular Radio* (MNVR)[101].

[99] Jeff Foust, "DARPA and the future of space", *The Space Review*, September 10, 2018.

[100] Jeffrey L. Caton, *Impacts of Anti-Access/Area Denial Measures on Space Systems: Issues and Implications for Army and Joint Forces*, *op. cit.*, p. 30.

[101] Mais leurs performances lors des expérimentations sont insuffisantes. Major Andrew H. Boyd, *Satellite and Ground Communication Systems: Space and Electronic Warfare Threats to the United States Army*, The Land Warfare Papers, n°115, Arlington, AUSA, November 2017, p. 10.

Recours aux services spatiaux commerciaux	En juin 2018, le DoD a passé un contrat avec SES *Government Solutions* pour l'utilisation de sa constellation SATCOM O3b (20 satellites en MEO) jusqu'en 2023.
Distribution	
Répartition des capacités pour remplir une fonction sur plusieurs éléments	Programme *Blackjack* (2018) de la DARPA pour démontrer la possibilité de remplacer de gros satellites militaires géostationnaires par des constellations de petits satellites (60 à 200 unités), basés sur une plateforme commerciale standardisée[102]. Architecture théorique envisagée par la *Space Development Agency*
Redondance	
Multiplication des capacités destinées à remplir une même mission	Programme de *l'Air Force Research Laboratory* : lancement en 2022 d'une constellation de satellites (NTS-3) en orbite géosynchrone, pour compléter les GPS en MEO[103].
Protection	
Amélioration de la manœuvrabilité des satellites[104]	
Protection des liaisons de données	PNT : Développement du signal GPS sécurisé *M-Code.* SATCOM : Programme *Enterprise Management and Control* (EM&C) destiné à assurer la continuité des communications par recherche automatique des satellites accessibles[105].

3.3.2 Les capacités offensives

Durant la Guerre froide, les États-Unis avaient de multiples programmes dans tous les domaines du *counterspace*. Mais dans la préface du rapport du CSIS sur la menace, le sénateur Jim Cooper (fervent promoteur de la création de la *Space Force*) déplore que "*The United States is not the leader in anti-satellite technology*"[106]. Ils disposent toutefois, comme leurs rivaux, de toute la gamme de capacités potentiellement offensives.

---

[102] Léo Barnier, « Airbus rafle la mise avec le Blackjack de la Darpa », *Le Journal de l'Aviation*, 16.01.2019.

[103] Sandra Erwin, « *Air Force* experiment NTS-3 could point the way to the next generation of GPS », *Space News*, March 16, 2019. https://spacenews.com/air-force-experiment-nts-3-could-point-the-way-to-the-next-generation-of-gps/

[104] Patrick Tucker, "Pentagon Wants Satellites That Can Dodge Incoming Fire", *NextGov*, February 25, 2019. https://www.nextgov.com/emerging-tech/2019/02/pentagon-wants-satellites-can-dodge-incoming-fire/155111/

[105] Dr. Mark Dale, « DoD's Automated Satellite Roaming: How the technology protects against denial of satellite services », *MilSat Magazine*, March 2019.

[106] Jim Cooper, "Foreword", in Todd Harrison, Kaitlyn Johnson, Thomas G. Roberts, *Space Threat Assessment 2019*, *op. cit.*, p. iv.

➧ Capacités d'attaque cinétique depuis la Terre

Les systèmes de défense anti-missile balistique constituent des moyens ASAT potentiels et un rapport de 2016 de l'*Atlantic Council* soulignait qu'il était « *plus facile de viser un satellite avec un intercepteur anti-missile* […] *que de frapper un missile balistique* »[107]. Les différents systèmes déployés ou expérimentés par les États-Unis ont tous la capacité d'attendre les engins en orbite basse :

- En 2008, lors de l'Opération *Burnt Frost* un intercepteur SM-3 Block IA, tiré depuis le croiseur Aegis *USS Lake Erie,* a détruit un satellite de reconnaissance à une altitude de 240 km. Cette portée est trop limitée pour avoir une véritable utilité en ASAT.
- Mais la nouvelle version, SM-3 Block IIA, développée avec le Japon, pourrait atteindre une altitude entre 1.450 and 2.350 km[108], menaçant la plupart des satellites opérant en orbite basse.

➧ Capacités non-cinétiques depuis la Terre

Dans le domaine de la guerre électronique, les États-Unis disposent depuis 2004, du ***Counter Communications System*** (CCS). Il s'agit de plateformes mobiles destinées à brouiller le signal montant vers les satellites de communication en orbite géostationnaire pour dégrader le C2 adverse. 2 premières unités ont été déployées en 2014 et plus d'une dizaine sont actuellement en service, au sein de la *21st Space Wing* (*4th Space Control Squadron*, Peterson AFB).

➧ Capacités d'attaque co-orbitale

Bien qu'il n'y ait pas officiellement de programme à vocation offensive, les États-Unis ont procédé à de multiples expérimentations de suivi, localisation et interception d'engins en orbite[109], ainsi qu'à des manœuvres de rendez-vous et proximité[110] :

- En orbite basse :
  - En 2003 avec le **XSS-10**, satellite expérimental de l'USAF ;
  - En 2005 avec l'*Experimental Satellite System 11* (**XSS-11**), microsatellite de 100 kg produit par Lockheed Martin pour l'*Air Force Research Laboratory* ;
  - Avec le **DART** (*Demonstrator of Autonomous RendezvousTechnologies*) de la NASA, expérimenté en 2005, mais dont la mission a échoué[111] ;

---

[107] Theresa Hitchens, Joan Johnson-Freese, *Toward a New National Security Space Strategy: Time for a Strategic Re-balancing*, *op. cit*., p. 43.

[108] Bohumil Dobos, Jakub Prazak, "To Clear or to Eliminate? Active Debris Removal Systems as Antisatellite Weapons", *Space Policy*, n°47, February 2019, p. 219.

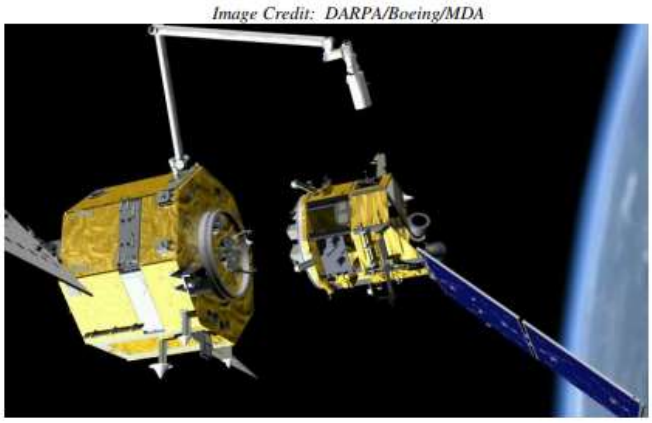
[109] Ils ont notamment effectué une interception en orbite en septembre 1986 lors de l'expérimentation Delta 180 dans le cadre de l'Initiative de Défense Stratégique.

[110] Brian Weeden, Victoria Samson, *Global Counterspace Capabilities: An Open Source Assessment,* [2018] op. cit., p. 3-2.

[111] Plusieurs dysfonctionnements ont entrainé une collision avec le satellite de rendez-vous. https://directory.eoportal.org/web/eoportal/satellite-missions/d/dart

- De mars à juillet 2007, avec le satellite ASTRO, lors de l'**Orbital Express mission** de la DARPA, qui expérimentait la première capture d'un objet spatial par un bras robotisé.

Figure n° 15 : VÉHICULE SPATIAL ASTRO



- En orbite géosynchrone :
  - Par les satellites ***Micro-satellite Technology Experiment*** (MiTEx), lancés en 2006 et passés à proximité d'un satellite d'alerte avancée défectueux fin 2009 ;
  - Par le ***Geostationary Space Situational Awareness Program*** de l'USAF, déployant des paires de satellites en 2014 et 2016.

Il faut également mentionner le programme de véhicule orbital **X-37B**, initié par la NASA en 1999, qui relève de la DARPA depuis 2004. Il s'agit d'une « navette » entièrement robotisée, lancée par une fusée, qui peut rester en orbite plusieurs années (à une altitude de 285 à 400 km) et rentrer ensuite dans l'atmosphère en planant pour atterrir. Le véhicule a été testé en 2010, 2011 (il a passé 469 jours dans l'espace), en 2012 et 2015 (718 jours dans l'espace)[112]. Les opérations sont menées par le *3rd Space Experimentation Squadron* (Schriever AFB)[113].

Ses missions sont peu claires, mais la navette :

- Pourrait emporter des capteurs pour des missions de télédétection ;
- Ou peut offrir une capacité de déploiement rapide de plusieurs petits satellites (*Operationally Responsive Space*).

Outre les capacités de manœuvre, les États-Unis expérimentent des systèmes potentiellement capables d'endommager des satellites. Pour développer l'aptitude à contrôler et réparer des satellites à haute altitude, la DARPA a notamment lancé en 2019 un appel d'offre pour un programme qui devrait durer environ 5 ans. Le projet *Robotic Servicing of Geosynchronous Satellites* prévoit le développement à la fois de systèmes robotisés pour

[112] Tate Nurkin, *China's Advanced Weapon Systems*, *op. cit.*, p. 146.

[113] Brian Weeden, *X-37B Orbital Test Vehicle Fact Sheet*, Secure World Foundation, June 2017. https://swfound.org/media/205879/swf_x-37b_otv_fact_sheet.pdf

opérer sur les satellites et de véhicules spatiaux capables de les placer en orbite. Une fois déployés ils pourraient procéder à des inspections périodiques et des réparations si nécessaire[114].

Dans le domaine des engins d'élimination des débris, la DARPA a commencé en 2012 le programme ***Phoenix***[115], visant à récupérer sur des satellites hors service en GEO, les antennes encore fonctionnelles pour les implanter sur d'autres systèmes. Le programme est entré dans sa deuxième phase en 2014, concernant notamment le développement de la partie robotique.

3.4 Conclusion

Le gain opérationnel que les forces chinoises pourraient tirer d'une attaque contre-spatiale « *s'avère a priori limité. Ceci pour les raisons suivantes :*

- *L'attaque par la Chine d'une constellation américaine (ISR, GPS, ou satellites de communication) ne générerait que des bénéfices très limités. Les fonctions militaires des satellites américains sont réparties entre de très grandes constellations dotées de redondances destinées à prévenir ce genre d'imprévus. Ces constellations demeurent donc opérationnelles, même après la perte d'un satellite. De plus, certaines fonctions de ces satellites sont redoublées par des systèmes terrestres et aériens (AWACS, E-8A JSTARS) ;*
- *Il faudrait que la Chine lance une attaque massive (plus de dix satellites visés) pour pouvoir tirer des bénéfices tactiques (à court terme) d'une telle opération* »[116].

Cette analyse de Jaganath Sankaran se trouve confortée par les projets de nouvelle architecture actuellement en cours de conception par la DARPA et la nouvelle *Space Development Agency*. Ces dernières envisagent ainsi plusieurs constellations de plusieurs centaines de minisatellites en orbite basse et médiane incluant par exemple une couche SATCOM (*Space Transpotation Layer*), une couche Tracking (reprenant le projet de *Space Sensor Layer* et fondée sur le programma Blackjack de la DARPA). Cependant, il est a noté que l'USAF est en désaccord avec ces projets de la SDA, préférant combiner ce type de constellations et celles de systèmes plus robustes (comme OPIR ou les SATCOM EHF) et que le Congrès a demandé, selon son habitude, des clarifications sur les missions de chacun avant de financer ces programmes[117].

---

[114] Jack Corrigan, "The Pentagon is Investing in Space Robots to Repair Satellites", *op. cit.*

[115] Joan Johnson-Freese, "Taking Out the Space Trash; A Model for Space Cooperation", *Breaking Defense*, May 2, 2014.

[116] Analyse de Jaganath Sankaran, "Limits of the Chinese Antisatellite Threat to the United States", *Strategic Studies Quarterly*, vol. 8, n°4, hiver 2014, p.19-46. Reprise in : Florence Gaillard-Sborowski, Isabelle Facon, Xavier Pasco, Isabelle Sourbès-Verger, Philippe Achilleas, *Sécuriser l'espace extra-atmosphérique : éléments pour une diplomatie spatiale à l'horizon 2030*, *op. cit.,* p. 178.

[117] Valerie Insinna, « House appropriators put pressure on the Space Development Agency in FY20 funding proposal », *Defense News*, May 14, 2019, https://www.defensenews.com/space/2019/05/14/house-appropriators-put-some-pressure-on-the-space-development-agency-in-fy20-funding-proposal/

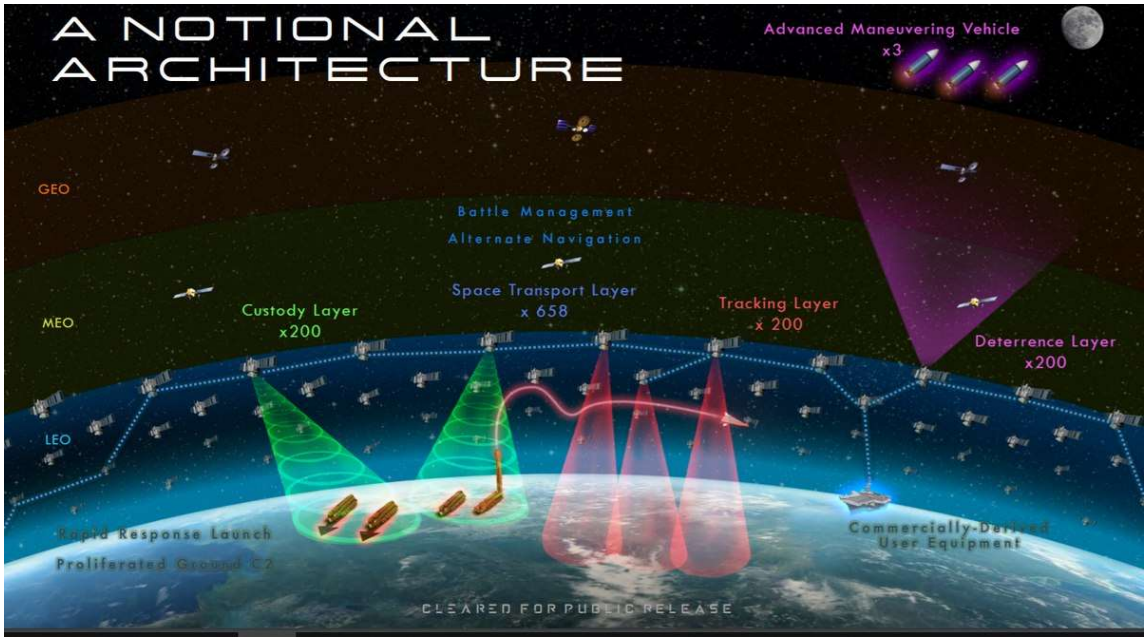


Figure n° 16 : VISION DE L'ARCHITECTURE SPATIALE AMÉRICAINE FUTURE PRÉSENTÉE PAR LA *SPACE DEVELOPMENT AGENCY*

Quoi qu'il en soit, les Américains s'acheminent comme envisagé vers des capacités dont la désagrégation et la redondance garantissent un niveau de résilience largement supérieur à celui qui existe actuellement. Les capacités offensives, cinétiques et électroniques, chinoises et russes seraient donc probablement en mesure d'entraver certaines fonctions, notamment les capacités ISR souveraines les plus rares et les moins « distribuables », comme les satellites ROEM, mais elles ne seraient probablement pas en mesure d'interdire aux Américains l'exploitation de l'ensemble de leurs capacités spatiales ISR et SATCOM, ce d'autant que le recours à des interceptions cinétiques en LEO auraient des conséquences catastrophiques pour elles aussi. La création de la SSF suggère cependant l'usage massif de la LIO contre les architectures américaines, dont la portée reste évidemment très incertaine mais peut s'avérer plus disruptive encore.

Dans la situation inverse, la Chine entend elle aussi mettre sur pied des architectures SATCOM LEO, comme la constellation Hongyan de 300 satellites, ce qui tend à montrer que le niveau de résilience de Pékin. La situation se pose cependant de façon différente. En effet, dans des engagements proches leurs atterrages, les forces chinoises et russes seraient probablement beaucoup moins dépendantes de leur SATCOM que les Américains. Les moyens ISR en revanche, comme au temps de la guerre froide, seraient déterminants pour cibler les groupes navals américains. On peut donc penser que les Américains destineraient leurs capacités de *counterspace* offensives à des constellations comme les Yaogan SAR/EO/ELINT…que Pékin renforce de façon régulière.

1. L'intelligence artificielle

1.1 Apport de la technologie

La quête de l'Intelligence artificielle (IA) est aussi ancienne que l'informatique elle-même. Elle a été marquée depuis soixante ans par une succession de périodes d'espoir et de déception. Cependant, son décollage contemporain date du début de la présente décennie. Elle est généralement associée aux seuils atteints par la puissance de calcul des ordinateurs dans le contexte de la fameuse loi de Moore et d'autres progrès comme la gestion de la mémoire. Cette notion d'IA apparaît malaisée à définir. Entre cent autres, on retiendra ici une, celle de Marvin Lee Minsky, l'un des pères de la discipline : « *la construction de programmes informatiques qui s'adonnent à des tâches qui sont, pour l'instant, accomplies de façon plus satisfaisante par des êtres humains car elles demandent des processus mentaux de haut niveau tels que : l'apprentissage perceptuel, l'organisation de la mémoire et le raisonnement critique* »[118]. L'IA se manifeste par une grande variété de solutions.

L'IA procède historiquement de deux principales logiques : l'IA « symbolique » qui consiste à faire effectuer à la machine un raisonnement logique en déclinant des concepts et l'IA « connexionniste » qui consiste, de façon plus *bottom-up*, à faire émerger la réponse à un problème par agencement de mécanismes élémentaires, connectés à la façon des neurones du cerveau humain. C'est cette dernière approche qui est massivement mise en œuvre actuellement. Elle procède de « l'apprentissage machine » qui consiste à faire reconnaître à l'ordinateur un objet en réduisant progressivement son taux d'erreurs par la masse des exemples traités. « L'apprentissage profond », reposant sur des réseaux de neurones de plus en plus compliqués, est une évolution de l'apprentissage machine.

Dans le domaine stratégique, plus qu'une réelle rupture, on prête à l'IA dans le futur la capacité à représenter un accélérateur capacitaire phénoménal, que l'on catégorise ainsi :

- Les solutions de reconnaissance de forme (langage, images, vidéos, sons) et de classification semi-automatisée de données massives structurées ou non-structurées démultiplient et accélèrent les capacités d'analyse. Ces applications, qui représentent la seule solution pour traiter des flux d'imagerie devenus ingérables par les interprètes photos, révolutionnent déjà le ROIM et le GEOINT. Elles sont aussi une

[118] https://www.ukonline.be/cours/cshistory/characters/marvin-minsky

réalité en ce qui concerne l'analyse prédictive dans le domaine du MCO et le deviendront progressivement pour les autres fonctions opérationnelles consommatrices de ces données : typiquement, les autres aspects du soutien ou de l'exploitation toutes sources du renseignement.

- L'IA permet de reproduire également des environnements et donc de démultiplier les capacités de simulation et de modélisation.
- Les capacités de raisonnement automatisé doivent contribuer à l'optimisation de la prise de décision, par exemple en identifiant les anomalies dans une situation (procédés classiques des déclinaisons de la *situational awareness* dans les différents domaines de lutte), en proposant des analyses prédictives en fonction des *patterns* identifiés, ce qui permet d'améliorer les options de modes d'action, en planification comme conduite mais aussi, le cas échéant, d'automatiser certaines tâches de réactions. Ce champ du raisonnement s'appliquera bien entendu en première étape à de nombreuses tâches spécifiques : monitoring de mouvements, guerre électronique, etc.
- Enfin, en intégrant ces différentes technologies au sein des plateformes, l'IA constituera le cerveau des systèmes autonomes (drones navals et aériens, robots terrestres, spatiaux) en facilitant le *manned-unmanned teaming* puis en assurant l'autonomie plus ou moins grande de leurs opérations, individuelles ou collectives (essaim, etc.)

L'IA permet donc fondamentalement trois choses : l'exploitation optimale des « big data », l'accélération de la prise de décision et la diffusion des systèmes de plus en plus autonomes, l'une des seules manières de retrouver de la masse, qui est aussi une préoccupation des compétiteurs stratégiques.

On n'en est cependant qu'aux prémices de cette révolution. Plusieurs obstacles sont encore à franchir :

- Tout d'abord la lourdeur des solutions actuelles d'apprentissage machine. Elles nécessitent sur le plan organique encore beaucoup de temps et de ressources. Des techniques permettent cependant de réduire cette contrainte de supervision, comme les *Generative adversarial networks* (GANs), soit un apprentissage semi-supervisé permettant à deux machines d'apprendre réciproquement. Ensuite, elles nécessitent des bases d'apprentissage extrêmement lourdes (les milliers d'exemples mentionnés) qui ne sont pas toujours disponibles.
- Le phénomène de « boite noire », l'incapacité de la machine à expliquer son résultat, un obstacle à la confiance que l'opérateur peut lui accorder. La DARPA entend ainsi dépasser cette limite avec *Explainable IA* (voir ci-dessous) ;
- L'acceptation, sous les angles normatif et éthique, de l'autonomie des systèmes ;

- Enfin la polyvalence. Les solutions d'IA développées actuellement répondent à des problèmes spécifiques. Les réseaux de neurones doivent être conçus, ou modifiés profondément s'ils proviennent d'une autre application, en fonction des spécificités du besoin et de l'information traitées. Associée à la question de la disponibilité des bases d'apprentissage, il peut s'agir d'un problème sur le plan militaire, lequel recèle de domaines d'application particuliers, très éloignés de ceux traités massivement dans la logique commerciale des GAFAM (*Google*, *Apple*, *Facebook*, *Amazon* et *Microsoft*). Le caractère dual des technologies trouve ici une limite. L'enjeu majeur est donc de parvenir à réaliser des solutions d'IA généralistes en mesure de régler de multiples problèmes très différents, un horizon très lointain que certains situent entre 2040 et 2060.

