Nouvelles technologies de défense, quelle souveraineté pour la France ?

Thomas GRATIOLET - Guillaume KOCH - Danin MAGLOIRE GUEI MSIE 40 de l'Ecole de Guerre Economique

Problématique
Si une crise majeure survenait, la France, serait-elle résiliente et souveraine dans les nouvelles technologies d'armement afin d'y faire face ?

I) Quelles crises retenir ?

La France et l'Europe doivent faire face à de nouvelles crises qui fragilisent leur BITD. En effet, celles-ci ont cruellement démontré la fragilité des économies occidentales dans les approvisionnements stratégiques : semi-conducteurs, masques, gel, paracétamol, aujourd'hui l'énergie, demain les terres rares… Nous sommes perpétuellement en tension et une réflexion sur le renforcement de la résilience française est donc nécessaire pour se préparer à ces nouveaux défis dans tous les champs de conflictualité.

Nous considérons une crise comme une « *rupture dans le fonctionnement normal d'une organisation ou de la société, résultant d'un événement brutal et soudain. La crise est marquée par un trouble profond menaçant la stabilité voire l'existence de l'organisation ou de la société*. »

En effet, une crise est caractérisée par sa soudaineté et par l'urgence des mesures à prendre, par une complexité d'analyse accrue due au caractère erratique ou parcellaire de l'information, par l'irrationalité des acteurs en situation de panique (désorganisation, tensions, urgence) et par la perte de références. Ainsi, il nous semble que 2 crises majeures pourraient impacter le domaine militaire français dans sa dimension technologique :

- **Tensions sur les matières premières** (en particulier sur les composants électroniques) :

Elle impacterait l'ensemble des industriels français de la BITD et causerait de catastrophiques pénuries de composants et de matériels électroniques et informatiques clés. Les chaînes d'approvisionnement rompues fragiliseraient de nombreux secteurs de l'économie française.

- **Crise dans le cyberespace** (réseaux de communications et gestion informatique (systèmes de guidage, Cloud, IA, calculateurs quantiques) :
Elle impacterait de nombreux services informatiques et de partage de données, traditionnels ou basés sur l'IA. Des cyberattaques à l'impact multidimensionnel et exponentiel s'appuyant sur des malwares, des techniques de rançonnage ou de désinformation. De nombreuses sociétés du complexe militaro-industriel seraient durablement pénalisées.

Ces deux types de crises sont étroitement liées au profil des menaces impactant le domaine militaire et économique français et en constante augmentation. En effet, les menaces terroriste, criminelle ou étatique restent omniprésentes et cristallisent les tensions sur le sol national et entre Etats. En outre, le risque climatique (catastrophes naturelles, incendies, pénurie d'eau, pollution) concourt au manque de ressources naturelles essentielles aux industriels militaires français. Des stratégies de puissance renouvelées mettent l'Europe à l'épreuve, et les nouveaux champs de conflictualité s'étendent au cyberespace ou à la sphère informationnelle (cybercriminalité, cyberespionnage, concurrence déloyale et vols, désinformation)

Cyberattaques 2021 : rétrospective • HeadMind Partners
Lithium, cobalt et terres rares : la course aux ressources de (...) - pressegauche.org)

II) Impact des crises sur les technologies de défense

a) Rupture des approvisionnements

Le cas d'une crise de grande ampleur agissant sur la disponibilité de matières premières apparaît largement plausible au regard de la séquence 2019 - 2022, qui a vu se succéder une rupture des chaînes d'approvisionnement mondiale en composants clés et en matières premières (semi-conducteurs et puces, terres rares), puis en ressources alimentaires et énergétiques avec la guerre en Ukraine. Ce scénario est donc à prendre au sérieux et aurait des conséquences catastrophiques pour l'économie et la BITD française.

Les dimensions hardware étudiées (missilerie, matériel quantique) seraient les premières impactées, avec des conséquences en cascade sur les volets logiciels (IA, Cloud, Cyber), qu'ils fournissent.