1.2 Un « match » principalement sino-américain

Alors que de nombreux États ont fait de l'Intelligence artificielle l'une des priorités de leurs politiques technologiques et industrielles[119], certains experts considèrent que deux acteurs se distinguent clairement par leurs capacités et les moyens qu'ils engagent actuellement pour les renforcer : les États-Unis et la Chine[120]. La « course mondiale » à l'IA serait donc stimulée par un « duel » entre ces deux pays. Leurs autorités politiques entretiennent d'ailleurs cette perception, les discours publics sur l'Intelligence artificielle étant très souvent fondés sur l'idée d'un affrontement entre les deux nations. Certains responsables américains lancent ainsi des alertes, affirmant que la Chine est en train de rattraper les États-Unis et qu'il convient donc de renforcer les actions publiques dans ce domaine[121].

1.3 Forces et faiblesses des écosystèmes nationaux chinois et américain

La position dominante des États-Unis et de la Chine s'explique avant tout par la puissance et la complétude de leurs écosystèmes. Selon de nombreux observateurs, parmi les 6 pôles en IA les plus puissants au monde, 5 sont américains ou chinois. Cette cartographie illustre le phénomène :

---

[119] En 2017 et 2018, le Canada, la Chine, les Émirats arabes unis, la Finlande, la France, la Suède, la Corée du Sud, le Mexique, l'Inde et l'Allemagne ont par exemple publié des stratégies nationales dédiées à l'Intelligence artificielle.

[120] Voir par exemple Horowitz (M.), Kania (E. B.), Allen (G. C.), Scharre (P.), *Strategic Competition in an Era of Artificial Intelligence*, Center for a New American Security, July 2018.

[121] Voir par exemple Long (H.), « In Davos, U.S. executives warn that China is winning the AI race », *The Washington Post*, January 23 2019.

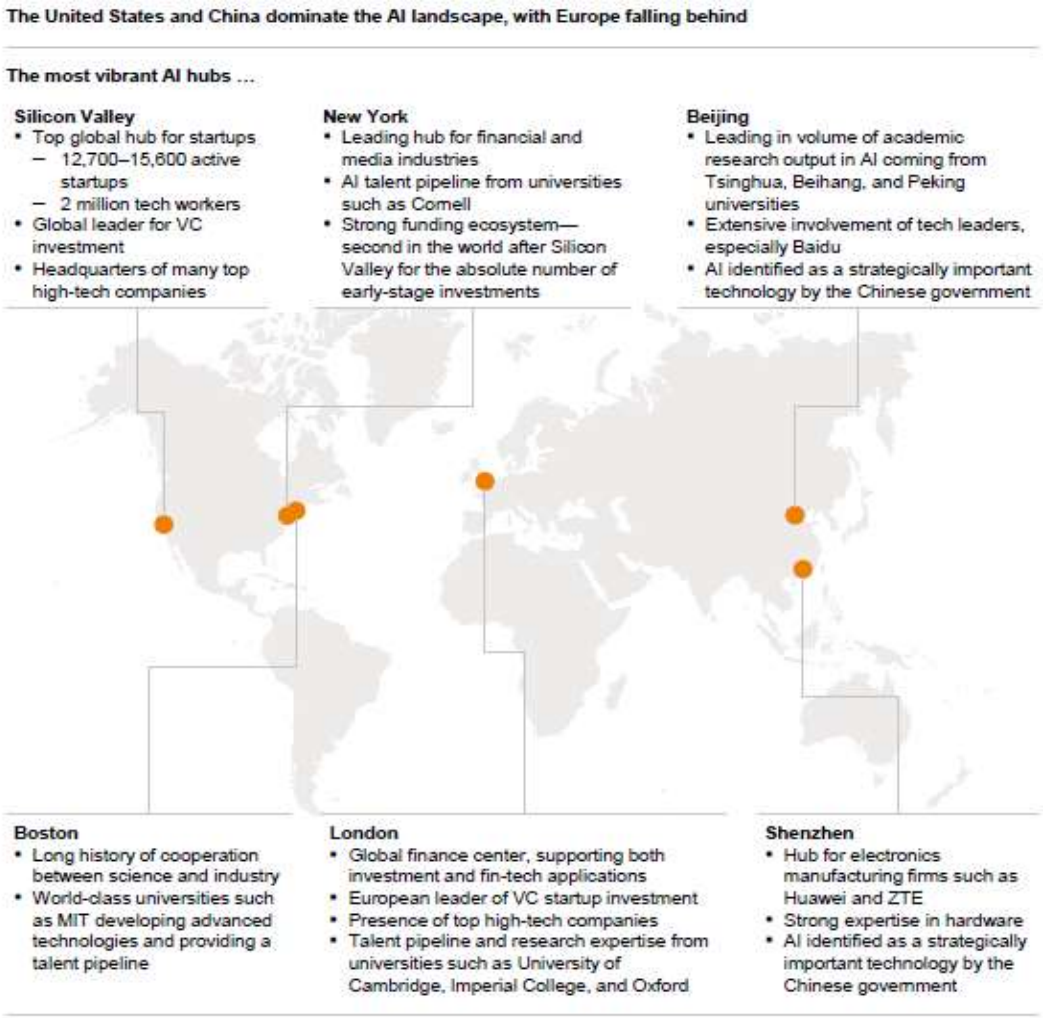


Figure n° 17 : LES GRANDS ÉCOSYSTÈMES MONDIAUX EN MATIÈRE D'IA[122]

1.3.1 États-Unis

Les États-Unis bénéficient de trois écosystèmes de très haut niveau en matière d'IA (en plus d'autres de moindre importance) : Boston, New-York et la baie de San Francisco.

1.3.1.1 Soutien des autorités

L'avance américaine s'explique notamment par la précocité de l'intérêt porté, par les administrations, aux techniques d'IA. Dès les années 1960, le Pentagone, en particulier l'*Advanced Research Projects Agency* (créée en 1958), a financé des travaux réalisés par les premiers laboratoires universitaires concernés et quelques entreprises pionnières (dont IBM)[123].

[122] Source : McKinsey Global Institute (2017

[123] Une partie des budgets du programme *Command & Control*, lancé en 1962, fut notamment attribuée aux recherches en IA (en particulier celles du MIT).

Plus récemment, les autorités américaines ont clairement manifesté leur volonté de renforcer les écosystèmes nationaux de l'IA. Différents exercices de réflexion ont été menés concernant les apports potentiels de l'Intelligence artificielle pour le pays. Les premiers documents généraux d'orientation politique ont été publiés à la fin de la Présidence Obama[124]. Ces documents ont notamment servi à poser des recommandations en matière de recherche, de régulation et de politiques publiques de soutien.

En mai 2018, la Maison Blanche a organisé un sommet national sur l'IA. Cet événement a permis de rassembler des représentants de l'industrie, du monde académique et des administrations. À cette occasion, Michael Kratsios, *Deputy Assistant to the President for Technology Policy*, a précisé l'approche développée par l'Administration Trump : maintenir l'avance américaine en matière d'IA ; soutenir les travailleurs américains ; alimenter la R&D publique ; faire disparaître les barrières à l'innovation. La création d'un *Interagency Select Committee on Artificial Intelligence* a également été annoncée. Rattaché au *National Science and Technology Council*, il est composé de responsables politico-administratifs de haut niveau en charge des politiques de R&D[125]. Sa fonction est de fournir des expertises à la Maison Blanche sur les priorités générales en matière de recherche et développement. Il s'agit par ailleurs d'une structure de coordination interministérielle et interagences ayant aussi pour mission d'aligner les priorités des agences et Départements en matière de R&D et de vérifier la bonne exécution des planifications budgétaires fédérales.

1.3.1.2 Facteurs expliquant la puissance des écosystèmes américains

En dehors de la précocité de l'intérêt national pour la discipline, d'autres facteurs expliquent l'avance américaine. Tout d'abord, il faut rappeler que l'IA se situe au cœur de l'activité des GAFAM (*Google*, *Apple*, *Facebook*, *Amazon* et *Microsoft*). Tous ont des programmes lourds de R&D depuis maintenant de nombreuses années. *IBM*, *Intel*, *Yahoo*, *Saleforces*, *SAS*… en disposent également[126]. La plupart de ces grands groupes ont développé un intérêt précoce pour les techniques d'apprentissage automatique[127]. Certaines de ces entreprises ont par ailleurs accès à des bases de données colossales pour entraîner leurs solutions.

---

[124] Le rapport *Preparing for the Future of Artificial Intelligence* et le *National Artificial Intelligence Research and Development Strategic Plan* ont notamment permis, en octobre 2016, au *National Science and Technology Council* de proposer une description des tendances de la R&D et de discuter des implications sociales et techniques pour un certain nombre de concepts (justice, responsabilité, sûreté et sécurité).

[125] Le directeur du *National Institute for Standards and Technology*, l'*Under Secretary for research and engineering* du DoD, l'*Under Secretary for science* du Département de l'Énergie, le directeur de la *National Science Foundation*, les directeurs de la DARPA et de l'IARPA…

[126] Dès 2006, *IBM* s'était par exemple engagé à financer à hauteur de 3 milliards de dollars (US) son *Watson cognitive computing service*, afin qu'il devienne un acteur incontournable du développement de l'Internet des objets.

[127] Elles les utilisent depuis relativement longtemps pour filtrer les contenus indésirables sur internet, ordonner des réponses à une recherche sur leurs moteurs, faire des recommandations ou sélectionner des informations intéressantes et personnalisées pour chaque utilisateur…

Par ailleurs, les États-Unis bénéficient de certaines des structures de formation (académiques et en ingénierie) parmi les plus performantes au monde (*Carnegie Mellon*, MIT, *Stanford*, *Berkeley*…). Ces organismes permettent au pays de disposer des plus vastes capacités à former des talents[128], ainsi que de la recherche la plus dynamique dans nombre des champs de l'IA. En avril 2018, *Synced* estimait ainsi que, sur les 1,9 millions d'ingénieurs spécialistes en Intelligence artificielle dans le monde, environ un million travaillait aux États-Unis[129].

Les écosystèmes américains sont par ailleurs constitués d'un très grand nombre de PME, dont certaines très innovantes. En 2017, selon le *Tencent Research Institute*, les entreprises (toutes tailles et secteurs d'activité confondus) développant des systèmes utilisant de l'IA étaient ainsi encore deux fois plus nombreuses aux États-Unis qu'en Chine.

La puissance américaine tient également au fait que les soutiens financiers se sont structurés bien plus rapidement que dans les autres pays. Le pays dispose ainsi de sociétés de capital-risque, de *Business angels* et de fonds d'amorçage spécialisés dans les nouvelles technologies qui ont intégré depuis quelques années déjà l'IA à leurs portefeuilles. Leurs apports viennent compléter les financements publics et les différents types d'interventions des GAFAM, *IBM*, *Intel* et *Yahoo*[130]. Certaines fondations spécialisées, comme *OpenAi*, créée par Elon Musk, sont également des financeurs et apportent des aides aux *start-ups* (incubation, formation des dirigeants à l'entreprenariat…).

---

[128] En novembre 2017, le *Tencent Research Institute* a publié un rapport sur la génération des talents en IA. L'institut a ainsi recensé les organismes d'enseignement supérieur (écoles et universités) ayant développé à cette époque un ou plusieurs cursus dédiés à l'IA. Sur les 367 établissements identifiés, 168 étaient situées aux États-Unis.

Pour une recension de ce rapport, voir Chen (C.), « China's AI dreams stymied by shortage of talent, with the US home to lion's share of experts », *South China Morning Post*, 1 December 2017.

[129] Ces chiffres ne prenaient en compte que les ingénieurs en titre, et donc pas les docteurs et les spécialistes n'ayant pas le titre d'ingénieur (mathématiciens et statisticiens par exemple).

[130] Parmi ces différents types d'actions, existe notamment le débauchage des talents étrangers et le rachat de PME non américaines. Les groupes américains ont ainsi absorbé de nombreuses *start-ups* britanniques, israéliennes, indiennes et canadiennes. Depuis le début des années 2010, cette méthode semble être leur principale voie de développement externe. Les fusions-acquisitions ont parfois été utilisées comme méthode pour faire signer aux talents créateurs des PME absorbées des contrats de travail (pratique appelée l'« *acqui-hiring* »). Les grands groupes américains ont par ailleurs multiplié les partenariats avec des organismes de recherche et de formation non-américains et se sont implantés dans les *hubs* étrangers.

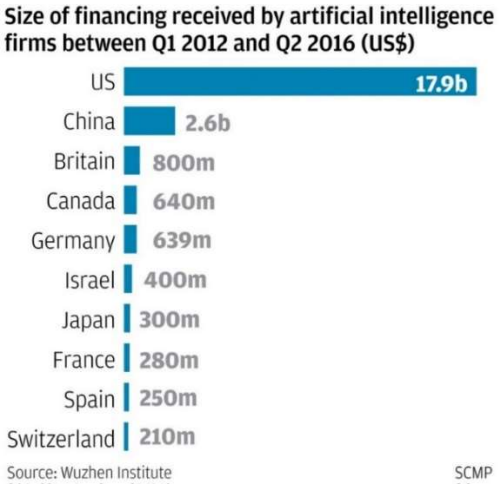


Figure n° 18 : MONTANT DES FINANCEMENTS REÇUS PAR LES ENTREPRISES D'IA PAR PAYS ENTRE 2012 ET 2017

Comme le montre ce graphique, les investissements, publics comme privés, américains ont donc été bien plus rapides à abonder que dans les autres pays.

Les États-Unis disposent ainsi de marchés bénéficiant d'une certaine maturité. Les applications de l'IA sont déjà employées dans de nombreux secteurs d'activités économiques (banque/finance/assurance, instruments médicaux…) et les réseaux de distribution de ces solutions sont structurés.

Enfin, les principales entreprises mondiales qui fournissent des micro-processeurs sont américaines. Certains acteurs nationaux se sont même lancés dans la course au développement de processeurs dédiés. Le pays possède aussi des sociétés *leaders* dans la fourniture de *data centers*. Il dispose des infrastructures et des productions de matériels pour asseoir le développement de l'IA.

1.3.2 Chine

1.3.2.1 Intégration du développement de l'IA aux stratégies économiques nationales

Depuis quelques décennies, la Chine cherche à modifier son modèle économique. Différentes réformes et plans ont ainsi eu pour fonction de renouveler les moteurs de la croissance, qui reposait essentiellement sur une main d'œuvre « bon marché » nombreuse et sur le transfert et l'imitation de technologies développées à l'étranger. Désormais, le pays veut devenir une puissance industrielle dotée de capacités d'innovation (une « *superpuissance scientifique et technologique* » – 科技强国)[131]. L'Intelligence artificielle fait pleinement partie de cette dynamique. Différentes initiatives de promotion des sciences

[131] Cheung (T. M.), Mahnken (T.), Seligsohn (D.), Pollpeter (K.), Anderson (E.), Fan (Y.), *Planning for Innovation: Understanding China's Plans for Technological, Energy, Industrial, and Defense Development*, U.S.-China Economic and Security Review Commission, 2016.

et technologies ont ainsi été lancées ces dernières années, dont quelques-unes portant spécifiquement sur l'IA.

Parmi les différentes initiatives, le *Next Generation AI Development Plan* (新一代人工智能发展规划), publié en juillet 2017, constitue un socle en matière de promotion de l'IA. Le Plan définit l'Intelligence artificielle comme une technologie stratégique, enjeu d'une compétition internationale. Il s'agit donc pour le pays d'obtenir un statut de *leader* mondial dans son développement.

Février 2006	State Council	*National Medium- and Long-Term Plan for the Development of Science and Technology* (2006-2020)
Avril 2012	State Council	*12th Five- Year Plan for Intelligent Smart Manufacturing*
Mai 2015	State Council (MIIT)	*Made in China 2025*
Avril 2016	National Development and Reform Commission	*Robotics Industry Development Plan* (2016-2020)
Mai 2016	National Development and Reform Commission	*« Internet Plus » Artificial Intelligence Three-Year Action Implementation Plan*
Aout 2016	State Council	*13th Five-Year Plan on National Science and Technology Innovation*
Décembre 2016	State Council	*13th Five-Year Plan for Developing Strategic and Emerging Industries*
Juillet 2017	State Council (MoST et MOE)	*Next Generation Artificial Intelligence Development Plan*
Aout 2017	MoST et CMC	*13th Five-Year Science and Technology Military-Civil Integration Special Plan*
Aout 2017	National Natural Science Foundation of China	*Guidelines on AI Basic Research Urgent Management Projects*
Novembre 2017	National Development and Reform Commission	*China Artificial Intelligence Industry Innovation Alliance*
Décembre 2017	MIIT	*Three-Year Action Plan to Promote the Development of Next-Generation Artificial Intelligence Industry]*
Janvier 2018	Chinese Academy of Engineering	*Artificial Intelligence 2.0 Plan*

1.3.2.2 Forces et faiblesses des écosystèmes chinois

Depuis 2016, les investissements chinois, publics comme privés, ont connu une croissance rapide. À partir de 2017, les efforts financiers nationaux ont même été plus importants que ceux des États-Unis[132]. Ces financements ne bénéficient pas qu'aux BAT (*Baidu*, *Alibaba*, *Tencent*) et à *Xiaomi*, mais également au vivier de PME en cours de constitution (voir ci-après). Ils servent notamment à la R&D. Les grands groupes chinois ont par ailleurs cherché à nouer des liens avec l'étranger, sous des formes très différentes (rachats d'entreprises étrangères, y compris américaines, prises de capital, établissement de partenariats avec des organismes de recherche et d'enseignement supérieur et implantation dans des *hubs* étrangers…), copiant assez largement les méthodes de leurs concurrents américains.

[132] L'État central n'est pas le seul à apporter des aides publiques, en particulier des financements. Début 2018, 12 provinces chinoises avaient développé des actions dédiées, de même que de grandes métropoles (Beijing, Shanghai, Hangzhou…). Il s'agit souvent d'exonérations de taxes et de la fourniture de locaux dans des parcs scientifiques et technologiques.

Les écosystèmes chinois ne se limitent pas aux grands groupes que constituent les BATX. Le pays fait preuve d'un très grand dynamisme entrepreneurial[133], qui a permis l'émergence de *start-ups leaders* au niveau mondial dans leur domaine (comme *Yitu Tech*, vainqueur du *Facial Recognition Prize Challenge* de l'IARPA en 2017). Les programmes d'aides gouvernementales incluent désormais quasi-systématiquement des volets spécifiques pour les PME.

Une des spécificités des entreprises chinoises en lien avec l'intelligence artificielle, et plus spécifiquement celle appliquée à la robotique est qu'elles sont pour la plupart des entreprises privées, des géants mais aussi beaucoup de *start-ups* créées à la fin des années 2000 ou au début des années 2010, soit près de vingt ans après les industries de robotique d'Etat. Ceci est un changement majeur en termes de tissu industriel chinois puisque les fleurons industriels chinois étaient jusqu'à présent quasi-uniquement des entreprises d'Etat. Notons que le Ministère des sciences et des technologies (MOST) a choisi cinq entreprises chinoises pour diriger le développement de plates-formes nationales d'innovation ouverte à l'IA dans ce qui est appelé une « équipe nationale » (国家队) : Baidu (conduite autonome), Alibaba (villes intelligentes), Tencent (imagerie médicale), iFLYTEK (voix intelligente) et SenseTime (vision intelligente). Ces entreprises ne semblent avoir aucun problème de financement, ce qui souligne du point de vue des marchés financiers, leur très fort potentiel. Au-delà des financements publics, les financements sur les marchés sont extrêmement importants, à travers les principales levées de fonds des licornes et *start-up* chinoises d'IA appliquée à la robotique. La plupart sont en lien soit avec la conduite autonome (Geek+, Yihang.ai, Roadstar.ai ou encore Pony.ai), les robots de service (UBTech, Rokid, Aiqi Tech ou ForwardX) ou la vision intelligente (SenseTime, Yitu Technology ou NASN). Parmi les dix entreprises de robotique et d'IA les mieux financées au monde en 2018, on note d'ailleurs quatre entreprises chinoises, contre cinq américaines et une britannique.

Les entreprises chinoises, en particulier les grands groupes, ont accès à des bases de données, notamment publiques, qui permettent d'entraîner les dispositifs fondés sur des traitements statistiques. Le pays bénéficie par exemple des plus grandes communautés d'utilisateurs de *smart phones* et d'abonnés à des réseaux sociaux, alors que les normes en matière de protection des données à caractère personnel restent faibles.

Les autorités chinoises ont décidé de faciliter les démarches administratives pour accueillir des étudiants et des chercheurs étrangers sur le territoire national. Elles ont aussi cherché à attirer des entreprises et à débaucher des spécialistes de haut niveau. La stratégie nationale repose également sur une politique de publication scientifique très agressive. Depuis 2014, les scientifiques chinois, de plus en plus présents dans les conférences

[133] En 2017, certains experts estimaient que 50 % des PME en IA créées au cours de l'année étaient chinoises.

internationales, sont ceux qui publient le plus sur le *deep learning* et les réseaux neuronaux. En parallèle, les acteurs chinois se sont organisés pour peser sur les mécanismes internationaux de normalisation.

En application des plans et feuilles de route, différents organismes de coordination ont été créés (dont le *New Generation AI Development Plan Promotion Office* et une *New Generation AI Strategic Advisory Commission*). De même, des « équipes nationales » ont été mises en place : les autorités ont nommé certains acteurs nationaux majeurs pour qu'ils soient responsables du développement, dans des domaines particuliers (*smart cities*, imagerie médicale, voitures autonomes…), de projets applicatifs pris en charge par des consortiums. Des parcs technologiques dédiés sont également en cours de constitution. Des fonds d'investissement, en particulier public-privé, ont vu le jour.

La Chine a ainsi développé de véritables capacités en algorithmie, dans des champs particuliers (reconnaissances faciale et vocale, voiture autonome, voire même outils d'analyse prédictive[134]) la plaçant peut-être en tête de l'innovation mondiale. Compte tenu des facteurs qui précèdent, la Chine excelle, plus encore que les États-Unis, à la fabrication et à la commercialisation d'innombrables solutions à base d'IA, une masse qui contribue en retour à sa capacité d'innovation[135].