Les grands groupes français comme ATOS ou MBDA, coupés dans leurs approvisionnements, pourraient perdre de grandes commandes et appels d'offres internationaux du fait de la rupture de disponibilité de ces composants. Des opportunités saisies par leurs concurrents plus proches des sources d'approvisionnement, en Asie (Corée du Sud, Japon, Chine) et aux Etats-Unis (Lockheed Martin, Northrop Grumman, Raytheon). La situation explosive dans le détroit de Taïwan, renforcerait la position américaine, forçant TSMC à prioriser ses commandes et même à investir sur son sol (Texas, Californie) dans des usines géantes. De facto, les composants en question se

retrouveraient par ailleurs encore plus soumis aux réglementations ITAR et Cloud Act, bloquantes pour les industriels français.

Cette perte de commandes aurait nécessairement un impact fort sur la profitabilité de ces groupes, et donc sur leur santé financière et boursière, ce qui les exposerait davantage à des risques d'OPA hostiles. Une profitabilité parallèlement grevée par les surcoûts logistiques et ceux liés à une asymétrie entre l'offre et la demande en composants clés.

Si les approvisionnements sont bloqués, des conséquences sont à anticiper sur les capacités de production des industriels de défense sur le territoire national, qui se verraient obligés de ralentir le rythme des usines avec des conséquences sur l'emploi : chômage partiel, gel des recrutements, voire licenciements. Les chaînes de sous-traitance auprès des PME et ETI spécialisées seraient mécaniquement impactées, avec le double risque de défaillance et de perte de savoir-faire clés, préjudiciable à court et à long terme pour la BITD, et de perte d'emplois dans les territoires. Des mouvements sociaux seraient à craindre.

Une cascade d'évènements qui verrait aussi fondre les recettes de l'Etat émanant de la filière Défense (TVA, impôts, taxes).

Par ailleurs, le ralentissement global de la filière dû à cette rupture d'approvisionnements verrait les grands industriels de défense perdre l'initiative sur des projets clés (MGCS - char du futur, avion du futur - SCAF) à cause d'un ralentissement de leurs investissements en R&D. Les délais de développement de certains projets clés et structurants pour l'Etat (missiles, quantique militaire) sont à anticiper, ainsi qu'une raréfaction des stocks de munitions, déjà très faibles, sur la partie missilerie.

Enfin, les clients finaux, notamment les Armées seraient touchés par la non-livraison ou le retard de commandes, mettant en péril leurs capacités sur le terrain.

b) Cyber Pearl-Harbor

Le terme *Cyber Pearl-Harbor* fait référence à une cyberattaque majeure qui touche les infrastructures vitales de tout un pays. L'Estonie en 2007 et l'Ukraine fin 2015 se sont retrouvées dans des situations critiques à cause de cyberattaques russes généralisées. Les dégâts furent colossaux pour les systèmes financiers, de santé, de transport ou dans la relation aux administrés ainsi que pour l'économie en général (milliers d'entreprises dont les systèmes informatiques furent bloqués).

Si la France, et plus particulièrement sa BITD, étaient ciblés de cette manière, les dégâts pourraient être colossaux. Par exemple, un arrêt, même court, des services informatiques viendraient désorganiser les capacités de production et de distribution des industriels répondant à leurs commandes. Sur certaines chaînes de production, des machines peuvent faire goulot d'étranglement par leur taille, leur rareté ou leur coût. Si elles venaient à être ciblées spécifiquement, c'est toute la production de l'usine qui serait arrêtée. On peut imaginer le cas chez MBDA pour la production de missiles sol-air, ce qui empêcherait les forces armées de reconstituer des stocks déjà bas. Le scénario peut être envisagé sur d'autres types de munitions, comme les obus (Nexter), ou bien sur des pièces de rechange de Rafale (Safran), gelant en partie les capacités des armées françaises.