Le développement en matière d'IA connaît toutefois de sérieuses limites. Tout d'abord, la main d'œuvre hautement qualifiée manque. De même, de nombreuses *start-ups* sont encore très jeunes et il est fort probable que la plupart ne parviendront pas à survivre plus de quelques années. Ensuite, la recherche théorique semble trop faible. Ainsi, les logiciels de base de l'apprentissage machine sont encore tous américains. Contrairement à ce qui se passe dans la téléphonie mobile, la Chine accuse un retard certain dans l'élaboration des standards techniques de l'IA. Le pays connaît également des faiblesses dans les domaines des semi-conducteurs et des processeurs spécialisés, généralement conçus aux États-Unis et fabriqués en Corée du Sud ou à Taiwan[136]. Plus globalement, la Chine manque de grands programmes privés, qui pourraient structurer le développement des capacités nationales. À court terme, les marchés domestiques ne permettront probablement pas que des projets à forte rentabilité émergent. Enfin, dans de nombreux domaines, les acteurs chinois n'innovent pas véritablement, mais continuent de capter les technologies étrangères et les adaptent.

---

[134] Entretien avec un ingénieur en informatique, chef de projet ayant recours à beaucoup d'IA

[135] Kai-Fu Lee, « What China Can Teach the U.S. About Artificial Intelligence : Visionary research is no longer the most important element of progress », *The New York Times*, Sept. 22, 2018

[136] Gregory C. Allen, *Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security*, Center for a New American Security, February 2019

1.4 Développement de l'IA de défense

1.4.1 États-Unis

1.4.1.1 Structuration des efforts américains

L'Intelligence artificielle est l'un des éléments clés de la *Third Offset Strategy*, qui vise notamment à renforcer les capacités d'innovation de la Défense américaine et à accélérer les cycles de développement et d'acquisition des matériels. De très nombreux *services* et organisations du DoD portent ainsi un intérêt au développement et à l'utilisation d'équipements intégrant de l'IA. Portant, jusque 2019, il n'existait pas véritablement de stratégie coordonnée pour l'ensemble du *Department*, alors même que de multiples programmes étaient en cours de réalisation. Lors de l'hiver 2017, le constat de ce manque s'est imposé, notamment lors de la rédaction de la *National Defense Strategy*. En mars 2018, dans une présentation devant une commission parlementaire, Mary Miller, *acting Assistant Secretary of Defense for research and engineering*, annonçait qu'une rationalisation des efforts internes au DoD en matière d'IA allait être menée. Différentes actions ont ainsi été mises en œuvre.

Tout d'abord, l'*Interagency Select Committee on Artificial Intelligence* a été organisé, en juin 2018, en deux sous-comités. L'un d'eux est un groupe de travail qui doit notamment gérer le programme NITRD[137]. Au même moment, le projet de loi de finance 2019 pour la Défense a intégré plusieurs dispositions concernant l'Intelligence artificielle[138]. Un haut responsable en charge de la coordination des activités internes au DoD de développement et de démonstration des systèmes recourant à l'IA a été nommé[139]. Une Commission de sécurité nationale sur l'Intelligence artificielle (« *AI Commission* ») a aussi été fondée. Organisme de conseil indépendant rattaché au pouvoir exécutif, sa principale mission est de réaliser une revue, accompagnée de recommandations pour le Congrès et les administrations. Enfin, la création du *Joint Artificial Intelligence Center* a été confirmée par le NDAA. Son action doit compléter celle du Coordinateur : le *Center* a en effet été

[137] Ce programme est le principal outil de financement fédéral sur les technologies de l'information avancées. Indépendant des outils de financement dont disposent les Départements et Agences, il sert à soutenir des projets de R&D et des actions permettant d'accélérer le transfert de la recherche vers la phase commerciale dans les domaines de l'informatique, des réseaux et des logiciels.

[138] Ce projet a été adopté par les parlementaires et est devenu un *National Defense Authorization Act* (NDAA) en août. Le texte pose comme objectif global au DoD de développer, améliorer et convertir les technologies de l'IA en vue d'emplois opérationnels.

[139] Entre autres fonctions, ce coordinateur doit élaborer une feuille de route stratégique visant à l'identification et à la coordination des technologies de l'IA et des capacités critiques indispensables pour les soutenir. Par ailleurs, il a la charge de produire une évaluation continue des capacités en IA développées par le DoD, mais également à l'extérieur (comme au sein de la DARPA).

instauré pour aider et superviser, sur le plan technique, les actions des différents *services* du DoD gérant des programmes de développement d'outils recourant à l'IA[140].

Le financement de la R&D en IA a largement progressé ces dernières années. Le Pentagone a consacré en 2017, 2,4 Mds$ à ces technologies soit :

- 1,1 Mds$ pour le développement et l'acquisition de systèmes d'IA, principalement des systèmes de réalité virtuelle et de visualisation, par exemple pour le GEOINT) ;
- 800 M$ pour la R&D des technologies d'IA (modélisation et simulation, apprentissage machine et apprentissage profond, traitement du langage, data mining) ;
- Le reste en R&D sur le calcul avancé[141].

1.4.1.2 Capacités et fonctions investiguées

En avril 2018, Michael Griffin, *Under Secretary for research and engineering*, a reconnu devant une commission parlementaire que 592 projets séparés impliquant de l'IA étaient en cours de réalisation au sein du DoD. Il n'a pas précisé si ce chiffre intégrait les programmes de la DARPA. Le spectre d'applications sur lequel les efforts américains se sont déployés semble donc être très vaste. Les paragraphes suivants ne donnent que quelques exemples.

En février 2019, le DoD a annoncé qu'une *Defense Artificial Intelligence Strategy* avait été rédigée. Le document n'a toutefois pas été rendu public. Seul un résumé, de 17 pages, a été publié. Cette synthèse rappelle que l'objectif du DoD est bien d'accélérer la livraison de prototypes et démonstrateurs dans les mois à venir. Il précise en effet que l'incorporation des dispositifs d'IA – si elle doit reposer sur des processus itératifs – doit être plus rapide. Pour ce faire, la logique est de disposer d'un socle commun (articulé autour du Coordinateur et du *Joint Artificial Intelligence Center*), mais de laisser les initiatives décentralisées en matière de développement et d'expérimentation s'épanouirent.

Si le document indique que l'IA peut être développée pour toutes les fonctions et domaines, il cite quelques objectifs particuliers : *Improving situational awarness and decision making* ; *Increasing safety of operating equipment* ; *Implementing predictive maintenance and supply* ; *Streamlining business processes*. Il semble donc que, dans un premier temps, les fonctions logistiques et de soutien doivent être celles qui vont être plus particulièrement investiguées.

---

[140] Plus précisément, le *Joint Artificial Intelligence Center* a pour mission d'accélérer la livraison de capacités recourant à l'IA et de coordonner les différents organismes et services concernés par l'Intelligence artificielle au sein du *Department* (notamment de synchroniser les programmes qu'ils lancent).

[141] *Department of Defense, Artificial Intelligence, Big Data And Cloud Taxonomy*, Govini Report, https://fr.calameo.com/read/0000097792ddb787a9198

➡ Cyber-opérations (notamment cyber-protection) :

L'IARPA est devenue, depuis sa création en 2006, l'un des principaux acteurs américains finançant les activités de recherche en IA. Parmi les programmes qu'elle a initiés, le *Cyberattack Automated Unconventional Sensor Environment* (CAUSE), lancé en 2015, avait par exemple pour objectif le développement de méthodes automatisées et auto-apprenantes de prédiction et de détection extrêmement précoce des cyberattaques. Peu d'informations ont filtré sur les travaux menés dans le cadre de ce programme, qui s'est terminé en mars 2019. L'une des équipes financées a toutefois révélé à la revue *Forbes* qu'elle avait été chargée d'améliorer un outil, *OmniSense*, de *monitoring* global et permanent d'Internet[142]. Des « serveurs d'écoute » ont été répartis partout dans le monde, analysant le trafic et cherchant à attacher les adresses IP à certaines actions particulières (comme celle de voler des mots de passe en masse).

La DARPA a, pour sa part, lancé des programmes de création de dispositifs recourant au *machine learning* pour détecter les écarts à l'activité normale de réseaux[143].

Les actions dans le domaine cyber prennent d'autres formes que des programmes de R&D. La DARPA a notamment organisé le *Cyber Grand Challenge*. L'une des fonctions de l'événement était de stimuler les acteurs du cyber pour qu'ils travaillent au développement de systèmes automatisés et autonomes capables de surveiller, détecter et réparer les failles de sécurité des réseaux informatiques[144]. En 2016, une équipe de la *Carnegie Mellon University* a par exemple remporté le challenge avec MAYHEM, dispositif qui découvre, confirme et corrige les failles des logiciels et leurs vulnérabilités en temps réel[145].

L'Agence s'est même positionnée comme l'autorité fournissant les jeux de données pour le développement et l'expérimentation de ces solutions. Elle a surtout réussi à faire de ses critères d'évaluation des performances des standards dans ce domaine.

➡ Renseignement :

Dès le début des années 2010, la DARPA a lancé des programmes pour aider les analystes à exploiter de grands volumes de textes. Il s'agissait d'intégrer des solutions de *big data*. Bien que les données concernées utilisassent les mêmes types de formats, elles

---

[142] Brewster (T.), « Omnisens: U.S. Intelligence-Backed Startup Claims It Can Predict Cyberattacks Days Before They Happen », *Forbes*, March 29, 2019.

[143] Allen (G.), Chan (T.), *Artificial Intelligence and National Security*, Belfer Center for Science and International Affairs, Belfer Center Study, July 2017, p. 19.

L'intérêt de ces outils intelligents est qu'ils ne fonctionnent pas à partir d'indicateurs et de seuils prédéfinis pour caractériser l'activité courante d'un réseau. Auto-apprenants, ils doivent être capables d'intégrer les variations normales d'intensité pour éviter de lancer des fausses alarmes.

Cet intérêt de la DARPA est en réalité assez ancien. Les premières actions datent du début des années 2000. Voir Michael (C.), Ghosh (A.), « Simple state-based approaches to program-based anomaly detection », *ACM Transactions on Information and System Security* (TISSEC), 2002.

[144] Le Challenge était organisé lors de la conférence en cyber-sécurité *Defcon*.

[145] Coldewey (D.), « Carnegie Mellon's MAYHEM AI takes home $2 million from DARPA's Cyber Grand Challenge », TecCrunch.com, August 5, 2016.

pouvaient être déstructurées. Le programme *Deep Exploration and Filtering of Text* (DEFT) devait notamment permettre de développer des solutions capables d'identifier et d'interpréter les informations à la fois explicites et implicites dans des textes descriptifs vagues et ambigus. Ce projet de 4 ans et demi, débuté en 2012, a permis de progresser dans la création de technologies capables de convertir des informations contenues dans les textes en représentations structurées alternatives[146].

De même, le programme *Low Resource Languages for Emergent Incidents* (LORELEI) avait aussi pour fonction de développer des modèles devant convertir des *inputs* déstructurés en *outputs* structurés exploitables par les analystes. Il a plus spécifiquement investigué les méthodes de réponse rapide à des situations émergentes (comme l'assistance après un désastre) à partir de ressources limitées. Le système a été développé pour disposer de fonctions initiales de reconnaissance de langage (notamment pour les sources audio et vidéo) et de traduction, devant permettre de fournir une connaissance de la situation en identifiant les éléments d'information les plus pertinents, en anglais et en langue étrangère.

➡ Reconnaissance, détection, identification et ciblage :

En 2015, les systèmes de reconnaissance d'image développés par *Google* et *Microsoft* sont parvenus à dépasser les concurrents humains lors d'un challenge dédié (l'*ImageNet challenge*)[147]. Ces dispositifs, fondés pour la plupart sur des techniques de *Machine learning*, ont été adaptés par les agences de renseignement américaines pour l'analyse des images de reconnaissance satellitaire[148].

Au niveau tactique, l'IA a déjà été identifiée comme une voie d'amélioration pour les systèmes de détection, d'identification et de ciblage. La DARPA a lancé, dans la première moitié des années 2010, un programme de recherche intitulé *Target Recognition and Adaptation in Contested Environments* (TRACE) visant au développement de systèmes de reconnaissance de cibles précis en temps réel et peu consommateurs d'un point de vue énergétique. L'objectif est que des dispositifs de reconnaissance automatique de cibles (*automatic target recognition* – ATR) puissent être combinés aux systèmes radar existants, afin de fournir des capacités de ciblage de longue distance pour la surveillance aérienne vers le sol[149]. Pour que cette capacité soit véritablement utile, il faut cependant qu'elle

---

[146] « DARPA prepares artificial intelligence system for understanding language », Dataconomy, May 5, 2014.

[147] Johnson (R. C.), « Microsoft, Google Beat Humans at Image Recognition », EE Times, February 2015.

[148] Simonite (T.), « Why Amazon and the CIA want algorithms to understand satelitte photos », *MIT Technology Review,* August 25, 2016.

[149] Les radars permettent en principe d'opérer des identifications et l'engagement de cibles au sol pour les aéronefs à des distances de sécurité. Ces fonctions sont cependant réalisées au prix de nombreuses fausses alarmes et du risque de générer des dommages collatéraux.

Sur les objectifs du programme TRACE, voir Keller (J.), « DARPA TRACE Program Using Advanced Algorithms, Embedded Computing for Radar Target Recognition », *Military & Aerospace Electronics*, July 24, 2015.

offre de faibles taux de fausses alertes, dans des environnements pourtant complexes. Surtout, elle doit pouvoir apprendre par elle-même avec des données d'entraînement limitées et différentes[150]. Dans ce cadre, la *start-up Deep Learning Analytics* a, par exemple, développé un prototype d'ATR. Ce système a même été testé lors d'exercices au cours desquels il a été employé comme aide au repérage et à l'engagement de cibles[151].

En avril 2017, le Secrétaire adjoint à la Défense Robert Work a annoncé le lancement d'un projet ambitieux, MAVEN, pris par en charge par une *Algorithmic Warfare Cross-Functional Team*[152]. Dans ce cadre, le DoD a, au début de l'année 2017, contracté avec une filiale de *Google*, la société *ECS Federal*, pour le développement de dispositifs d'aide au ciblage pour les frappes opérées par des drones[153], utilisant des outils de *deep learning* pour la traduction et la reconnaissance visuelle. Ce travail vise à développer des systèmes capables d'aider les analystes image à interpréter les très nombreuses données générées par les capteurs de la flotte américaine de drones[154].

➧ Préparation des déploiements :

La préparation au déploiement peut concerner les personnels responsables de l'entretien des matériels. Certaines armées utilisent notamment des *Intelligent tutoring systems*. Il s'agit de logiciels qui fournissent des formations ou des instructions d'emploi de matériels (tutoriels), sans intervention d'un enseignant. L'*U.S. Air Force* recourt ainsi à un ITS nommé SHERLOCK pour ses techniciens aéronautiques, afin qu'ils puissent pratiquer des diagnostics des systèmes électriques des appareils. Avec les outils intelligents en développement, ces formations et enseignements pourraient être adaptés à l'apprenant et à son futur déploiement.

De même, des systèmes ont été développés pour favoriser l'insertion des personnels déployés au sein des populations. L'*Information Sciences Institute* de l'Université de Caroline du Sud a ainsi créé un programme d'entraînement, dans lequel l'apprenant, guidé par un avatar, prépare les personnels militaires allant être déployés à développer une communication appropriée dans l'environnement culturel au sein duquel la mission va prendre place[155]. Les dispositifs « intelligents » en cours de conception devraient pouvoir

---

[150] *Ibid.*

[151] Host (P.), « Deep Learning Analytics Develops DARPA Deep Machine Learning Prototype », *Defense Daily*, November 5, 2016.

[152] C'est cette équipe qui a été transformée en *Joint Artificial Intelligence Center.*

[153] Fang (L.), « Google is quietly providing AI technology ofr drone strike targeting project », *The Intercept*, March 6, 2018.

[154] Le DoD a officiellement annoncé que des outils intelligents avaient ainsi été employés par des analystes pour préparer des frappes contre *Daesh* au Moyen-Orient.

[155] Johnson (W. L.), Valente (A.), « Tactical Language and Culture Training Systems: Using Artificial Intelligence to Teach Foreign Languages and Cultures », *AI Magazine*, 30 (2), 2009.

recourir au RETEX (sous différentes formes) pour modifier d'eux-mêmes les informations transmises aux personnels et les situations simulées dans lesquelles les insérer virtuellement.

➡ Entraînement :

À l'été 2016, des combats aériens simulés ont été organisés, opposant un officier à la retraite de l'*U.S. Air Force* et un pilote de chasse artificiel « intelligent », ALPHA, développé par la société *Psibernetix*[156]. L'humain a été battu. La machine est en effet capable de traiter les données issues des capteurs et de planifier ses mouvements bien plus rapidement que le pilote humain. Ces essais ont été pratiqués en environnement simulé et donc contrôlé. De nombreux travaux seront donc encore nécessaires avant que ce type de systèmes soit véritablement utilisable dans des conditions opérationnelles.

➡ Aide à la décision (pendant les opérations) :

La DARPA et les *Services* investiguent cette fonction depuis maintenant de nombreuses années. Face à l'incertitude, au stress et au tempo particulièrement rapide imposé par les opérations militaires, les machines peuvent en effet produire des analyses situationnelles plus rationnelles, intégrant un plus grand nombre de variables, que les humains. La DARPA a ainsi financé les projets TIGER et MATE, qui ont permis de développer des algorithmes d'analyse en temps réel du champ de bataille pour le niveau tactique.

➡ Aide à la guerre électronique :

Au cours de la décennie, les armées américaines ont testé des dispositifs cognitifs renforçant certains équipements de guerre électronique[157]. Trois programmes proches ont ainsi été lancés ces dernières années, dont *Adaptive Radar Countermeasures* (ARC) et *Behavioral Learning for Adaptive Electronic Warfare* (BLADE). Il s'agit notamment de systèmes permettant de mieux caractériser les adversaires en temps réel et ainsi de générer des contremesures adaptées de manière autonome. ARC concerne par exemple les signaux radars nouveaux, inconnus et adaptatifs. Le programme BLADE sert au développement d'algorithmes de *machine learning* et de systèmes capables de détecter et caractériser rapidement de nouvelles menaces radio, afin de synthétiser de nouvelles contremesures.

1.4.1.3 La DARPA entend développer la troisième génération d'IA

Enfin, la DARPA a lancé un nouveau programme intitulé « *Explainable AI* » (XAI), qui ambitionne d'aboutir à une troisième génération de l'IA. Il s'agit en effet de dépasser les

[156] Reilly (M. B.), « Beyond video games: New artificial intelligence beats tactical experts in combat simulation », *University of Cincinnati Magazine*, June 27, 2016.

[157] Seffers (G. I.), « Smarter AI for Electronic Warfare », *Signal*, 17 November 2017.

actuelles technologies d'apprentissage machine fondées sur l'analyse statistique, qui restent des « boites noires » pour l'opérateur, et de développer sur la base de modèles contextuels, des outils en mesure d'expliquer leurs raisonnements aux opérateurs.

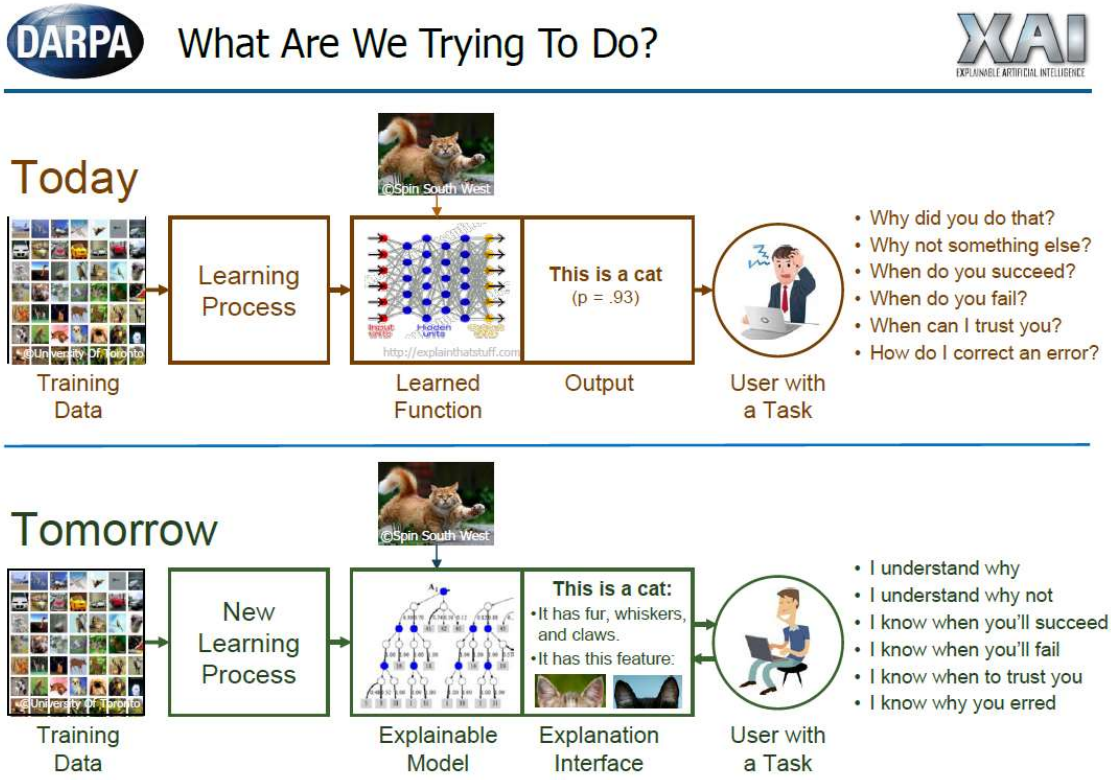


Figure n° 19 : PROJET D'*EXPLAINABLE AI* DE LA DARPA[158]

1.4.2 La Chine

La promotion de l'IA repose sur une approche *Top-down*. Même si les provinces et certaines métropoles soutiennent les acteurs présents sur leurs territoires, il s'agit bien d'une stratégie centralisée et planifiée. Le gouvernement définit et coordonne les efforts, met en place des politiques dédiées et investit massivement pour développer la R&D et améliorer la génération de talents. Cette stratégie repose essentiellement sur la promotion de la coopération entre les structures gouvernementales et les entreprises, en particulier les grands groupes. Ceux-ci doivent avoir un rôle d'entraînement pour toute l'économie du pays.

Dans les discours officiels et les plans, il existe une certaine focalisation sur les emplois industriels de l'IA[159]. Ils sont clairement définis comme un outil permettant de renforcer la compétitivité économique du pays. La convergence civilo-militaire est cependant au

[158] Source : https://www.darpa.mil/attachments/XAIProgramUpdate.pdf

[159] Notamment les applications pour les industries manufacturières.

cœur de la stratégie nationale. Les autorités considèrent que, pour développer les capacités de R&D et d'innovation nationales, les armées et les acteurs industriels – y compris ceux qui n'ont pas l'habitude de travailler avec la Défense – doivent se rapprocher, en particulier dans les secteurs de haute technologie. Dans les documents officiels, les expressions « *définition partagée des besoins technologiques* », « *construction commune* » des technologies et « *partage des ressources en innovation* » sont employées pour définir les principales composantes de cette convergence. L'IA a ainsi été identifiée comme l'une des technologies devant servir de test pour cette convergence.

Sur le plan technologique, l'IA appliquée à la défense devrait jouer sur les mêmes forces et faiblesses qu'évoquées précédemment. Il convient cependant d'ajouter un autre point de faiblesse potentiel de la Chine par rapport aux États-Unis, celui de la masse de données disponibles pour les apprentissages profond sur les applications militaires les plus pointues. Si la reconnaissance de forme ou encore la *situational awareness* peuvent se fonder sur les ressources sociétales ou économiques du marché intérieur, on peut penser que les Américains jouissent encore d'un avantage certain en termes de bases de données sur certains environnements opérationnels (comme par exemple le domaine sous-marin pour les applications de traitement des données acoustiques et d'aide à la décision en opérations ASM).

1.4.3 La Russie

Vladimir Poutine l'a résumé en 2017 en cette phrase déjà fameuse : « *celui qui deviendra le leader dans cette sphère deviendra le maître du monde* ». La Russie s'est donc lancée dans cette course. Cependant les investissements consacrés par Moscou sont estimés à 12,5 M$ par an, donc nettement inférieurs à ceux consacrés par les États-Unis et la Chine. De plus, « l'écosystème » russe en matière d'IA en est encore à ses balbutiements et aucun *hub* russe ne figure parmi les 20 premiers mondiaux (contrairement à Paris ou Londres par exemple)[160]. Il est toutefois espéré que les investissements privés augmentent à 500 M$ en 2020. Certaines initiatives publiques-privées ont déjà été lancées comme par exemple un projet de recherche en analyse de données sémantiques piloté par l'*United Instrument Making Corporation* et impliquant une trentaine d'institutions et entreprises. Une feuille de route était attendue pour le milieu de l'année 2019.

En l'état, il semble que les initiatives sont principalement publiques et pour beaucoup à finalité militaire. L'IA est l'un des 8 grands projets de la nouvelle technopole d'innovation militaire (MIT ERA) en cours de création à Anapa sur les côtes de la mer Noire[161]. Plusieurs systèmes d'armes seraient dotés de techniques d'IA, sans que l'on sache exactement quelle réalité algorithmique ce type de déclarations recouvre : SU-35, RB-109A

[160] Alina Polyakova, « Weapons of the weak: Russia and AI-driven asymmetric warfare », Brookings, November 15, 2018, https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/

[161] 'Sergey Sukhankin, « Special Outsider': Russia Joins the Race for Global Leadership in Artificial Intelligence », Eurasia Daily Monitor, Volume: 16, Issue: 35, March 13, 2019, https://jamestown.org/program/special-outsider-russia-joins-the-race-for-global-leadership-in-artificial-intelligence/

Bylina, système de C2 des capacités des brigades de guerre électronique de districts (incluant les Krasukha évoqués plus haut), futurs missiles de croisière de la *Tactical Missiles Corporation*. Les armées russes investissent également dans l'autonomisation : programme de « drones de combat autonome » lancé par Kalashnikov, swarming d'UAV[162], future programme Ratnik, équivalent du Félin français. Certains analystes estiment cependant que l'IA pourrait être particulièrement exploitée pour la guerre de l'information dont Moscou s'est fait une spécialité[163].

2. Les technologies quantiques

Les technologies quantiques offrent selon beaucoup le potentiel de rupture stratégique le plus important de l'ensemble des technologies considérées dans ce rapport. Comme dans le cas de l'IA, la course entre les États-Unis et la Chine est maintenant lancée[164]. Deux facteurs distinguent les deux domaines :

- Alors que l'IA relève surtout d'une capacité logicielle diffuse aux contours variables, le quantique désigne une famille bien cernée de technologies physiques aux concrétisations bien identifiables ;
- Alors que l'IA est déjà, à des degrés divers, présente dans nos systèmes, les technologies quantiques en sont encore au stade de la recherche fondamentale ou appliquée. Leur mise en œuvre opérationnelle est une question, au mieux, de moyen terme, au pire, est encore inenvisageable en l'état, même si les manifestations de la physique quantique, parfaitement déterminées, sont déjà prises en compte dans une multiplicité de réalisations (des lasers au nucléaire).

Comme dans le cas de l'IA, si les deux grandes puissances sont largement en avance sur les autres, elles ne sont cependant pas seules. Il convient ici de rappeler que les scientifiques européens ne sont pas encore distancés et l'UE a fait en 2017 du quantique un de ses trois projets « *flagship* », devant être financé à hauteur de 1Mds€ sur 10 ans[165].

---

[162] Samuel Bendett, « In AI, Russia Is Hustling to Catch Up », *Defense One*, April 4, 2018, https://www.defense-one.com/ideas/2018/04/russia-races-forward-ai-development/147178/

[163] Alina Polyakova, *op cit.*

[164] Voir de façon générale sur l'ensemble de cette section, le récent rapport du CNAS, très complet : Elsa B. Kania & John K. Costello, *Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership*, Center for New American Century, September 2018, 52 p.

[165] Olivier Ezratty, « L'Europe et le quantique », Opinions libres, 8 novembre 2018, https://www.oezratty.net/wordpress/2018/europe-et-quantique/

2.1 L'apport de ces technologies

2.1.1 Intrication et superposition

Les technologies quantiques désignent la pleine exploitation des principes de la physique quantique qui régissent la nature, le comportement et les interactions de la matière au niveau subatomique, et sont largement différents de ceux de la physique classique aux échelles supérieures. Il ne s'agit pas ici de décrire l'ensemble des bases de cette physique. On en rappellera simplement les éléments nécessaires à la compréhension des enjeux technologiques qui nous intéressent ici. On retiendra aussi deux de ses phénomènes clés, l'intrication et la superposition :

- **La superposition** : tant qu'elle n'a pas été mesurée, une onde-particule (électron, photon, etc.) est potentiellement dans tous les états d'énergie à la fois (position, polarisation, quantité de mouvement, etc.). C'est la fameuse image du chat de Schrödinger, à la fois mort et vivant dans sa boite. Toute mesure la « fige » en revanche dans un état particulier : c'est la « réduction de la fonction d'onde ». En revanche, la probabilité que l'onde-particule soit dans tel ou tel état est parfaitement maîtrisée. L'état de superposition est fragile : toute interférence extérieure mène à sa « décohérence », sa disparition et l'onde particule reste ensuite dans un seul état ;
- **L'intrication**. Deux ondes-particules émises en même temps, interagissant, vont partager le même état à distance. Si l'on mesure l'état d'une de ces ondes-particules, aboutissant ainsi à sa décohérence, on est certain à 100% que l'autre adopte le même état au même moment. Les deux éléments forment ainsi un système cohérent.

2.1.2 Les technologies quantiques exploitant ces propriétés

La physique quantique peut être exploitée par trois familles de technologies, les capteurs, les communications et le calcul. Une myriade de phénomènes et de solutions sont explorées par les scientifiques. On en évoquera ici que les plus connus.

2.1.2.1 Les capteurs.

La physique quantique permet de concevoir des capteurs nettement plus précis :

- **Le radar quantique** qui exploite l'intrication : un photon d'une paire intriquée est émis par un faisceau micro-ondes. L'autre est conservé par le radar, ce qui permet à ce dernier d'identifier le premier photon s'il est réfléchi par un objectif. Le niveau de précision est incomparablement meilleur que tout radar classique et permet de détecter les appareils furtifs, en théorie. L'intrication rend aussi inutile tout effort d'usurpation du signal par les contre-mesures électroniques.
- **Le « ghost imaging »** : un des photons d'une paire intriquée compose un faisceau « objet » pour détecter une cible dans un espace donné et est ensuite récupéré pour être corrélé avec l'autre photon constituant le faisceau de référence n'éclairant pas la zone cible. La différence d'intensité entre les deux faisceaux permet d'obtenir

l'image de l'objet à des émissions d'énergie nettement plus basse qu'avec un détecteur classique[166]. La technologie est expérimentée depuis les années 2000.

- La technologie quantique trouve également son utilité dans **la fonction PNT** (positionnement, navigation, timing). En effet, les technologies « d'atome froid » (dans lequel les atomes polarisés par laser sont extrêmement sensibles à la rotation du système) permettraient à des centrales inertielles d'atteindre en théorie des précisions de navigation et de timing supérieures à celle du GPS. Le principal défi réside ici dans le facteur SWAP de tels systèmes, encore confinés aux recherches de laboratoire.

2.1.2.2 Les communications.

L'intrication et la superposition des ondes-particules permettent en théorie des systèmes de communication à la sécurité infaillible car tout intervenant extérieur tentant de lire le message aboutit systématiquement à modifier l'état de l'onde-particule.

- **La « téléportation » quantique** est la technologie la plus mature : démontrée dès 1998 par plusieurs laboratoires, elle est testée désormais sur des distances de centaines de km par plusieurs centres de recherche. Il s'agit de générer des couples de photons intriqués dont un seul est communiqué et l'autre conservé. Ce dernier est lui-même intriqué par l'émetteur avec un autre photon porteur de l'information à communiquer. L'émetteur communique ensuite au récepteur comment mesurer son photon intriqué, ce qui permet de téléporter l'information sans transmission de contenu[167].
- L'autre technologie est celle de la **distribution de clé quantique (QKD)**, dont le premier protocole a été conçu en 1984 : les bits sont encodés avec des photons polarisés différemment. Une fois le message adressé, pour le lire, l'expéditeur partage avec son destinataire leurs bases de polarisation aboutissant, là où elles sont identiques, à la même décohérence donc la même clé[168].

Le problème est ici que le signal ne peut être répliqué ou amplifié, ce qui limite les distances de transmission par fibre optique. La liaison QKD Pékin-Shanghai de 1400 km nécessite ainsi par moins de 32 points de relais où il faut décoder, réencoder et réémettre le message. L'une des solutions serait d'utiliser des répétiteurs quantiques à base d'atomes froids artificiels en mesure de conserver les photons encodés (dits « atomes de Rydberg »)[169]. La communication quantique est également démontrée par SATCOM

---

[166] Dilano Saldin, « Viewpoint: Ghost Imaging with X Rays », Department of Physics, University of Wisconsin-Milwaukee, Milwaukee, *Physics*, 9, 103, September 7, 2016, https://physics.aps.org/articles/v9/103

[167] Dr. Henry Everitt, Physics Division, U.S. *Army* Research Office, *Nanoscience and Quantum Information Science in the Army*, présentation, 2001, http://www.niac.usra.edu/files/library/meetings/fellows/oct01/Everitt_oct01.pdf

[168] Pour une explication simple : David Louapré, « La communication quantique et le protocole BB84 », Science étonnante, 14 février 2019, https://sciencetonnante.wordpress.com/2019/02/14/bb84/

[169] « Axe communication quantiques », Science et ingénierie en région Ile-de-France pour les technologies quantiques, http://www.sirteq.org/axe-communications-quantiques/

mais les interférences notamment diurnes avec l'environnement resteraient encore un obstacle que la recherche est en train de surmonter[170]. De plus, des failles de sécurité ont été démontrées il y a dix ans environ, comme par exemple au niveau des photo-diodes utilisées pour capter les photons émis[171] ou encore en raison du taux d'erreur nécessairement toléré dans la transmission en raison de l'environnement…ou prétendu tel, qui permettrait tout de même à un *hacker* d'opérer[172].

2.1.2.3 Le calcul

Dans un microprocesseur classique, les opérations consistent à manipuler un nombre de bits, chacun étant à l'état 0 ou 1. Dans un ordinateur quantique, le « qubit » est dans un état de superposition, en même temps 0 et 1. Cela signifie que l'ordinateur quantique est en mesure de réaliser des calculs massifs en parallèle. Les applications sont nombreuses comme le traitement de masses de données sans commune mesure avec l'existant ou encore le déchiffrement.

Malheureusement, pour réaliser un ordinateur quantique, les ingénieurs doivent surmonter trois grands défis : « *1) disposer d'un grand nombre de qubit ; 2) parvenir à les combiner en des états intriqués* [un élément non affiché dans les annonces de records de qubit des grandes firmes] *; 3) maintenir la cohérence de ces états assez longtemps pour que les calculs puissent aller à leur terme* » comme l'explique Pascale Senellart-Mardon du CNRS[173]. Bon nombre de scientifiques estiment donc que parvenir à un réel ordinateur quantique est un objectif illusoire, même à plusieurs décennies. Des solutions intermédiaires, hybrides, semblent cependant murir. Par ailleurs, « *un ordinateur quantique fonctionnant sur un principe différent, ne remplacera pas un ordinateur classique mais il le complètera quand un problème sera hors de sa portée* »[174].

En outre, il existe des parades en matière de chiffrement car tout ne réside pas uniquement dans la puissance de calcul. Les algorithmes sont tout aussi fondamentaux. La plupart des systèmes de chiffrement à clé publique actuels (comme le RSA), reposent principalement sur deux piliers : la factorisation de nombres premiers et les « logarithmes discrets », ce que précisément peut résoudre l'algorithme de calcul quantique inventé par Peter Shor en 1994, un ingénieur d'ATT[175]. Il existe toutefois d'autres solutions de chiffrement immunes aux algorithmes quantiques, comme par exemple la clé symétrique

---

[170] Elsa B. Kania & John K. Costello, *op cit*, p.3

[171] Lars Lydersen, et alii, « Hacking commercial quantum cryptography systems by tailored bright illumination », *Arwiv*, Cornell University, Submitted on 26 Aug 2010 (v1), last revised 4 Mar 2011, https://arxiv.org/abs/1008.4593

[172] Emerging Technology from the arXiv, « Commercial Quantum Cryptography System Hacked », MIT Technology Review, May 17, 2010, https://www.technologyreview.com/s/418968/commercial-quantum-cryptography-system-hacked/

[173] Pascale Senellart-Mardon, « L'ordinateur quantique devient un enjeu politique », propos recueillis par François Savatier, *Pour la science*, n°500, juin 2019, p.39

[174] Ibidem

[175] Interagency Working Group on Quantum Information Science of the Subcommittee on Physical Sciences, *Advancing Quantum Information Science: National Challenges And Opportunities*, A Joint Report of The Committee on Science And Committee on Homeland And National Security of The National Science And Technology Council,July 2016, p.2, https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Quantum_Info_Sci_Report_2016_07_22%20final.pdf

(tel le standard AES de la NSA) à condition qu'elle soit renforcée, la clé publique reposant sur les « réseaux euclidiens » (*Lattice-Based*) qui recueille ainsi une attention renouvelée de la communauté scientifique ces dernières années, etc[176].

Name of Cryptographic Algorithm	Type	Purpose	Resilience against Quantum Computer	
AES-256	Symmetric Key	Encryption	Ok but larger key sizes needed	High level of confidence
SHA-256, SHA-3		Hash function	Ok but larger output needed	
Lattice-based (NTRU)	Public Key	Encryption; signature	Believed	Under investigation
Code-based (Mc Eliece)	Public Key	Encryption	Believed	
Multivariate polynomials	Public Key	Encryption; signature	Believed	
Supersingular elliptic curve isogenies (SIDH)		Encryption; possibly signature	Believed	
ECDSA, ECDH (Elliptic Curve Crypto)	Public Key	Signatures, Key exchange	No longer secure	
RSA	Public Key	Signatures, Key establishment	No Longer secure	
DSA (Finite Field Crypto)	Public Key	Signatures	No Longer secure	

Figure n° 20 : LA RÉSILIENCE DES CLÉS DE CHIFFREMENT FACE AU CALCUL QUANTIQUE[177]

Une autre raison qui rend la concrétisation de ces recherches incertaine est que si ces manifestations de la physique quantique sont parfaitement validées par de multiples expériences, les débats font encore rage pour expliquer le fonctionnement à l'origine de ces invariables constats. Par exemple, la superposition existe-t-elle réellement dans la nature où s'agit-il simplement d'une lacune de connaissance physique restant à combler ? Comment expliquer l'intrication ?

Les recherches correspondantes sont extrêmement variées et portent sur les solutions technologiques permettant de générer ces particules ayant ces propriétés, de maintenir leur état, de les manipuler, etc. Leur lecture pour le profane est donc d'une extraordinaire complexité.

2.2 Les avancées américaines

Aux États-Unis, le Pentagone, le *National Institute of Standards and Technology* et l'industrie œuvrent à la recherche fondamentale sur ces technologies depuis le milieu des années

[176] Olivier Ezratty, « Comprendre l'informatique quantique – cryptographie », *Opinions Libres*, Publié le 3 septembre 2018 et mis à jour le 27 septembre 2018, https://www.oezratty.net/wordpress/2018/comprendre-informatique-quantique-cryptographie/

[177] Source : Quantum-Safe Security Relevance for Central Banks, IDQ, présentation, June 2018, https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180718/Documents/O_Pfeiffer.pdf

90 mais ces recherches, jusqu'à une période récente, s'effectuaient à un train de sénateurs.

2.2.1 La recherche quantique dans les armées

Au sein des armées américaines, les laboratoires de recherche des trois *services* travaillent sur ces technologies. Au-delà des efforts de recherche fondamentale sur les priorités de la physique, leurs priorités vont surtout aux capteurs et aux communications, un peu moins au calcul.

2.2.1.1 L'Army

L'*Army Research Laboratory* se place actuellement en position de leadership sur plusieurs segments :

- Les capteurs quantiques. Le centre a par exemple réalisé des percées dans le domaine des capteurs à atome de Rydberg[178] ;
- L'encodage quantique (l'étude des phénomènes de cohérence/décohérence, la gestion du « bruit ») ;
- Il collabore activement avec les autres centres sur les communications quantiques (mais peu sur la distribution des clés quantiques)[179]. L'ARL a été l'un des pionniers dans le domaine de la téléportation quantique.

2.2.1.2 L'Air Force

L'*Air Force Research Laboratory* concentre depuis des années ses efforts sur :

- La communication quantique. Il vient par exemple d'expérimenter des communications diurnes en espace ouvert avec des optiques adaptatives[180]. Michael Hayduk, *chief of the computing and communications division* à l'AFRL n'entend pas « imiter » les Chinois dans le domaine unique des SATCOM (voir ci-dessous) mais développer un réseau non seulement spatial mais aussi aérien et terrestre[181].
- Les travaux relatifs au PNT à base d'atomes froids.

Cependant, l'*Air Force Scientific Advisory Board* a tempéré les ardeurs de beaucoup en 2015 en soulignant les défis évoqués plus haut sur plusieurs technologies. Il a recommandé que l'USAF se concentre sur la réalisation de systèmes de navigation reposant sur des centrales inertielles à atome froid, et d'horlogerie atomique pour améliorer la fonction

---

178 RDECOM Research Laboratory Public Affairs, « *Army* researchers make giant leap in quantum sensing », October 25, 2018, https://www.arl.*Army*.mil/www/default.cfm?article=3320

179 *Army* Research Laboratory, *S&T Campaign Plans 2015-2035*, p. 9, https://www.arl.*Army*.mil/www/pages/172/docs/ARL-S&T-Campaign-Plans-FINAL.pdf

180 88th Air Base Wing Public Affairs, « *Air Force* Research Laboratory demonstrates world's first daytime free-space quantum communication enabled by adaptive optics », May 23, 2019, https://www.afmc.af.mil/News/Article-Display/Article/1856558/air-force-research-laboratory-demonstrates-worlds-first-daytime-free-space-quan/

181 Sandra Erwin, « Pentagon sees quantum computing as key weapon for war in space », *Space News*, July 15, 2018, https://spacenews.com/pentagon-sees-quantum-computing-as-key-weapon-for-war-in-space/

timing des systèmes de communications, de ROEM et de guerre électronique. Ces systèmes devraient pouvoir atteindre un TRL 6 dans les 5 à 10 ans. En revanche, les scientifiques de l'USAF ne recommandaient pas d'investissement dans les autres technologies : la distribution de clés de chiffrement quantiques accroît selon eux la complexité des systèmes sans apporter de réelle plus-value au regard des techniques existantes. Ils n'estimaient pas non plus que les technologies de calcul quantique offrent des solutions réalistes pour résoudre les problèmes de calcul de l'USAF et ne recommandaient dans ce domaine qu'un investissement minimal dans le suivi des avancées via les centres de recherche[182]. Cependant, Michael Hayduk a expliqué que les investissements dans le domaine du calcul quantique se poursuivaient activement[183].