Les industriels souffriraient ainsi de pertes financières importantes (retards, pénalités, manque à gagner) mais aussi de dommages réputationnels particulièrement préjudiciables à l'export. La cyberattaque peut en effet avoir pour objectif le vol de données secrètes (brevets, plans, manuels etc.) comme l'a connu Naval Group en 2011 et 2016, et dont la réputation fut mise à mal alors qu'elle était en pleine négociation avec l'Inde et l'Australie. D'autres données, plus préjudiciables encore aux forces armées pourraient être piratées, notamment des protocoles secrets en lien avec son organisation interne (localisation des forces et des armements) ou autour de la dissuasion nucléaire, à laquelle concourent certains industriels de défense (Naval Group).

Une attaque de grande ampleur pourrait aussi cibler les services de soutien aux armées comme le service des essences (gel des capacités à distribuer du carburant), du train (piratage de systèmes de routage), de santé (cyberattaque contre des hôpitaux militaires) ou bien de mobilisation de réservistes (déni de service) avec pour effet le gel des capacités de soutien et la démoralisation des troupes. La guerre en Ukraine a ainsi parfaitement démontré l'importance de la logistique et du soutien arrière dans la résilience et la combativité des troupes au front. L'utilisation du quantique pour un attaquant décuplerait la puissance de l'attaque, puisque celui-ci serait en mesure de pénétrer, en quelques heures, 100% systèmes d'information n'utilisant pas de cryptographie post-quantique. La bataille est donc lancée.

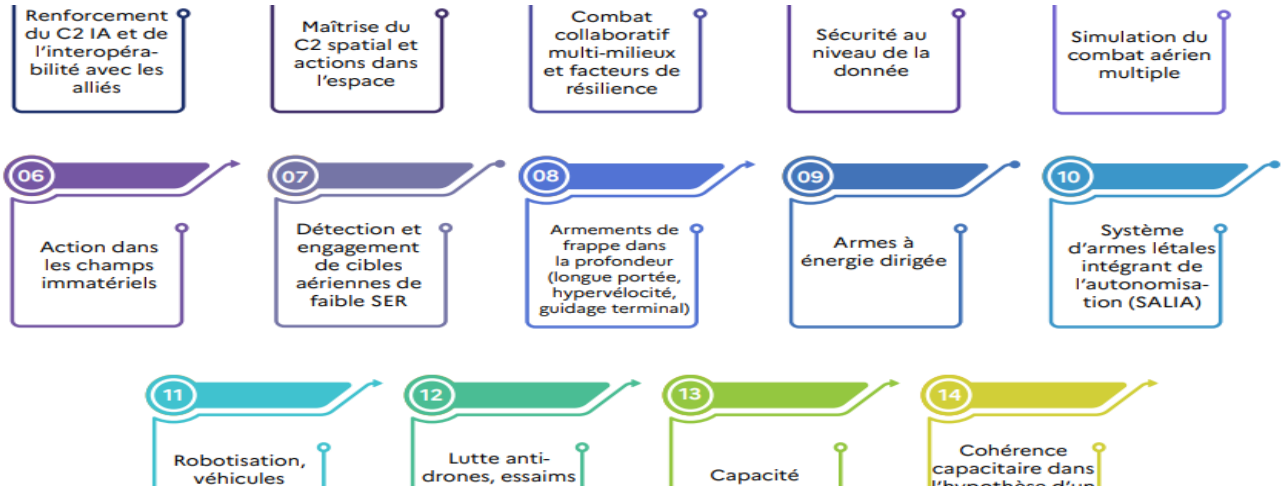
Plus largement, un cyber Pearl-Harbor, couplé à une attaque informationnelle de grande ampleur, provoquerait une désorganisation générale de l'industrie de défense qui rejaillirait sur la société civile: perte d'emplois, panique, crise de confiance, discrédit des armées et du politique, piratage d'infrastructures vitales non militaires (santé, énergie, finance, télécommunications, transport), dont le pays aurait du mal à se relever.