2.2.1.3 La DARPA

La DARPA a bien entendu depuis 15 ans multiplié les travaux en matière de technologies quantiques. Elle a été par exemple à l'origine de la première génération d'horlogeries atomiques et œuvre actuellement à la maturation de dispositif beaucoup plus stables, moins sensibles aux conditions extérieures ou à des horloges d'une précision largement supérieure en lien avec les ingénieurs du *National Institute of Standards and Technology* (NIST). L'agence se lance également dans le calcul quantique. Avec le programme *Optimization with Noisy Intermediate-Scale Quantum devices*, ONISQ, elle vise le développement de solutions hybrides de moyen terme combinant des dispositifs de calcul quantique de « taille intermédiaire » et des ordinateurs classiques, fondées sur un nouvel « algorithme quantique d'optimisation approximative » développé par le MIT qui permettrait des progrès immenses dans la résolution de problèmes d'optimisation par rapports aux ordinateurs classiques[184].

2.2.2 Les lourds investissements des grands du web et de l'informatique

Les grandes firmes américaines, *Google*, IBM et Intel, se sont largement engagées dans la course pour la réalisation du premier ordinateur qui leur permettrait d'asseoir une « suprématie quantique ». Ainsi, *Google* a annoncé en 2018 être parvenu à développer un processeur de 72 qubit, dépassant les 50 qubit atteint par IBM l'année précédente[185].

Les entreprises et institutions américaines sont également les principaux clients d'une PME canadienne, D-Wave, qui réalise depuis 2007 une lignée de machines présentées comme des ordinateurs quantiques. Le fort scepticisme initial de la communauté de la recherche a laissé place à une controverse plus équilibrée. Après des années de doute,

---

[182] USAF Scientific Advisory Board Study, *Utility of Quantum Systems for the Air Force*, Study Abstract, https://www.scientificadvisoryboard.af.mil/Portals/73/documents/AFD-151214-041.pdf?ver=2016-08-19-101445-230

[183] Sandra Erwin, *op cit*

[184] « Optimization with Noisy Intermediate-Scale Quantum devices (ONISQ) Proposers Day », March 19, 2019, https://events.sa-meetings.com/ehome/index.php?eventid=405345&

[185] Martin Giles and Will Knight, « Google thinks it's close to "quantum supremacy." Here's what that really means », *MIT Technology Review*, by Mar 9, 2018, https://www.technologyreview.com/s/610274/google-thinks-its-close-to-quantum-supremacy-heres-what-that-really-means/

tout le monde semble d'accord pour dire qu'il ne s'agit pas d'un ordinateur quantique mais d'un supercalculateur quantique, presque un simulateur, spécialisé dans les calculs « d'optimisation ». La puissance affichée des machines actuelles est de « 2000 qubit » (en attendant une version à 4000 qubit en 2019), une performance irréaliste s'il s'agissait d'un réel ordinateur car elle permettrait selon les spécialistes de modéliser l'univers. *Google* et la NASA ont tout de même annoncé en 2015 avoir résolu un problème d'optimisation en une seconde contre 10 000 ans avec un calculateur classique. Lockheed Martin est propriétaire d'une de ces machines[186].

2.2.3 *La stratégie tardive destinée à réaliser un écosystème de la R&D en technologies quantiques*

Depuis l'an dernier, devant le défi posé par la Chine, Washington entend fédérer ses efforts et développer un véritable écosystème de recherche sur ces technologies. C'est tout l'objet de la revue stratégique réalisée sous l'auspice du *National Science and Technology Council* (NSTC) en 2018 et qui vise à améliorer la coordination entre les structures gouvernementales, le monde académique et l'industrie (par exemple avec la mise sur pied de *Joint Centers*), à développer une *workforce*, à améliorer les connections entre les disciplines de recherche et maintenir une « culture de la découverte » tant les incertitudes demeurent[187].

A l'appui de cette stratégie, le Congrès a voté un *U.S National Quantum Initiative Act* en décembre 2018. Le NQIA met sur la table 1,25 Mds$ sur 10 ans pour développer un écosystème de recherche fondamentale et renforcer cette dernière : planification et coordination de la recherche fédérale, développement des partenariats avec les universités, pour y promouvoir la formation dans ces technologies, et l'industrie. Trois entités principales sont impliquées : le NIST pour le développement des standards destinés à l'ensemble de cet écosystème, la *National Science Foundation* pour les aspects formation et qui doit mettre sur pied 2 à 5 *Multidisciplinary Centers for Quantum Research and Education* dotés chacun de 10 M$/an et enfin le département de l'énergie qui devra notamment mettre sur pied deux à cinq *National Quantum Information Science Research Centers*, qui seront chacun dotés de 25 M$/an[188]. Certains observateurs, comme Elsa Kania, du CNAS, estiment que si la Loi est la bienvenue, son ambition reste cependant assez limitée : elle n'offre par exemple aucune directive pour la préservation de cette BITD et la

---

[186] La machine recourrait à une technique de simulation par « recuit simulé » à l'échelle quantique. D. Dq, « La boîte noire de D-Wave fait des vagues », *Le Monde*, le 02 mars 2012, https://www.lemonde.fr/sciences/article/2012/03/02/la-boite-noire-de-d-wave-fait-des-vagues_1647718_1650684.html & Laurent Sacco, « Buzz : Google est encore loin de l'ordinateur quantique miracle », Futura-Sciences, 01/10/2016, https://www.futura-sciences.com/tech/actualites/ordinateur-quantique-buzz-google-encore-loin-ordinateur-quantique-miracle-maj-60811/ & Ryan F. Mandelbaum, Why Did NASA, Lockheed Martin, and Others Spend Millions on This Quantum Computer?, *Gizmodo* , 1/17/19 https://gizmodo.com/why-did-nasa-lockheed-martin-and-others-spend-million-1826241515

[187] Subcommittee on Quantum Information Science, Committee on Science, *National Strategic Overview for Quantum Information Science*, National Science & Technology Council, September 2018

[188] La loi est disponible au https://www.congress.gov/bill/115th-congress/house-bill/6227/text

mise en œuvre de ces technologies ou pour l'évaluation des risques de surprises dans ce domaine et des défis de la mise en œuvre de cette technologie[189].

L'enjeu est également une meilleure intégration avec les travaux du DoD financés à hauteur de 700 M$ sur les cinq ans, selon la *National Photonic Initiative*[190].

2.3 Le rattrapage chinois

La recherche fondamentale sur les technologies quantiques n'est pas une nouveauté en Chine. Elle est inscrite dans le fameux plan national de R&D en haute technologie (le « plan 863 ») de 1986. Les principaux travaux sont cependant lancés au début du millénaire par Pan Jianwei, considéré comme le « père de la science quantique chinoise », qui fonde en 2001 le laboratoire d'information et de physique quantique à l'université des sciences et des technologies de Chine.

Les investissements n'ont cessé de croître depuis. Comme dans bien d'autres domaines, la démarche de Pékin est décidée, constante et vise à obtenir la première place à terme. Les technologies quantiques sont l'un des quatre « mégaprojets » du plan scientifique à 15 ans (2006-2020). Xi Jinping les inclut en 2015 parmi les priorités pour lesquelles une rupture est attendue en 2030. La réorganisation de la planification de la R&D en 2016 destinée à favoriser l'innovation, renforcerait encore plus la place des recherches dans ce domaine. La Chine leur aurait ainsi consacré environ 300 M$ sur les années 2013-2015, un montant sans doute encore accru selon le CNAS pour les années suivantes : le nouveau plan de R&D nationale de 2016 leur consacre environ160 M$ auxquels il faut ajouter les lourds financements de la fondation nationale des sciences naturelles, de l'académie des sciences dans le domaine spatial, et bien entendu le département de développement des équipements de l'APL qui investit dans le domaine des capteurs. Plusieurs nouvelles structures sont créées, comme l'institut de recherche et d'innovation dans les sciences et technologies et l'information quantique, et surtout le laboratoire national pour les sciences et l'information quantique, la plus grande structure de R&D quantique chinoise, dotée de 14 Mds$ pour les cinq ans à venir ! Ce laboratoire travaillerait, entre autres, à fournir des recherches d'utilisation immédiate à l'APL[191]. L'académie des sciences militaires de l'APL a elle aussi augmenté son effort en la matière en 2017. Ces technologies quantiques font partie des « projets spéciaux de fusion civilo-militaire ».

Les effets ne tardent pas à se faire sentir. Ainsi, à partir des années 2013-2014, la Chine devient le premier pays en termes de dépôt de brevets, dont le nombre croit depuis

[189] Paulina Glass, « Congress's Quantum Science Bill May Not Keep the US Military Ahead of China », *Defense One*, September 17, 2018, https://www.defenseone.com/threats/2018/09/congresss-quantum-science-bill-may-not-keep-us-military-ahead-china/151319/?oref=d-river

[190] National Photonic Initiative, The Role of the Defense Department in the NQI, non daté 2018, https://www.lightourfuture.org/getattachment/95ab5e36-0049-4e19-90d3-0e7e566b8f8c/FINAL-DOD-Role-in-the-NQI-Apr-3-2018.pdf

[191] Elsa B. Kania & John K. Costello, *op cit*, p.8-9

exponentiellement. La comparaison avec les États-Unis met en lumière l'accélération tardive et mesurée de ces derniers.

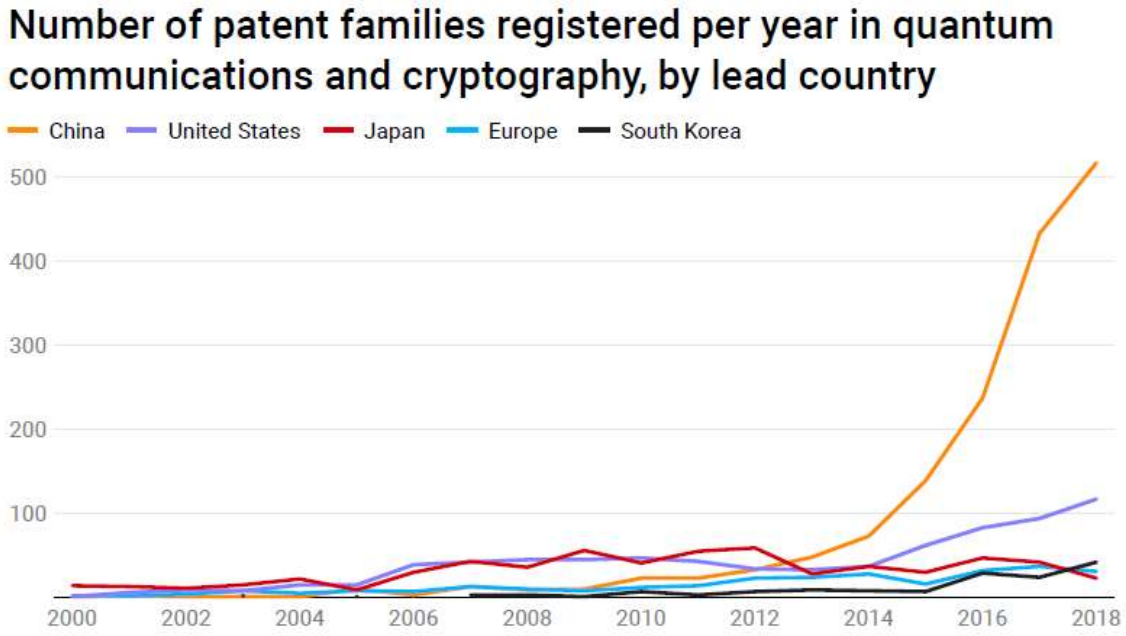


Figure n° 21 : NOMBRE DE BREVETS DÉPOSÉS PAR AN RELATIFS AUX COMMUNICATIONS ET AU CHIFFREMENT QUANTIQUES, PAR PAYS

La Chine se rapproche, rattrape voire dépasse déjà les États-Unis selon les technologies considérées. Elle revendique ainsi plusieurs « premières » :

- En 2016, la réalisation par la *China Electronics Technology Group Corporation* (CETC) d'un prototype de radar quantique, d'une portée de 100 km soit 5 fois supérieure au système de laboratoire développé en 2015 par les Américains. Les experts du MIT et canadiens travaillant sur ces projets, restent cependant sceptiques faute d'éléments tangibles[192]. Le CETC évoque une seconde génération de radar en mesure de détecter les appareils furtifs. Les chinois travaillent également à d'autres types de détecteur comme le « ghost imaging » ;
- La même année, la première liaison satellitaire (Milcius) avec clé quantique entre Vienne et Pékin est menée en partenariat avec l'institut autrichien du Dr Zeilinger, le directeur de thèse de Pan Jianwei …et avec le soutien de la *Space Support Force* de l'ALP ;
- Le développement du réseau à clé quantique entre Pékin et Shanghai déjà évoqué ;
- Le recours à 18 paires de photons intriqués en parallèle.

De fait, ces efforts produits dans le domaine de la sécurisation des communications concrétisent les conceptions élaborées par Pan Jianwei dès 2003. Il déclare cependant avoir

[192] Martin Giles, « The US and China are in a quantum arms race that will transform warfare », *MIT Technology Review*, January 3, 2019, https://www.technologyreview.com/s/612421/us-china-quantum-arms-race/

accentué ses recherches après les révélations d'Edward Snowden, mettant en lumière les vulnérabilités chinoises aux efforts de renseignement américain[193]. Pan Jianwei envisagerait un réseau de SATCOM entièrement sécurisé.

Pour Isaac Chuang, du MIT, la Chine a ainsi dépassé les États-Unis dans le domaine de la communication mais reste en retard dans le domaine du calcul quantique[194].

---

[193] Elsa B. Kania & John K. Costello, *op cit*, p.3

[194] Martin Giles, « The man turning China into a quantum superpower », *MIT Technology Review*, Dec 19, 2018

PARTIE 3 – ANALYSE D'ENSEMBLE DES POTENTIELS ET DES FACTEURS DE LA COMPÉTITION

1. Une érosion relative de la supériorité américaine ?

Qualifier l'état et les perspectives de la compétition technologique entre les États-Unis et leurs compétiteurs est une gageure du fait de la complexité des différentes interactions et du manque de données comparatives. De fait, si les données manquent souvent pour caractériser les programmes chinois et russes, il est tout aussi probable, sinon certain, que nombre d'avancées américaines restent elle aussi classifiées dans ces secteurs.

Cette section différencie, de façon un peu artificielle il est vrai, la façon dont les technologies de systèmes d'arme sont susceptibles d'affecter la balance des potentiels dans les différents domaines de lutte avant de s'élargir à la compétition dans les technologies de l'information dans leur ensemble.

1.1 Essai de balance des perspectives de potentiel capacitaire

Les avancées sur ces technologies, de même que leur caractère de rupture, n'ont de sens que replacées dans le contexte plus large des balances des potentiels que leur mise en œuvre affecte. Cet essai de balance va donc procéder d'une approche par domaines de lutte puis au niveau interarmées.

1.1.1 Un domaine aérien encore largement à la main des Américains

En dépit des difficultés budgétaires et programmatiques, l'USAF et la *Navy* modernisent considérablement leur inventaire avec l'entrée en service massive de F-35 arrivant, péniblement mais indiscutablement, à maturité, en attendant la nouvelle génération de bombardiers furtifs B-21 Raider. Les modernisations russes et chinoises n'ont pas cette portée. Les Chinois ont certes recapitalisé leur flotte de combat et renforcent celle du soutien pour accroître leur capacité de projection de puissance. Ils sont parvenus à mettre au point leurs appareils de 5ème génération mais ces derniers, aux capacités incertaines, ne semblent pas impressionner la communauté des observateurs. Dans le domaine sol-air, si les avancées chinoises en matière de radars sont importantes, leurs systèmes SALP restent en retard techniquement par rapport à ceux des Russes. Ces derniers modernisent eux-mêmes leurs moyens, avec difficultés comme en témoignent

les mises au point laborieuses du SU-57 et du S-500. On ajoutera que les fameux IADS d'inspiration russe, conçus pour contrer l'*airpower* américain, redondant, anti-PGM, mixant GE et interception cinétique (etc.), restent « *combat unproven* » donc d'une efficacité réelle incertaine et ne pourront sans doute par grand-chose face aux planeurs puis MdC hypersoniques que l'USAF s'apprête à mettre en œuvre à l'orée de la prochaine décennie et qu'elle destine certainement à la neutralisation des radars les plus performants contre le reste de ses moyens, furtifs notamment.

L'autre facteur de supériorité américaine réside dans leur architecture de défense antimissile, dont les évolutions planifiées à moyen terme (*Space Sensor Layer,* THAAD-ER, etc.) leur permet d'envisager de pouvoir intercepter les planeurs hypersoniques de Pékin alors qu'inversement, les systèmes russes et chinois ne peuvent pas grand-chose encore contre ceux que les Américains s'apprêtent à mettre en service dans la prochaine décennie. Le dernier facteur de supériorité américain réside dans l'architecture C2 et ses liaisons de données tactiques qui permettent les opérations réseau-centrées, gage démontré de supériorité tactique. Il est évident par rapport aux Russes, mais moins par rapport à la Chine qui progresse dans ce domaine du combat connecté. Cela étant, la migration par le cloud de combat est susceptible également de rebattre les cartes de la sécurisation de ces réseaux et des risques afférents en y généralisant la problématique de la lutte informatique offensive (LIO), où les Chinois sont sans doute en position nettement moins défavorable.

1.1.2 Le domaine naval : les missiles changent la donne en surface

L'US *Navy* conserve la maîtrise du milieu sous-marin face à une puissance russe qui a considérablement peiné à retrouver la maîtrise de sa technologie et une puissance chinoise qui part d'une expérience technique et opérationnelle encore proche du néant il y a 15 ans. Les progrès chinois sont cependant fulgurants. Si ses submersibles sont encore sans doute loin d'égaler les Virginia, Pékin semble avoir réussi à maîtriser l'intégration des systèmes sur ses plates-formes à en juger par la longévité accrue de ses classes, et surtout, investit massivement dans la dronisation et les capteurs pour compenser l'avantage américain.

Dans le domaine de surface, les choses sont plus équilibrées pour deux raisons. La première réside dans la maturation des armements antinavires supersoniques puis hypersoniques des plateformes aériennes, de surface et sous-marines russes et chinoises, ce qui leur offre clairement un avantage opérationnel. L'autre raison est l'émergence spectaculaire des forces aéronavales chinoises dont la route est cependant encore très longue pour conférer à la marine de l'APL une aptitude à la projection de force et même à la supériorité aérienne locale, analogue à celle dont jouissent les groupes aéronavals américains. Là encore, pour garantir sa résilience, la *Navy* est donc en train de faire évoluer son modèle vers une guerre en réseau de nouvelle génération, les *Distributed Maritime Operations* (DMO), reposant sur des opérations réellement distribuées au niveau théâtre,

replaçant les forces de surface sur une mission offensive qui était il y a encore peu l'apanage des seuls porte-avions. Ces DMO consacrent le primat de l'architecture C4ISR sur les plateformes. Ces architectures reposeront évidemment sur une vaste composante de drones sous-marins et de surface.

1.1.3 Dans le domaine terrestre, l'Army entend rétablir sa supériorité sur l'armée russe

Dans ce domaine terrestre, le compétiteur principal de Washington est Moscou, contexte géostratégique oblige. Selon l'antienne connue mais néanmoins vraie, les forces terrestres américaines, engagées pendant 15 ans dans l'adaptation à la contre-insurrection et dans le fiasco de l'ambitieux *Future Combat Systems*, ont largement stoppé leurs modernisations pendant 10 ans, sauf au niveau du C2, lequel se révèle inadapté et vulnérable à la présente compétition. L'*Army* est donc « *outgunned* » et « *outranged* » par l'armée russe. Sa réaction de ces dernières années est néanmoins vigoureuse : le vaste chantier des « *Big Six* » doit lui permettre de mener des opérations multidomaines (MDO) en mesure de fracturer les bulles de déni d'accès à la fin de la prochaine décennie. La principale priorité réside dans les feux à longue portée (les *Long Range Precision Fires - LRPF*) qui amènent ainsi l'*Army* à émuler la guerre des missiles dont les Russes et les Chinois se sont fait une spécialité. Les « feux stratégiques », dont le missile hypersonique, doivent constituer le fer de lance de ces LRPF.

Une autre priorité capacitaire est de reconstituer la défense sol-air courte portée, notamment pour faire face aux essaims de drones. Dans ce domaine, l'*Army* étudie cette fois sérieusement l'emploi des armes à énergie dirigée, dont la maturité, si elle est avérée, fera rentrer la défense sol-air dans un nouvel âge. Il est probable que sur ce plan, les Chinois et les Russes suivent les Américains.

1.1.4 L'exploitation du spectre électromagnétique : la dimension la plus problématique pour les Américains

C'est dans ce domaine que la balance semble la plus équilibrée. Les capacités russes de GE sont largement mises en avant depuis l'Ukraine et le général Selva, vice-CJCS, mentionne la GE comme l'un des domaines de supériorité de la Chine. Peut-être faut-il ici nuancer. Si l'on prend en compte (certes très empiriquement !) non seulement les plates-formes mais aussi les bases de données ROEM que les déploiements américains permettent par essence de mieux garnir que ceux des forces chinoises et russes, on peut faire l'hypothèse que les capacités d'attaque cyber-électronique aéroportée américaine sont encore en avance sur celles de leurs homologues russes voire chinois. En revanche, il est indubitable que les forces terrestres américaines (*Army* et *Marines*) ont enregistré un retard énorme sur l'armée russe, qu'elles tentent de combler à marche forcée depuis quelques années. Autre élément : le degré de convergence d'attaque électronique-LIO. Elle est actée chez les Américains et se situe au cœur du concept chinois d'*Integrated Network Electronic Warfare*. Les Russes en revanche, qui semblent disposer des capacités de GE les plus complètes, déclinaient encore il y peu cette convergence au futur.

Il n'est donc pas impossible dans ce domaine d'assister à un effet de ciseau : le rétablissement d'une parité voire d'une supériorité américaine dans le domaine aéroterrestre face aux Russes, compensé par des progrès constants de la Chine à l'heure des nouvelles technologies de la guerre cyber-électronique « cognitive » (c'est-à-dire une attaque cyber-électronique très agile, proactive reposant sur les technologies d'IA). Quoiqu'il en soit, il est certain que les vulnérabilités américaines peuvent être beaucoup plus critiques que celles de leurs compétiteurs, notamment des Russes, étant donné le niveau d'intégration du C4ISR et l'importance des opérations en réseau dans la doctrine américaine.