Enfin, une difficulté supplémentaire dans le cas d'une cyberattaque massive réside dans sa caractérisation (est-ce un acte de guerre ?), son attribution (quelles preuves formelles présenter au grand public), puis son évaluation (quels dégâts réels, comment les chiffrer, ou s'arrête réellement l'attaque). La France, pourtant, s'organise en renforçant ses capacités de cyberdéfense autour du COMCYBER, de la DGA et de la DRSD sur le volet militaire, de l'ANSSI et de la DGSI sur le plan civilo-intérieur. La liste des OIV, OSE, et entreprises de la BITD est ainsi classée secret défense, et les moyens alloués aux différentes cyber agences sont en augmentation constante.

III) Technologies de défense, quelle souveraineté française sur le champ de bataille ?

Les nouvelles technologies ayant une application militaire sont nombreuses. L'extrait du document DRoid 2022 montre bien le vaste panel de technologies pouvant intéresser les Armées françaises. Dans le cadre de cette étude, nous retenons 4 domaines qui nous semblent prioritaires, et où la France doit concentrer ses efforts de souveraineté au profit des entreprises concernées : Hyper vélocité, Cloud, Intelligence Artificielle, capacités dans le calcul quantique.

L'intérêt de chaque technologie sera présenté et 1 à 2 entreprises majeures dans chaque domaine analysé.



Thèmes d'intérêt de l'AID – extrait DRoid 2022

Nous proposons un code couleur de souveraineté sur les critères suivants :

- **Indice général** : Contribution à la souveraineté économique française
- **Indice 1** : Force d'innovation technologique ;

- **Indice 2** : Contribution à la puissance économique française ;
- **Indice 3** : Contribution au rayonnement de la France ;
- **Indice 4** : Indépendance vis-à-vis de puissances étrangères ;
- **Indice 5** : Indépendance de la société par rapport à des fonds et des ressources hors France

note		
perfectible	moyen	bon

Hyper vélocité et énergies

La Guerre Froide a plongé le monde dans une longue période de « paix belliqueuse » et de « guerres limitées ». Bien que les affrontements s'intensifiassent sur le terrain idéologique, il régnait un « équilibre de la terreur », caractérisé par la course aux armements et au développement de capacités nucléaires. Cette capacité dont dispose les grandes puissances dont la France, suscitait de la part des blocs Est et Ouest des craintes de *mutual assured destruction* (MAD) et des conséquences à long terme que devaient contenir la **dissuasion nucléaire**.

Pour être efficace, celle-ci nécessite non seulement de posséder de l'arme nucléaire mais aussi de disposer des moyens (vecteurs trois dimensions) de s'en servir : bombardiers stratégiques, missiles balistiques, sous-marins. En 1996, Jacques Chirac décide de se séparer des lanceurs de missiles fixes. La France dispose donc de la capacité d'envoyer des missiles via ses 4 SNLE, regroupés au sein de la force océanique nucléaire stratégique (FOST), et via sa flotte de Rafales.

Afin de maintenir équilibre stratégique et influence, les grandes puissances ont ainsi intensifié la course aux armements en développant des technologies dites de rupture, comme l'Hypervélocité.

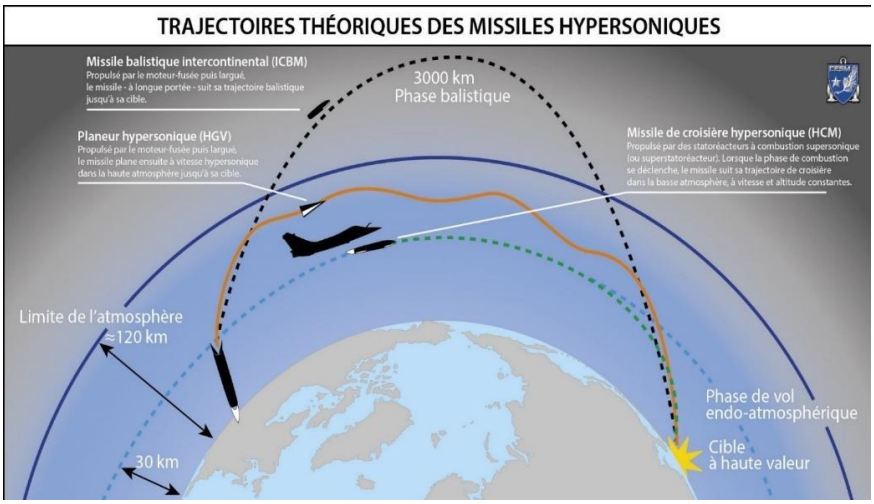
- **Hypervélocité et applications militaires**