1.1.5 Dans le domaine spatial : la course au counterspace…et à la résilience

Chacun des compétiteurs semble désormais disposer qualitativement de systèmes terrestres comme exo-atmosphériques en mesure d'affecter les constellations de l'adversaire. Cependant, on peut considérer que les Américains disposent encore de plusieurs avantages : leur dispositif de *Space Situational Awareness* qui leur permet une meilleure tenue de situation, la variété des options (combinant peut-être des lasers, en tout cas de la GE et des systèmes orbitaux) et surtout une masse de satellites SATCOM et ISR garantissant une plus grande résilience. Cette résilience va s'accroître avec la logique de « désagrégation » des architectures, mixant les fonctions, les doublant avec une architecture aéroportée (*Aerial Layer Network*), avec l'exploitation des nouvelles constellations commerciales de microsatellites SATCOM et de télédétection, en LEO ou MEO et enfin avec la réactivité des lancements. Autre élément de résilience, la recherche effrénée de solutions de substitution aux GNSS pour les capacités PNT (pseudolites, centrales inertielles à MEMS, etc). Certes, les Chinois vont probablement disposer de ces atouts aussi. Ce n'est pas forcément le cas des Russes. Au final, si les trois compétiteurs se dotent d'outils de *counterspace*, il apparaît de plus en plus douteux que les deux grands puissent mutuellement s'interdire l'ensemble de leurs capacités d'ISR et de SATCOM en cas de confrontation. Il n'en reste pas moins qu'il s'agit à terme d'une rupture majeure par rapport à l'ère de l'exploitation de l'espace en toute impunité dont ont joui les Américains ces dernières décennies.

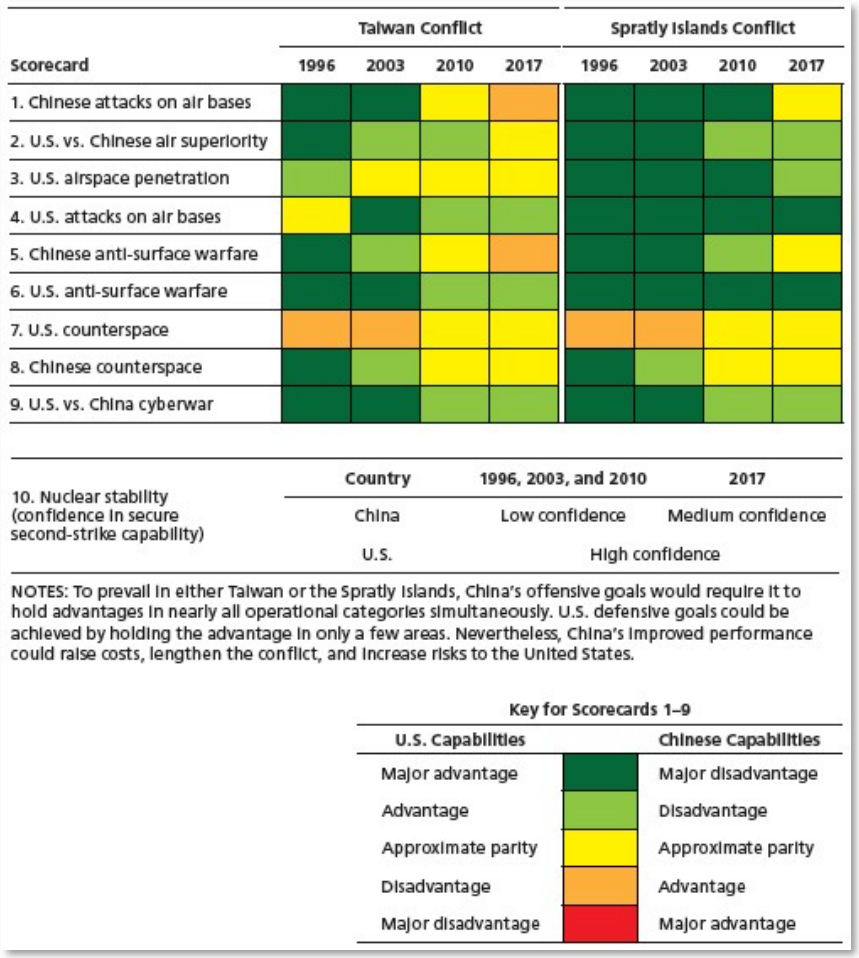
1.1.6 L'intégration interarmées et multidomaine : les Américains entendent pousser leur avantage

Lorsque Bob Work lance la *Third Offset Strategy*, il identifie, parmi les trois grands avantages dont jouiraient les États-Unis sur leurs compétiteurs russes et chinois, le niveau de *Jointness* des forces américaines, développé péniblement ces dernières décennies, et que les compétiteurs ne peuvent répliquer aisément. De fait, elle est une réalité au plan opérationnelle même si l'interarmisation de la stratégie capacitaire reste un talon d'Achille du système à décideur multiples que constitue l'appareil de défense américain. Les Américains accentuent leur développement en la matière : le mantra de leurs concepts depuis 10 ans (*Air-Sea Battle, Joint Operational Access Concept*, MDO) réside dans la synergie interdomaine, la prolongation du concept de NCW par l'intégration au plus bas niveau tactique des actions dans les différents domaines de lutte. Plusieurs briques sont déjà

bien présentes pour envisager réaliser des « *kill chain* » multidomaines, mais elles restent développées par chaque *service* (synergie air / espace / cyber pour l'USAF, synergie air / mer / cyber pour la *Navy*, etc.). Il reste à mesurer si le recours massif aux architectures modulaires ouvertes permettra enfin de réaliser cette synergie entre les *services*, obtenue actuellement de façon transitoire lors d'un engagement donné, par un commandement opérationnel. C'est l'une des clés de la résilience américaine face aux technologies de ruptures de leur compétiteur (*counterspace*, armes hypersoniques, etc.)

Les militaires chinois reconnaissent tout à fait cet état de fait et estiment que c'est l'un des domaines dans lequel ils doivent le plus progresser. Quant aux Russes, il est certain que les récents engagements leur ont permis d'engranger de l'expérience sur le C2 des opérations, mais ils accusent un retard certain dans le domaine du C4ISR. Leur culture opérationnelle reste de surcroît axée sur l'appui des autres domaines aux opérations terrestres.

1.1.7 Une contextualisation stratégique



Scorecard	Taiwan Conflict 1996	2003	2010	2017	Spratly Islands Conflict 1996	2003	2010	2017
1. Chinese attacks on air bases								
2. U.S. vs. Chinese air superiority								
3. U.S. airspace penetration								
4. U.S. attacks on air bases								
5. Chinese anti-surface warfare								
6. U.S. anti-surface warfare								
7. U.S. counterspace								
8. Chinese counterspace								
9. U.S. vs. China cyberwar								

	Country	1996, 2003, and 2010	2017
10. Nuclear stability (confidence in secure second-strike capability)	China	Low confidence	Medium confidence
	U.S.	High confidence	

NOTES: To prevail in either Taiwan or the Spratly Islands, China's offensive goals would require it to hold advantages in nearly all operational categories simultaneously. U.S. defensive goals could be achieved by holding the advantage in only a few areas. Nevertheless, China's improved performance could raise costs, lengthen the conflict, and increase risks to the United States.

Key for Scorecards 1–9

U.S. Capabilities		Chinese Capabilities
Major advantage		Major disadvantage
Advantage		Disadvantage
Approximate parity		Approximate parity
Disadvantage		Advantage
Major disadvantage		Major advantage

Figure n° 22 : « SCORECARD » DE LA RAND CO. DES CAPACITÉS AMÉRICAINES ET CHINOISES EN CAS DE CONFLITS POUR TAIWAN OU LES SPRATLEYS[195]

Enfin, il importe de **contextualiser cette balance des potentiels**. Or, cette dernière reste fondamentalement **asymétrique sur le plan stratégique**. En ce qui concerne les domaines terre/air/mer/EM, elle jouerait principalement dans le cadre d'engagement de projection de force américain dans les atterrages de ses deux compétiteurs, où la masse de leurs moyens, missiles et aéronavals dans le cas chinois, et terrestres dans le cas russe, rétabliraient partiellement l'équilibre dans la logique de l'A2/AD. D'où le contre-A2/AD comme unique horizon des développements capacitaires et doctrinaux américains depuis 10 ans. L'analyse de la Rand de 2015 le montre de façon assez convaincante. Etant donné les dynamiques en cours, il est probable que les catégorisations fixées glissent désormais en faveur d'une supériorité opérationnelle nette de Pékin dans le cas d'un scénario Taiwan, et à tout le moins d'une parité dans un scénario type Spratleys.

1.2 Les technologies de l'information : le pari du saut de grenouille

Pour nombre d'observateurs, **la Chine cherche le « leapfrog », le saut de grenouille**, la surcompensation de la supériorité américaine dans les armements conventionnels, en investissant massivement dans ces « mégaprojets » susceptibles de refaçonner la compétition militaire, au premier rang desquels figurent l'Intelligence artificielle et les technologies quantiques. **Si Xi Jinping a demandé à l'Armée populaire de libération (APL) de devenir une « armée de classe mondiale » (世界一流军队) d'ici 2050, les autorités sont plus confiantes en matière d'IA puisque l'objectif est de devenir la première puissance mondiale d'ici 2030**. La Russie, à plus petite échelle, poursuit une IA principalement opérationnelle.

L'un des enjeux majeurs, dans le domaine militaire, de l'investissement dans ces technologies réside dans l'avantage informationnel dont jouiront les systèmes de renseignement et de forces des compétiteurs. Elle s'inscrit ainsi dans la problématique plus large de la cybersécurité, autre domaine critique du Dr Griffin. Sur ce plan, le *scorecard* de la Rand évoquait en 2015 une relative avance des Américains, fondée sur l'emploi généralisé en Chine d'OS Windows piratés donc non patchés, qui constituerait une faille de sécurité béante. Cependant, qu'elle soit ou non aiguillonnée, au moins dans le discours, par les fuites de Snowden, la Chine semble avancer à grand pas dans la sécurité de ses systèmes. Dans le domaine commercial, Alibaba disposerait par exemple d'un avantage clair sur Amazon, obligé de modifier tous les ans l'architecture physique de son cloud – ce dernier

[195] Eric Heginbotham (dir), *The U.S.-China military scorecard : forces, geography, and the evolving balance of power, 1996-2017*, Rand Co, 2015, p.xxix

étant de conception plus « ouverte »[196]. L'avance prise par la Chine dans le développement du chiffrement par QKD participe de façon générale, de cette recherche effrénée de sécurité.

Inversement, les failles de beaucoup de réseaux américains civils, publics voire commerciaux, ne sont un secret pour personne, et sont largement exploitées par les innombrables intrusions dont beaucoup sont attribuées à la Chine et la Russie. Dans le domaine militaire également les vulnérabilités américaines existent. En témoignent les grandes opérations cyber chinoises « Titan Rain » ou « Byzantine Hades » des années 2000, aboutissant dans ce dernier cas au vol de 50 térabits de données incluant des informations sensibles : données sur les designs de SNA, de missiles air-air de la *Navy*, données sur les appareils les plus sensibles (F-35, F-22, B-2 etc.) sur les sites de contractants, etc. La « bonne nouvelle » est que le ROEM de la NSA aurait permis, selon Snowden, de détecter certaines de ces attaques en cours d'élaboration permettant de corriger certaines vulnérabilités en avance de phase et d'observer les attaques[197]. Un de ces pirates, nommé Su Bin, qui avait récupéré des données sur le C-17 et secondairement le F-35, le F-22 a été arrêté au Canada, extradé et a été condamné par la justice américaine à 4 ans de prison en 2016[198]. L'accord passé en 2015 par les administrations américaine et chinoise, qui aurait abouti à une diminution de ces attaques, aurait fait long feu à l'heure présente de la guerre commerciale. Autre illustration des vulnérabilités américaines, les rapports du *Director Operational Test & Evaluation* (DOT&E) mentionnent par exemple celles du F-35 et des nouveaux *Joint Regional Security Stack* en cours de déploiement, le dispositif centralisé de cybersécurité du *Joint Information Environment*, la vaste entreprise de refonte de l'architecture IT du Pentagone, lancée en 2010. Le déploiement de ces sites JRSS pour sécuriser les réseaux classifiés est d'ailleurs retardé pour cette raison[199].

Bien entendu, ces quelques éléments ne représentent qu'une facette de la partie émergée de l'iceberg que constituent les luttes quotidiennes dans le domaine cyber dont il est rigoureusement impossible, en source ouverte, de se faire un idée claire des facteurs de supériorité réelle des différents camps. Quoi qu'il en soit, la bascule progressive des dispositifs de C4ISR vers des *cloud* tactiques, véritable « NCW 2.0 », certes garantes d'avancées réelles dans l'efficacité et l'efficience opérationnelle, démultiplie l'exposition des systèmes de force américains à la LIO et en même temps accroît la criticité de ces

---

196 Entretien avec un ingénieur informaticien.

197 Jacob Appelbaum, et alii, « NSA Preps America for Future Battle », *Spiegel Online*, January 17, 2015, https://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409-2.html l

198 Garrett M. Graff, « How The US Forced China To Quit Stealing—Using A Chinese Spy », *Wired*, 10.11.18, https://www.wired.com/story/us-china-cybertheft-su-bin/

199 Jared Serbu, « DoD's Joint Regional Security Stacks still aren't effective, chief tester says », Federal News Network, February 5, 2019, https://federalnewsnetwork.com/dod-reporters-notebook-jared-serbu/2019/02/dods-joint-regional-security-stacks-still-arent-effective-chief-tester-says/ & Director, Operational Test and Evaluation, FY 2018 Annual Report, www.dote.osd.mil/pub/reports/FY2018/

attaques dans la mesure où elles peuvent permettre d'aboutir à des paralysies systémiques des architectures C4ISR.

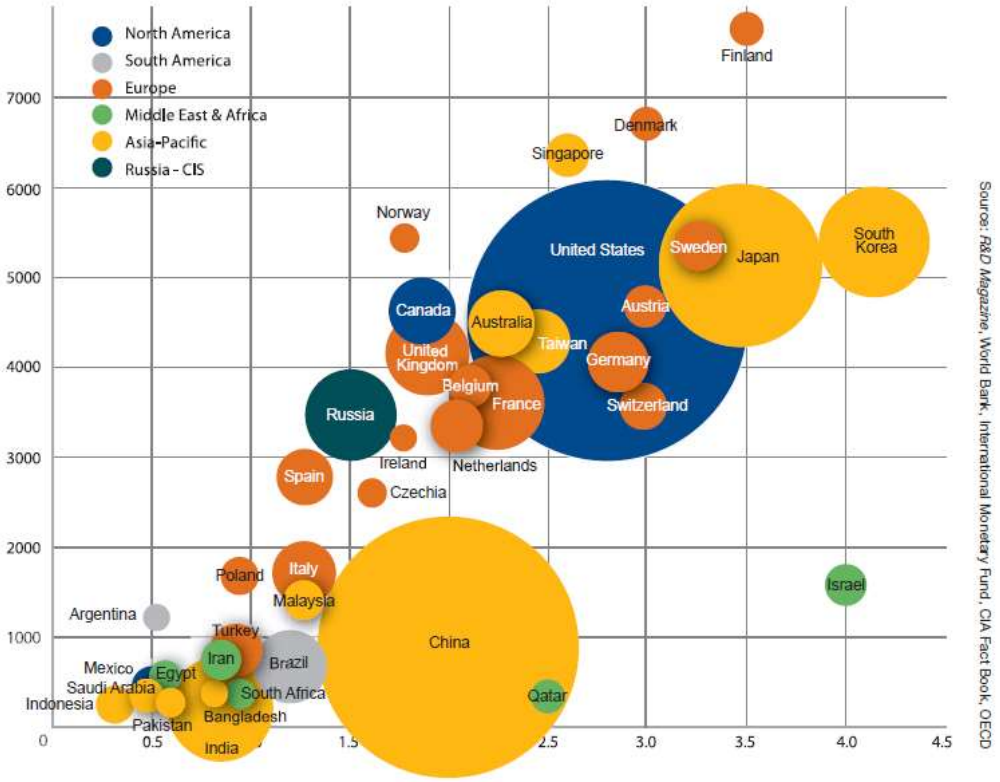
Un autre domaine mentionné par le Dr Griffin, est celui de la micro-électronique. L'USDR&E est particulièrement préoccupé par le fait que 80% des puces utilisées par l'industrie américaine, y compris dans la défense, bien que de conception américaine, sont fabriquées à Taiwan, un élément de vulnérabilité majeure dans le contexte géostratégique de long terme[200]. Cependant, dans ce domaine, les fabricants chinois sont encore plus dépendants que les Américains puisque les semi-conducteurs représentent en valeur le premier poste d'importation de la Chine (près de 300 Mds$), le pays ne fabriquant que 16% des semi-conducteurs qu'il utilise. Pékin a lancé depuis des années de vastes plans de plusieurs dizaines de Mds$ pour développer une industrie nationale du semi-conducteur garantissant à terme son autonomie, avec un succès mitigé jusqu'à présent semble-t-il. Les sanctions américaines actuelles visant ce secteur sont donc particulièrement importantes. Nous reviendrons sur ce point dans le troisième rapport de cet observatoire portant sur la BITD américaine.

2. Forces et faiblesses des compétiteurs

2.1 Le niveau de ressources

Les États-Unis restent à bien des égards les *leaders* de la R&D mondiale. Selon le *R&D Magazine*, en parité de pouvoir d'achat, ils y consacrent en 2017 environ 537 Mds$ contre 444 Mds$ pour la Chine (soit 256 Mds$ en plus si on calcule en taux de change), 185 Mds$ pour le Japon et 114 Mds$ pour l'Allemagne. Tous les autres pays sont à moins de cent milliards comme la France (62 Mds$). En termes relatifs, comme le nombre de scientifiques et d'ingénieurs rapporté à la population ou encore la part de la R&D dans le PIB, les États-Unis sont dans le peloton de tête et font encore beaucoup mieux que la Chine. La Russie fait figure de puissance très moyenne en consacrant 58 Mds$ à sa R&D, une part assez faible de son PIB.

[200] Paul Mcleary, « Pentagon, Intel Agencies Set Up New AI Joint Office », *Breaking Defense*, April 13, 2018, https://breakingdefense.com/2018/04/pentagon-intel-agencies-set-up-new-ai-joint-office/



The size of the circles in this Chart reflects the relative amount of annual R&D spending by the indicated country. Note the regional grouping of countries by the colors of the balls. The horizontal axis reflects R&D spending as a percent share of the countries' GDP (gross domestic product). The vertical axis reflects the number of researchers (including scientists and engineers) per million population for the respective countries.

Figure n° 23 : DÉPENSES DE R&D EN MONTANT BRUT ET PART DU PIB, ET NOMBRE DE CHERCHEURS PAR MILLION D'HABITANTS[201]

Dans le domaine aérospatial / défense, à l'image d'ailleurs des écarts de budget de la défense en général, le leadership est encore plus flagrant puisque les États-Unis comptent pour la moitié des dépenses mondiales soit 15,3 sur 30,5 Mds$ en 2018, l'essentiel étant composé du budget du Pentagone, soit environ 13 Mds$, dont les 5 groupes majeurs (Boeing, BAE Systems, Lockheed Martin, Raytheon et Northrop Grumman) captent l'essentiel puisqu'ils dépensent 9 Mds$. On ne dispose pas de données équivalentes pour la Chine. Pour la Russie, l'objectif du plan d'équipement 2011-2020 était de consacrer 10% des 30 Mds$ d'investissement annuel en R&D[202]. Cependant, comme le reste est consacré à l'acquisition et à la modernisation des équipements existant, ce chiffre est peut-être plutôt à comparer à l'ensemble de l'enveloppe de 82 Mds$ du budget RDT&E (incluant ainsi les tests et évaluations) du DoD.

Dans le domaine nettement plus vaste des technologies de l'information et des communications, l'autre secteur clé de cette compétition stratégique, le schéma est assez identique puisque les États-Unis comptent pour 125 des 228 Mds$ de dépenses mondiales.

[201] Source : *2018 Global R&D Funding Forecast*, a Supplement to R&D Magazine, Winter 2018, p.4, https://www.rdmag.com/article/2018/03/2018-global-r-d-funding-forecast-snapshot

[202] Susanne Oxenstierna, « Russia's defense spending and the economic decline », *Journal of Eurasian Studies*, Volume 7, Issue 1, January 2016, Pages 60-70, https://www.sciencedirect.com/science/article/pii/S1879366515000287#t0010

Les géants que sont *Amazon, Google, Intel, Microsoft et Apple* à eux seuls y consacrent au total plus de 82 Mds$. Les dépenses fédérales en matière d'IT atteignent 88 Mds$ en 2019, dont 20% sont consacrés à la R&D, soit 17 Mds$. La moitié de ces dépenses relèvent de la défense.

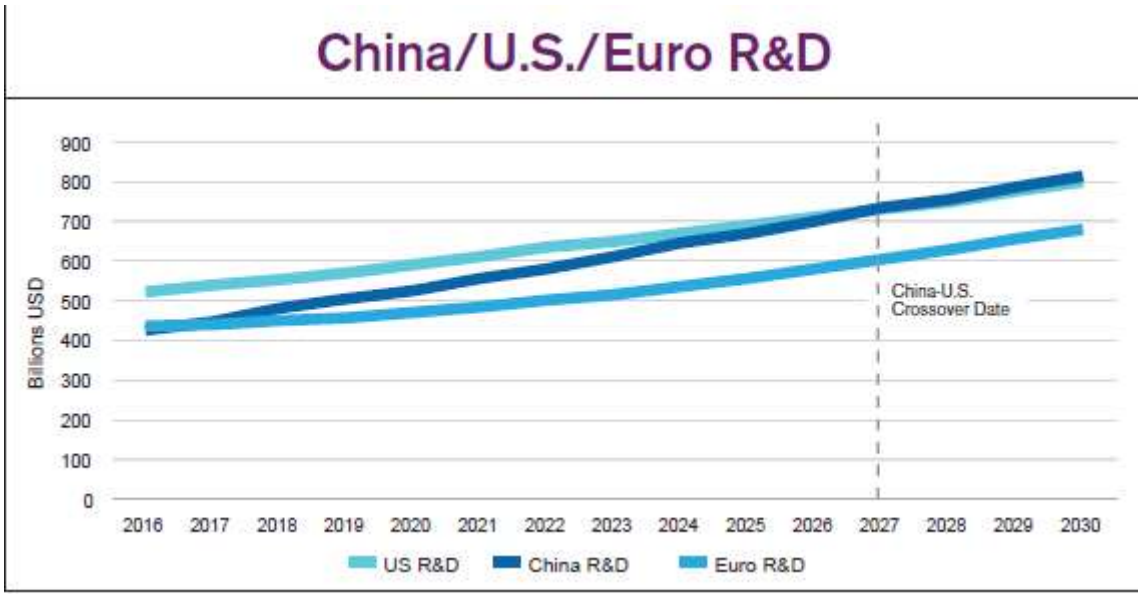


Figure n° 24 : COURBES DE PROGRESSION DES DÉPENSES DE R&D DES ÉTATS-UNIS , DE LA CHINE ET DE L'EUROPE[203]

C'est surtout la courbe de progression des investissements chinois qui inquiètent les hiérarques du Pentagone : ces derniers devraient dépasser ceux des États-Unis en 2027 selon l'*Industrial Research Institute*. Il convient cependant de relativiser ces prédictions. Ainsi en 2014, l'OCDE anticipait que le croisement des courbes interviendrait en 2019[204]. Dans son rapport 2017, le *R&D Magazine* fixait la date en 2025. Il n'en reste pas moins que la dynamique de croissance est clairement du côté chinois.

2.2 *Des R&D russe et chinoise aux routes très divergentes*

2.2.1 *Un système d'innovation chinois performant et massif mais aux faiblesses non négligeables*

Pour réaliser ses ambitieux objectifs, la Chine dispose d'une vaste base industrielle et technologique qui repose sur de nombreux points forts mais souffre encore de multiples handicaps par rapport à celle des États-Unis [205].

---

[203] Source *: 2018 Global R&D Funding Forecast,* a Supplement to R&D Magazine, Winter 2018, p.4, https://www.rdmag.com/article/2018/03/2018-global-r-d-funding-forecast-snapshot

[204] « China headed to overtake EU, US in science & technology spending, OECD says », OCDE, 12/11/14, https://www.oecd.org/newsroom/china-headed-to-overtake-eu-us-in-science-technology-spending.htm

[205] Lire de façon générale, CHEUNG Tai Ming, MAHNKEN Thomas, SELIGSOHN Deborah, POLLPETER Kevin, ANDERSON Eric, FAN Yang, Planning for Innovation : Understanding China's Plans for Technological, Energy, Industrial, and Defense Development, U.S.-China Economic and Security Review Commission, 2016,

Au plan des avantages, nous avons vu que ses **financements** en termes de parité de pouvoir d'achat se rapprochent de ceux des États-Unis et pourraient les dépasser à moyen terme. Elle est **bien orientée** par de multiples plans gouvernementaux (plan R&D 2006-2020, *Made in China 2025*, etc.).

La création d'une puissante R&D de défense est un des objectifs majeurs des réformes depuis 20 ans. La logique est de faire assumer la part majeure de cette R&D auparavant réalisée par les organismes institutionnels (académies, etc.) par les dix grands conglomérats qui composent l'essentiel de la BITD chinoise. Ces entreprises, devenues rentables depuis le milieu des années 2000, se réforment, s'allègent, pour devenir plus compétitives encore sur les marchés.

Dans le domaine des **technologies de l'information**, le principal facteur de supériorité chinois résiderait dans la **cohérence de son écosystème**. Pour Isaac Chuang, du MIT, c'est cet effort soutenu et cette étroite coordination entre centres de recherche gouvernementaux, l'académie des sciences et les universités qui expliquent les progrès fulgurants de la Chine. Le scientifique parle pour les technologies quantiques mais la remarque vaudrait également pour l'Intelligence artificielle.

Enfin, elle procède d'une logique **d'intégration civilo-militaire (ICM).** La spécificité de cette intégration est l'association d'une forte planification stratégique avec des mécanismes de marché dans le but de « promouvoir le développement coordonné de la défense nationale et de l'économie », un thème désormais récurrent dans la rhétorique du Parti communiste chinois (PCC) et du gouvernement. L'ICM a été promue au rang de « stratégie nationale » en mars 2015, et l'adoption de mesures concrètes s'est multipliée du Bureau politique du PCC aux provinces. Xi Jinping est ainsi devenu le directeur de la nouvelle Commission du Comité central pour le développement de l'intégration civilo-militaire en janvier 2017 visant à superviser au plus haut niveau cette intégration, signe de son importance. Dans ce cadre, de sérieux efforts sont en cours pour accroître la supervision et la coordination de cette intégration au niveau national et provincial, faciliter l'entrée des entreprises non étatiques sur le marché militaire, inciter les participations privées dans les industries de défense à capitaux mixtes, ou encore accélérer les transferts de technologie du secteur militaire au secteur civil (spin-off), et du secteur civil au secteur militaire (spin-on).

Historiquement, la R&D est concentrée dans quelques institutions comme l'Académie chinoise des sciences. Les grands conglomérats de défense ont également un rôle important mais souvent en lien avec d'autres institutions. Il faut notamment rappeler le rôle majeur des Laboratoires nationaux clés (civils) et les Laboratoires clés de S&T de la Défense nationale (militaires). Une loi de juin 2018 passée complètement inaperçue

https://www.uscc.gov/sites/default/files/Research/Planning%20for%20Innovation%20-%20Understanding%20China%27s%20Plans%20for%20Tech%20Energy%20Industrial%20and%20Defense%20Development072816.pdf

ici oblige le partage des "ressources" entre eux : installations et équipements de recherche scientifique, données scientifiques, matériel expérimental, etc.

La nouveauté ces dernières années est le rôle des entreprises privées et des *start-up* ce qui explique l'accélération de l'ICM, pas tant en matière de spin-off qu'en matière de spin-on. C'est le civil privé qui abreuve désormais le militaire public car il est beaucoup plus innovant, notamment dans les nouvelles technologies : IA, robotique, etc. C'est fondamental et **c'est une révolution en Chine qui alimente la confiance des autorités quant à leur aptitude à devenir en 2030 la première puissance en IA**, comme évoqué supra.

Cependant, ce système se heurte encore à plusieurs problèmes.

- La culture de la recherche et le système de formation sont encore insuffisamment matures dans certains domaines **des sciences, de la technologie, de l'ingénierie et des mathématiques (STEM)** ;
- Le système de motivations provoquerait **beaucoup de corruption, de fraudes et de dépenses inefficaces.** Sur ce plan, **la concurrence entre les provinces et les villes** représente un facteur d'importance. Elles cherchent généralement à renchérir sur les objectifs en adoptant leur propre plan d'innovation. Cela s'explique par la volonté d'obtenir des avantages économiques et le soutien du gouvernement central tout en surperformant par rapport aux cadres locaux des autres villes ou province, un atout pour les avancements au sein du parti. Or, cela conduit à la création de bulles et à une surchauffe dans de nombreux domaines, ce qui ne rend pas le financement de cette innovation efficace. Par exemple, selon les calculs du MERICS, si l'ensemble des objectifs fixés par les gouvernements locaux étaient atteints en matière de robotique, alors le marché en Chine atteindrait 716 milliards de yuans (plus de 90 milliards d'euros) en 2020 alors que le gouvernement estime que le marché devrait être d'environ 150 milliards de yuans (environ 19 milliards d'euros)[206]…;
- La **BITD** proprement dite est encore **trop fractionnée et redondante,** marquée culturellement par **l'héritage d'une structuration sur le modèle soviétique,** favorisant peu l'innovation ;
- **La coordination entre Etat central et pouvoirs locaux.**

Dans le domaine militaire, il en résulte que la R&D chinoise a permis de développer de nombreux systèmes « mono-technologique » (par exemple missiles, drones, capteurs, etc.) mais reste encore focalisé sur **l'amélioration des technologies existantes et manque de capacités d'intégration de vastes systèmes complexes indigènes**.

[206] WÜBBEKE Jost, MEISSNER Mirjam, ZENGLEIN Max J., et al., "Made in China 2025: The making of a high-tech superpower and consequences for industrial countries", Mercator Institute for China Studies, 2017.

Ces limites expliqueraient par exemple les difficultés de développement du J-20 et d'une motorisation indigène par la CASIC[207].

Jane's assessment of China's technology and capability gaps and areas of strength in Figure 7 further demonstrates the point.

Figure 7: China's Strengths and Weaknesses in Technology and Capability Development across Land, Air, Sea, and C4ISR Domains

Source: Jane's Navigating the Emerging Markets, China

Figure n° 25 : FORCES ET FAIBLESSES CHINOISES EN DÉVELOPPEMENT TECHNOLOGIQUE DANS LES DOMAINES TERRE, AIR, MER ET C4ISR [208]

Cependant, certaines analyses classiques des lacunes de l'innovation chinoise procèdent d'une lecture trop étroite selon les travaux de la *McKinsey Global Institute* ou de l'*Information Technology Information Foundation* (ITIF)[209]. En effet, **l'innovation porteuse de nouvelles capacités n'est pas uniquement fondée sur la découverte scientifique**. Elle peut être portée par trois autres mécanismes :

- L'innovation par l'efficience de l'industrie à produire des biens à moindre coût, ce qui permet de gagner des parts de marché (la Chine comme « usine du monde ») ;
- L'innovation fondée sur la satisfaction rapide de la clientèle ;

---

[207] Tate Nurkin *et alii, China's Advanced Weapons Systems*, Jane's by IHS Markit, préparé pour la U.S.-China Economic and Security Review Commission, May 12 2018, https://www.uscc.gov/sites/default/files/Research/Jane%27s%20by%20IHS%20Markit_China%27s%20Advanced%20Weapons%20Systems.pdf

[208] Source : Tate Nurkin et alii, *China's Advanced Weapons Systems*, Jane's by IHS Markit, préparé pour la U.S.-China Economic and Security Review Commission, May 12 2018, p.70

[209] Jonathan Woetzal et al., *The China Effect on Global Innovation*, McKinsey Global Institute, July 2015, http://www.mckinseychina.com/wp-content/uploads/2015/07/mckinsey-china-effect-on-global-innovation-2015.pdf Robert D. Atkinson & Caleb Foote, *Is China Catching Up to the United States in Innovation?,* Information Technolohy Information Foundation, April 2019, http://www2.itif.org/2019-china-catching-up-innovation.pdf

- **L'innovation par l'ingénierie**, c'est-à-dire la faculté à intégrer les technologies élaborées ailleurs dans des équipements plus complexes, générateurs de systèmes devenant eux originaux. La Chine a su ces dernières décennies parfaitement exploiter les technologies étrangères par le biais des partenariats, des *joint-ventures*, et des investissements dans les fleurons technologiques étrangers.

La Chine a obtenu des résultats impressionnants avec les deux premiers mécanismes et fait de mieux en mieux avec le troisième. En témoigne l'avance prise par exemple dans le développement de la 5G par Huawei, seule entreprise mondiale à disposer de l'ensemble des briques technologiques, enregistrant ainsi avec ZTE les nombreux brevets nécessaires, distançant irrémédiablement en la matière Qualcomm, son principal compétiteur américain. Cette **innovation par l'ingénierie nous semble également évidente dans le domaine des systèmes d'armes**, comme par exemple les sous-marins (avec l'intégration des technologies russes, françaises, etc.) ou les navires de combat de surface. On peut penser que **l'exploitation militaire des technologies d'IA** suivra le même mécanisme.

Enfin, il apparaît que **la guerre commerciale en cours ainsi que le changement de perception des occidentaux** (États-Unis bien sûr mais aussi Canada, Australie, NZ et UE) auront probablement un impact sur les capacités d'innovation futures de la Chine. Cette dernière va être de plus en plus isolée avec **une baisse des coopérations internationales avec les pays les plus avancés** ce qui devrait ralentir l'innovation. **La Chine peut-elle seule arriver à être innovante ? C'est la vraie question** pour les années à venir. Elle s'y prépare (*Made in China 2025*, etc.) mais ce n'est en rien garanti.

2.2.2 Une R&D russe en déshérence sauf sur certains domaines clés

La recherche et le développement en Russie sont financés à 70% sur fonds publics, soit beaucoup plus qu'aux États-Unis (25% environ) et même qu'en Chine (environ un tiers). Elle est pour une large part assurée par les grands groupes sous contrôle étatique. La participation du monde académique à cette R&D reste extrêmement faible ou polarisée sur certains domaines comme par exemple l'Université de Moscou sur la LIO. Il apparaît donc que, si la Russie dispose « d'îlots d'excellence », elle ne dispose d'aucun écosystème de R&D porteur des grandes innovations en matière des technologies duales de l'information susceptibles d'émuler les réalisations américaines et chinoises[210].

Dans le domaine stratégique, l'innovation reste donc principalement celle de la R&D militaire. Cette dernière a été réorganisée en 2012 avec la mise sur pied d'une fondation pour la recherche avancée, bâtie sur le modèle de la DARPA, puis d'une douzaine de centres de recherche spécialisés et, enfin en 2018, de la technopole axée sur l'intelligence artificielle déjà évoquée[211]. Néanmoins, les chercheurs Richard Connolly et Mathieu

[210] Apurva Sanghi and Shahid Yusuf, « Russia's Uphill Struggle With Innovation (Op-ed) », *Moscow Times*, Sep. 18, 2018, https://www.themoscowtimes.com/2018/09/18/russias-uphill-struggle-with-innovation-op-ed-a62921

[211] Julian Cooper, *The Russian State Armament Programme, 2018 – 2027*, Russian Studies, NATO Defense College | 01/18 – May 2018, p.13, http://www.ndc.nato.int/download/downloads.php?icode=548

Boulègue en brossent un portrait extrêmement sombre : « *Russian military R&D today can be characterized as 'degraded science', meaning that the quality and quantity of military science undertaken has significantly deteriorated since the 1990s* »[212]. Elle aurait été marquée par une fuite massive des cerveaux vers le civil ou l'étranger que ne compense que faiblement l'industrie de défense, laquelle n'est pas tournée vers l'innovation et dont le nombre de brevets, par exemple, s'est effondré. Ceci explique que les Russes ne poursuivent d'efforts ambitieux que sur un nombre réduit de segments relevant de cette compétition : missiles balistiques et de croisière, défense antiaérienne et antimissile avec Almaz-Antey par exemple, guerre électronique, etc.

Cette situation peut générer des doutes quant à l'aptitude des Russes, à développer des solutions réellement innovantes en matière d'IA voire même, dans le contexte des sanctions actuelles, à pleinement exploiter les technologies développées ailleurs pour transformer les capacités militaires russes, du moins à l'échelle sous-tendue par les déclarations du président Poutine.

2.3 Une accélération notoire de l'innovation militaire américaine

2.3.1 La TOS est morte, vive la TOS !

Comme évoqué lors du premier rapport, l'appareil de défense américain entend considérablement accélérer son développement capacitaire pour faire face à la « vélocité du changement » qui marque cette compétition stratégique. A cet égard, si la notion de *Third Offset Strategy* (TOS), lancée par Ashton Carter en 2015 et portée par son adjoint, Bob Work n'a pas survécu au changement d'administration, son contenu et sa dynamique restent virtuellement inchangés sous James Mattis et Patrick Shanahan. On en rappellera ici les principales caractéristiques ;

- L'effort sur les « avantages compétitifs » forçant l'adversaire à dépenser plus pour s'en prémunir, tel que conçu par feu Andrew Marshall, concepteur de la seconde OS et depuis, âme de la *Transformation* des forces américaines ;
- Une innovation continue et rapide dans la mesure où l'adversaire dispose des mêmes technologies que les Américains ;
- La capitalisation sur les trois avantages des États-Unis : le niveau de *Jointness* des forces américaines ; l'expertise en management et en ingénierie de la BITD permettant d'élaborer des systèmes de systèmes, et que la corruption « notoire » en Chine et en Russie ne permet pas à ces puissances d'émuler ; enfin la jeunesse américaine « *growing up in an iWorld and a democracy who is a little irreverent of authority, is endlessly creative, unafraid to make mistakes, is going to be better than a young man or*

[212] Richard Connolly & Mathieu Boulègue, *Russia's New State Armament Programme - Implications for the Russian Armed Forces and Military Capabilities to 2027*, Research Paper, Russia and Eurasia Programme, Chatham House, May 2018, p.33, https://www.chathamhouse.org/sites/default/files/publications/research/2018-05-10-russia-state-armament-programme-connolly-boulegue-final.pdf

woman who grew up in the iWorld in an authoritarian regime where their initiative is not necessarily appreciated »[213].

L'explication des points de focalisation ont quant à eux changé avec le temps et selon les interlocuteurs. Work évoquait ainsi que le cœur de la TOS résidait dans la « collaboration homme-machine » mais exposait aussi le besoin de développer des « *raid breaking technologies* » [214]. La révolution doctrinale qu'il appelait aussi de ses vœux a pris la forme des *Multi-Domain Operations* au sein de l'*Army* et de *l'Air Force*.

Cette accélération est également portée par les **évolutions récentes des dispositifs législatifs**, sous l'impulsion des commissions des forces armées de l'ère McCain / Thornberry, particulièrement préoccupées de la modernisation des forces américaines.

2.3.2 Une réorganisation partielle du Pentagone

L'émergence de la compétition stratégique s'est traduite par des réorganisations structurelles, qui restent cependant limitées tant le DoD disposait déjà de structures dédiées aux expérimentations de solutions rapides. Les principales ont probablement été la création du *Strategic Capabilities Office* (SCO) en 2012 et les *Defense Innovation Unit-Experimental* (DIUx) en 2015 dans le cadre de la TOS, enfin et surtout en février 2018 la recréation du poste d'*Under Secretary of Defense for Research and Engineering* (USD(R&E)). Cette réforme, promue par le sénateur McCain, vise à réinsuffler la culture de l'innovation qui existait à l'époque de la seconde *Offset Strategy* avec les directeurs de la R&E tels Harold Brown et William Perry, et que le GNA 1986 avait « décapitée » en subordonnant cette fonction à l'USD ATL (*Acquisition,Technology, Logistics*)[215].

Au niveau de l'OSD, l'USD (R&E) repose sur de multiples structures :

- La DARPA bien évidemment ;
- Le programme de *Joint Capability Technology Demonstration* (JCTD) mis sur pied au milieu des années 90, qui a de multiples succès à son actif (drone Predator, Liaison-16, etc.) ;
- Le moins connu *Rapid Reaction Technology Office* (RRTO) mis sur pied après 2001 pour accélérer le développement de solutions pour la lutte anti-terroriste. Il pilote des expérimentations et des démonstrations complémentaires aux JCTD allant de *Quick Reaction Special Projects* aux plus ambitieux *Emerging Capabilities Technology Development* (ECTD) sur trois ans et au prototypage rapide. C'est par exemple le RRTO qui mène les expérimentations sur le laser aéroporté de l'USSOCOM et les missiles air-air de l'USAF et le prototypage rapide des *Multiple Electronic Warfare*

---

[213] *The Third U.S. Offset Strategy and its Implications for Partners and Allies*, As Delivered by Deputy Secretary of Defense Bob Work, Willard Hotel, Washington, D.C., January 28, 2015 & Sydney J. Freedberg, "' People, Not Tech_ DepSecDef Work On 3rd Offset, JICSPOC", *Breaking Defense*, 9 Feb 2016

[214] Christopher P. Cavas, « Human-Machine Collaboration' Could Be Key to Offset Strategy », *Defense News*, September 14, 2015

[215] Voir notre rapport 5 du précédent observatoire, juin 2016, p.59.

(EW) capabilities de l'*Army* ou de la *High Power Microwave (HPM) for Airbase Defense* de l'USAF[216] ;

- Le SCO déjà évoqué, dont le rôle est de concevoir et d'expérimenter des solutions combinant des technologies matures, éventuellement mises en œuvre au sein des forces, pour développer des capacités innovantes. Son budget a explosé, de 50 M$ en 2012 à 1,2 Mds$ actuellement, finançant un nombre de projets passé d'une demi-douzaine à près de 30, témoignant de son succès. Si les programmes du SCO sont tous classifiés, de multiples trouvailles ont popularisé son rôle : *swarming* de drones Perdix, adaptations du missile SM-6 antiaérien et de l'ATACMS pour la mission antinavire, adaptation des *Hyper Velocity Projectiles,* conçus comme munitions du Railgun (le canon électromagnétique), aux pièces d'artillerie conventionnelles de la *Navy* et de l'*Army*, adaptation des caméras de smartphone pour le guidage des munitions de précision, large drone de surface, etc. Cela étant, la structure est dans la tourmente. Tout d'abord, Will Roper, premier directeur et âme du SCO, a pris la tête de la direction des acquisitions de l'*Air Force*. Ensuite, le SCO est victime de son succès car la NDAA FY19 entend le supprimer pour étendre sa logique à l'ensemble du Pentagone, ce que beaucoup d'analystes considèrent comme une hérésie[217]. Mike Griffin a donc décidé de transférer le SCO sous l'autorité de la DARPA, faisant perdre à son directeur les liens privilégiés qu'il entretenait avec la tête de l'OSD, ce qui a provoqué la démission de ce dernier[218] ;
- Les *Defense Innovation Unit-Experimental* sur lesquels nous revenons ci-dessous.

Au niveau des *services,* l'USAF a été la première, en 2003, à mettre sur pied un *Rapid Capabilities Office* qui a œuvré au développement du véhicule orbital X-37 et se focalise depuis des années sur le B-21 Raider. En 2016, l'*Army* a répliqué le modèle. Son RCO s'est initialement concentré sur le rattrapage en matière de guerre électronique et la résilience de la fonction PNT en réponse aux besoins des COCOM. Cette année, le bureau est rebaptisé *Rapid Capabilities and Critical Technologies Office* (RCCTO) et va travailler de conserve avec l'*Army Futures Command* et ses différents *Cross-Functionnal Teams* chargé des « Big six » prioritaires de la stratégie capacitaire de l'*Army*[219].

2.3.3 Des processus d'acquisition beaucoup plus rapides et « agiles »

L'organisation n'est cependant pas le principal problème de l'innovation de défense américaine, qui réside historiquement sur un processus d'acquisition (PPBE + DAS + JCIDS)

---

[216] Dr. Chuck Perkins, Principal Deputy Emerging Capability & Prototyping (EC&P), Prototyping - A Path to Agility, Innovation, and Affordability, Présentation, 2018 NDIA S&T Conference, https://www.acq.osd.mil/ecp/DOCS/NDIA_ST_Conference_2018_MAR.pdf

[217] Scott Maucione, « Why is a House panel trying to get rid of one of DoD's most successful offices? », *Federal News Network*, April 26, 2018, https://federalnewsnetwork.com/defense/2018/04/why-is-a-house-panel-trying-to-get-rid-of-one-of-dods-most-successful-offices/

[218] Reuters, « Pentagon eyes expanding DARPA future warfare research office », 24 May 2019, http://news.trust.org/item/20190524104353-xy3gm

[219] Jen Judson, « *Army* Rapid Capabilities Office is getting a new name and mission », *Defense News*, March 13, 2019, https://www.defensenews.com/land/2019/03/13/*Army*-rapid-capabilities-office-is-getting-a-new-name-and-mission/

trop lourd. Ce processus avait certes été aménagé dans la décennie 2000 pour mieux prendre en compte les besoins opérationnels urgents des commandeurs, mais rien n'existait entre ces méthodes de satisfaction rapide de ces urgences et la gestion compassée des *program of record* de la stratégie capacitaire de moyen long terme.

La voie de la *Middle Tier Acquisition* (MTA) de la NDAA FY16 (Section 804) revêt donc une importance particulière. Elle permet d'adopter des processus accélérés, s'extrayant du JCIDS classique, sans pour autant relever de la satisfaction de besoins opérationnels urgents dans les deux ans. La MTA permet d'une part le *Rapid Prototyping*, c'est-à-dire l'exploitation d'une technologie innovante par le développement et le déploiement de prototypes offrant une capacité opérationnelle résiduelle dans les 5 ans, d'autre part le *Rapid Fielding* (déjà existant) permettant d'entamer la production d'un système mature dans les 6 mois et d'achever son déploiement dans les 5 ans.

Les *services* n'ont pas pris longtemps pour recourir au MTA. En avril 2019, selon la *Defense Acquisition University*, 40 programmes revus utilisaient ce processus (dont 34 de *Rapid Prototyping*) engageant 27 Mds$. **Les 26,5 Mds$ de programmes en *Rapid Prototyping* sont à rapporter aux 90 Mds$ de crédits RDT&E de la FY19. En d'autres termes, en volume financier, plus du quart de la « R&D » militaire américaine relève désormais de cette approche de développement accéléré.**

- C'est l'*Air Force* qui l'utilise le plus massivement, sur 17 programmes, engageant près de 18 Mds$, avant tout sur les armes hypersoniques, les programmes spatiaux, notamment les SATCOM sécurisés, la modernisation de la dissuasion et l'équipement de la *Cyber Mission Force*, et les modernisations de certaines plateformes ;
- L'*Army* le destine à certains de ses programmes majeurs comme le canon ERCA, le nouvel hélicoptère d'attaque, le char léger, ou le véhicule de combat optionnellement télépiloté. Ainsi, 8 de ses 31 programmes clés (voir rapport 1 de cet observatoire) sont gérés en MTA ;
- La *Navy* présente la situation la moins claire : la *Defense Acquisition University* ne mentionne que 5 programmes MTA alors que notre propre relevé nous en donne beaucoup plus. Cela provient du fait que la *Navy* mentionne beaucoup de *Rapid Prototyping* mais ne précise pas l'utilisation formelle au MTA. Quoi qu'il en soit, elle utilise cette acquisition accélérée avant tout pour ses programmes de missiles Standard et pour la modernisation rapide de ses sous-marins et de ses dispositifs de lutte ASM.
- Enfin, l'USSOCOM utilise les MTA pour 9 de ses programmes ; missiles, arme du combattant, mini-sous-marins des SEALS notamment.

Le tableau ci-dessous représente dans la requête budgétaire FY20 les programmes pour lesquels les *services* entendent utiliser un processus MTA, soit en totalité, soit pour certaine composante.

Figure n° 26 : PROGRAMMES DE LA REQUÊTE BUDGÉTAIRE 2020 INCLUANT UNE APPROCHE DE *RAPID PROTOTYPING/RAPID FIELDING*[220]

Army
• Extended Range Cannon Artillery • Mobile Protected Firepower (le char léger) • Future Attack Reconnaissance Aircraft • Lower Tier Air Missile Defense (LTAMD) Sensor (nouveau radar du PAC-3) • Systèmes robotisés - Robotic Combat Vehicle (RCV) - Squad Multipurpose Equipment Transport (SMET) • Adv Armor-Piercing (ADVAP) for Small Cal Ammo • Standoff Volcano Obstacle (SAVO) Adv Tech • C2 - Unified Network Operations (UNO) - Common Hardware Systems-Rapid Acquisition and Procurement Integrated Database System (CHS-RAPIDS) - Enroute Mission Command (EMC) • Integrated Visual Augmentation System (IVAS) • Cyberspace Real-Time Acquisition Prototype Innovation Development (C-RAPID)
***Navy*/USMC**
• Medium Unmanned Surface Vehicle (MUSV) • Advanced Submarine System Development (modernisation des sous-marins) - Common Unmanned Aerial Vehicle (UAS) Comms - Fleet Module Autonomous Underwater Vehicle (FMAUV) - Li-Ion Battery FMAUV Submarine Integration - Clandestine Delivered Mine (CDM) - Advanced Weapons Enhanced by Submarine UAS against Mobile targets (AWESUM)/Blackwing Unmanned Aerial System (UAS) - Submarine Payload Integration - Electronic Warfare/Intelligence Surveillance and Reconnaissance (EW/ISR) Unmanned Underwater Vehicle (UUV) Payload - Submarine Launch Decoy • Lutte ASM - Theater Anti-Submarine Warfare (TASW) Deployable Family of Systems (DFoS) - SURTASS-E - Project NAUTICA: Integrated Theater ASW C4I

[220] Source : justificatifs budgétaires des services, exploitation par l'auteur

- Standard Missile-6 (SM-6) Block 1B Phase 1A Rocket Motor
- MAGTF) Unmanned Aircraft System (UAS) Expeditionary (MUX) with Vertical/Short Take-Off and Vertical Landing (V/ STOVL) capability
- Next Generation Naval Mission Planning System
- Information Assurance (IA)

USAF

- Espace
  - Family of Beyond Line-of-Sight Terminals (SATCOM EHF)
  - Defense Meteorological Satellite Program (DMSP)
  - JSpOC Mission System (JMS)
  - Station de traitement d'imagerie Eagle Vision
  - Petits projets du Space Systems Prototype Transitions (SSPT) (nouvelles constellations de capteurs spatiaux
  - Protected Tactical Satellite Communications (PTS) incluant les nouveaux terminaux Protected Tactical Enterprise Service (PTES) SATCOM large bande utilisant la nouvelle Protected Tactical Waveform (PTW)
  - *Army* and *Air Force* Anti-jam Modem (A3M)
  - Polar MILSATCOM system (EPS)
  - Satellite Control Network (SPACE)
  - Multi-Mission Satellite Operations Center (MMSOC)
  - Evolved Strategic SATCOM (ESS) nouveau système EHF
- Armes hypersoniques
  - Air-Launched Rapid Response Weapon (ARRW)
  - Hypersonic Conventional Strike Weapon (HCSW)
- Nucléaire
  - Nuclear Planning and Execution System (NPES).
  - Ground Based Strategic Deterrent
- C2ISR
  - Air & Space Operations Center (AOC)
  - E-3 Electronic Protection (EP)
  - Combat Air Intelligence Systems (CAIS)
  - Intelligence Advanced Development (IAD) (outils d'exploitation du rens)
  - Wide Area Surveillance (WAS) du NORAD
  - Battlespace Acoustics
- Cyber
  - Unified Platform de la Cyber Mission Forces
  - Joint Cyber Command and Control (JCC2
- Plateformes
  - B-52 Commercial Engine Replacement Program (CERP)

- Digital Radar Warning Receiver du F-16
- Extended Range Weapon (ERWn) (nouveau missile air-air)

- Organique
  - Logistics, Installations and Mission Support - Enterprise View (LIMS-EV)
  - Outils de gestion des ressources humaines

Un autre dispositif législatif clé est **l'*Acquisition Agility Act (AAA)* inclus** dans la NDAA FY17 (Title VIII, Subtitle B, Sections 805 à 809). Les parlementaires expliquent ainsi que : « *Rather than setting requirements in anticipation of future technologies,* ***weapon system platforms should be designed to provide the needed warfighter capabilities in the short term and flexible, open system architectures that allow components to evolve*** *with technologies and threats* ». L'AAA enjoint ainsi qu'à partir de janvier 2019, tous les *Major Defense Acquisition Programs* (MDAP) soient conçus selon une *Modular Open Systems Approach* (MOSA) permettant leur évolution incrémentale. Pour le court terme, ceci inclut par exemple les nouvelles plateformes de l'*Army*. Elle est aussi un élément clé pour favoriser l'interopérabilité des systèmes, talon d'Achille permanent de l'interarmisation des forces américaines, d'autant plus nécessaire pour réaliser la synergie interdomaines. L'AAA s'inscrit dans la lignée des initiatives de *Better Buying Power* du Pentagone visant depuis 10 ans à améliorer l'efficience des acquisitions. On manque encore de recul pour estimer comment le Pentagone et la BITD, historiquement habitués à la juxtaposition de « systèmes clients », gèreront cette obligation qui pose des contraintes non négligeables en matière de droit de propriété intellectuelle.

2.3.4 *IA et technologies quantiques : une mobilisation tardive et structurellement difficiles mais qui enregistrent des résultats*

Lorsque l'on se tourne vers les technologies de l'information, notamment l'IA et le quantique, il est évident que les États-Unis ont consacré plus de moyens que leurs compétiteurs et ce depuis plus longtemps. Cependant, paradoxalement, la création de grands écosystèmes outre-Atlantique est tardive et s'inscrit en réaction des avancées chinoises.

Le développement de ces écosystèmes se heurte en outre à des divergences de logique et d'intérêt parfois importantes entre l'administration et les industries. Si l'on excepte les grands groupes de défense et de leur chevelure de sous-traitance, totalement interdépendant avec le Pentagone, **il n'existe pas aux** États-Unis **de logique de fusion « civilo-militaire »** analogue à celle que les experts décrivent pour la Chine. Deux facteurs affectent ainsi cette coopération :

- **La logique des grands groupes comme les GAFAM, avant tout orientée sur le business**. Toute la question réside dans la gestion des dissonances avec « l'intérêt national » américain. En témoigne les controverses récentes concernant *Google*, que le Pentagone accuse de travailler indirectement au profit de l'appareil de défense chinois via ses partenariats avec les universités de Fuda et de Tsinghua.

Or, il apparait que les autres géants américains de l'informatique collaborent également avec de multiples entités chinoises[221] ;

- **La dissonance culturelle**. Beaucoup d'entreprises de la *high tech* ont une culture « *Global* » qui peut rendre certaines méfiantes voire hostiles à toute coopération active avec l'instrument stratégique (militaire et de renseignement) américain. Peter Singer estimait ainsi en 2015 « *It's in Silicon Valley's interest to act more global and hold the U.S. government at a distance* »[222]. Là encore, *Google* en est un bon exemple : les remous provoqués en interne par le projet Maven utilisant l'IA de *Google* pour le traitement de l'imagerie des drones dans le cadre de la lutte anti-terroriste, ont amené la direction à ne pas prolonger son contrat puis à renoncer à la compétition pour le programme de *Joint Enterprise Defense Infrastructure* (JEDI), visant à développer le vaste cloud général du Pentagone, un marché à 10 Mds$. La sélection d'IBM et d'*Amazon Web Services* pour JEDI montre cependant aussi que cette attitude est loin d'être généralisée.

Cette question fondamentale de l'éventuelle divergence entre *Globalization* et intérêt stratégique des États-Unis, qui ont longtemps été de pair, va d'ailleurs bien au-delà de la simple problématique des entreprises des technologies de l'information.

Il n'en reste pas moins que le Pentagone enregistre des résultats que peu ont anticipé. Ainsi, lors d'une étude sur la TOS menée en 2016 pour le présent laboratoire, la FRS se faisait l'écho des doutes quant à la capacité du Pentagone à s'associer le concours de la BITD la plus innovante, précisément en raison de ces divergences d'intérêt et de culture mais aussi de processus bureaucratiques incompatibles avec les méthodes de management qui ont cours en Californie ou à Boston. Or, force est de constater qu'après un revers initial, les DIUx ont su s'adapter et sont parvenus à « embrayer » avec les entreprises de la *high tech*. Ces unités d'innovation se concentrent sur cinq portefeuilles : IA, l'autonomie, l'humain, les technologies de l'information, et enfin l'espace. Dans le domaine de l'IA, les DIUx se concentrent sur trois types d'applications : vision numérique, analyse de données (incluant notamment la maintenance prédictive), et raisonnement stratégique.

Leur budget a connu une accélération rapide pour atteindre 100 M$ [223]. Aux antennes de la Silicon Valley puis de Boston se sont ajoutées celles d'Austin et de Washington DC. Certes, seuls 13 des 81 prototypes ont été incorporés par les *Services* mais certains représentent de remarquables réussites. C'est d'un contrat passé via la DIUx de Boston que s'est développé par exemple Kessel Run, l'implication des programmeurs dans la

---

[221] Jeremy Hsu, « Pentagon Warns Silicon Valley About Aiding Chinese Military », *IEEE Spectrum*, 28 Mar 2019, https://spectrum.ieee.org/tech-talk/aerospace/military/pentagon-warns-silicon-valley-about-aiding-chinese-military

[222] Tom Risen, « A Disconnected Military », *US News*, May 14, 2015

[223] Emmanuel Chiva, « Capturer l'innovation de défense : à la découverte de DIUx » *Défense & Industries*, n°11, juin 2018, pp 11-13 https://www.frstrategie.org/publications/defense-et-industries/capturer-l-innovation-de-defense-a-la-decouverte-de-diux-11-3

refonte des logiciels des centres d'opérations de l'*Air Force*, qui connait un énorme succès.

Couronnement de cette approche, le SECDEF a signé en 2018 un mémo mettant un terme au caractère expérimental et pérennisant ces structures, qui deviennent simplement des DIU[224]. Cette DIU va absorber également d'autres initiatives la *National Security Innovation Network* et le *National Security Innovation Capital fund*, un fond d'investissements dans les entreprises naissantes, évitant qu'elles ne tombent sous le contrôle d'investisseurs étrangers. La requête budgétaire pour DIU a ainsi augmenté à 164 M$ pour la FY20[225].

2.3.5 Une flexibilisation des méthodes de financement et de contractualisation

Une des raisons facilitant cette mobilisation réside dans la flexibilisation de ces financements, avec un recours accru à l'***Other Transaction Authority* (OTA),** c'est-à-dire la passation d'accords hors des règles fédérales d'acquisition, permettant de ne pas suivre les clauses contractuelles obligatoires classiques. L'OTA facilite notamment la création de consortium sur un programme. Inventé pour la NASA il y a cinquante ans, les OTA sont précisément conçues pour financer la recherche, le prototypage et éventuellement la production en série de ces prototypes. Jusqu'à présent, le Congrès n'en autorisait l'usage qu'à condition que le DoD démontre que les procédés classiques étaient inadaptés.

Ceci n'a pas empêché l'explosion du recours aux OTA, qui est passé de 12 accords en 2013 à 94 en 2017 portant sur 2,1 Mds$. Ce sont les financements OTA qui ont permis de solliciter rapidement les PME via les DIUx. Or la NDAA FY 2018 change fondamentalement l'approche du Congrès. Sa section 807 stipule en effet que : « *In the execution of science and technology and prototyping programs, the Secretary of Defense shall establish a preference, to be applied in circumstances determined appropriate by the Secretary, for using transactions other than contracts, cooperative agreements, and grants* ». Les spécialistes s'attendent ainsi à un accroissement encore plus net des accords OTA. Or, bien que le Congrès considère que ces accords soient le meilleur véhicule pour financer les technologies duales, attirer la BITD innovantes, les spécialistes débattent encore du gain d'attractivité réel des entreprises hors BITD classique ou de l'accélération programmatique que ces arrangements procurent. Ces derniers ne sont pas sans risques en termes d'opacification de la dépense publique, ce qui pousse la NDAA FY19 à réclamer au DoD des directives plus claires concernant le recours à ces arrangements et leur suivi[226].

---

[224] Scott Maucione, « Pentagon's DIU picks new leader amid existential changes », Federal News Network, September 24, 2018, https://federalnewsnetwork.com/people/2018/09/pentagons-diu-picks-new-leader-amid-existential-changes/

[225] Mike Gruss, « The Pentagon wants to create a broader network of innovators », *C4ISRNet*, May 13, 2019, https://www.c4isrnet.com/pentagon/2019/05/13/the-pentagon-wants-to-create-a-broader-network-of-innovators/

[226] Moshe Schwartz, Heidi M. Peters, *Department of Defense Use of Other Transaction Authority: Background, Analysis,and Issues for Congress,* CRS Report, Updated February 22, 2019, https://fas.org/sgp/crs/natsec/R45521.pdf

3. Conclusions : quels enjeux pour la France ?

Le principal enjeu de cette compétition pour l'appareil de défense français réside bien entendu dans le risque de décrochage technologique et capacitaire. Les destinataires de ce rapport sont à même de comparer la situation présente de la France et des projets qu'elle nourrit avec le développement qui précède. D'un point de vue externe, ce décrochage semble déjà largement acté dans de nombreux domaines vis-à-vis des Américains (est-il besoin d'en faire l'énumération ? renseignement, plateformes furtives, défense antimissile, C4, moyens de projection, etc.). Pour autant, dans bon nombre des technologies de rupture évoquées dans ce rapport, la France n'est pas encore irrémédiablement distancée, principalement en raison de la qualité de sa R&D. Elle entend suivre le mouvement soit seule (lancement du programme de planeur hypersonique Vmax par exemple) soit comme contributrice d'initiative de niveau européen (flagship sur les technologies quantiques par exemple). Cela étant, de nombreux facteurs sont de nature à motiver cette crainte du déclassement : la justesse des financements, les difficultés à s'organiser pour traduire cette R&D en projets industriels, la vulnérabilité de sa base industrielle et technologique, une culture d'ingénieur qui a certes démontré toute sa plus-value par le passé mais n'est pas nécessairement adaptée aux évolutions incrémentales, rapides qui caractérisent l'assimilation des technologies de l'information, etc.

La question se pose ensuite de la criticité de cet éventuel décrochage. Elle se manifeste sur le plan industriel et par conséquent, sur l'économie du pays à terme et sur son autonomie stratégique, qui repose largement sur la faculté de la BITD nationale à équiper nos forces. Sur le plan capacitaire, elle est évidente en ce qui concerne les fonctions anticipation et dissuasion. Par exemple, la faiblesse numérique de nos moyens spatiaux les rend éminemment vulnérables dans un environnement où se développent les capacités de *counterspace* évoquées. En ce qui concerne la fonction intervention, le risque de rupture est moins évident. D'un côté, on peut avancer que cette compétition ne change pas fondamentalement la donne pour ce qui concerne les interactions directes avec les grandes puissances : l'asymétrie est déjà un fait avec les Américains et la France, seule ou en coalition limitée, n'est déjà pas en mesure de se confronter avec la Russie dans le grand Est. Cependant, les gains qu'enregistreront la Russie et la Chine accroîtront mécaniquement les capacités de leurs forces expéditionnaires, en Méditerranée, au Moyen-Orient voire en Afrique, contraignant plus encore la marge de manœuvre de nos dispositifs dans ces régions. De plus, Moscou et Pékin sont susceptibles d'exporter certaines de ces capacités à des puissances régionales qui, à leur tour, nivelleront leurs capacités avec les nôtres.

Il serait certes tentant, compte tenu de nos ressources comptées, de nous en tenir au strict financement de notre présente modernisation et de la préservation de notre disponibilité opérationnelle. Cependant, en raison de son volume réduit, notre modèle de force ne peut faire l'économie de la haute vélocité, de l'IA, de la synergie multidomaine

ou encore de la préservation de ses capacités spatiales, faute de quoi il s'expose à des risques accrus d'infériorité stratégique et militaire, pas uniquement avec la Russie et la Chine, qui peuvent s'avérer lourds de conséquence. Tout l'enjeu est donc de combiner cette montée en gamme, qui ne peut qu'être très sélective, avec le maintien voire le renforcement de la « masse » qui nous fait cruellement défaut. Pour la France, l'*offset strategy* est un impératif.

ANNEXE – CATÉGORIES D'ORBITES

Geosynchronous Earth orbit (GEO): 35,786 km (22,200 mi)

- Continuous coverage over a very large region, may be inclined for coverage of high latitudes
- Satellites over the equator appear to hover above a single spot on the Earth's surface
- Primarily used by communications satellites

Highly elliptical orbit (HEO): Approximately 40,000 km (25,000 mi) at highest point

- Provides coverage of high latitudes and Arctic region
- Primarily used by communications satellites

Medium Earth orbit (MEO): 2,000 to 35,000 km (1,200 to 22,000 mi)

- Intermittent coverage over a large region; requires multiple satellites for persistent coverage
- Almost solely used by navigation satellites

Low Earth orbit (LEO): Up to 2,000 km (1,200 mi)

- Revolves around the Earth in ~ 90 minutes with very limited coverage
- Often used by remote sensing and scientific satellites