Les vecteurs hypervéloces sont devenus aujourd'hui l'expression la plus significative de l'avantage stratégique militaire des forces armées. Si les missiles balistiques traditionnels volent à des vitesses folles, supérieures à Mach 20, leurs trajectoires paraboliques restent bien prévisibles.

Les missiles hypervéloces sont des armes conçues pour évoluer à des vitesses supérieures à Mach 5, soit 6.100 km/h. Ils sont donc extrêmement rapides, mais se démarquent également par leur capacité à effectuer des vols téléguidés suivant des trajectoires assez irrégulières et donc imprévisibles pour les défenses anti-aériennes. Ces missiles sont des vecteurs hautement manœuvrables et qui peuvent couvrir une portée minimum de 1.000 km. Les experts les catégorisent en deux classes :

- **Les planeurs hypersoniques** (HGV, Hypersonic Glide Vehicle) sont des ogives propulsées dans la haute atmosphère par des missiles balistiques à portées intercontinentales, avant de retomber suivant des mouvements évasifs et contrôlés par appuis aérodynamique vers le lieu de détonation ciblé. Ils sont ainsi dépourvus de propulsion propre. Les seuls développés et déployés à ce jour sont le DF-ZF chinois et l'AVANGARD russe.
- **Les missiles de croisière hypersoniques** (HCM, Hypersonic Cruise Missile) qui, contrairement aux planeurs HGV, sont dotés de leurs propres systèmes de propulsions. Ils évoluent dans les couches de l'atmosphère sous les 30 km sur une portée de 1.000 km.

La Russie et la Chine ont annoncé et déployé des vecteurs hypervéloces déjà opérationnels. Quant aux Américains, ils développent des programmes très avancés, au même titre que l'Inde, le Japon, La France ou la Corée du Nord.



- **<u>Puissances militaires dans la course à l'Hypervélocité</u>**

La **Russie** dispose d'un avantage stratégique considérable vu que ses systèmes de missiles sont déjà jugés opérationnels depuis 2018 et le début de sa production en série : Avangard et Kinjal, qui pourtant ont montré leurs limites en Ukraine car mal employés. En juillet 2021, la Défense russe a par ailleurs publié la séquence d'un tir de HCM de type Zircon depuis la mer Blanche. La Russie reste le seul pays à avoir utilisé des missiles hypervéloces sur un théâtre d'opérations, comme le 18 mars 2022, où un entrepôt souterrain de missiles et de munitions ukrainien a été détruit par un Kinjal aéroporté par un MIG 31.

La **Chine** a également montré des avancées remarquables dans le développement d'armes hypervéloces. Selon le Financial Time, la Chine a réalisé une manœuvre ultra sophistiquée que ni les Etats-Unis ni la Russie ne maîtrisent actuellement. En juillet dernier, les experts de l'agence de recherche du Pentagone ont identifié un projectile hypersonique tiré depuis un autre véhicule volant à vitesse hypersonique. Le missile hypervéloce chinois avait fait le tour de la terre avant de descendre vers sa cible (manquée de loin). Le Général américain Mark Milley a noté un *« test significatif d'un système d'armement hypervéloce »*. Le Dongfeng-17 aurait la capacité de percer des portes avions de l'US-Navy de façon imprévisible aussi bien en mer de Chine que dans les eaux du Pacifique.

Les **États-Unis** bien qu'accusant un retard dans le domaine, travaillent sur cinq programmes majeurs, dont le HGV Advanced Hypersonic Weapon testé en 2011, 2014 et 2020, le Hypersonic Technology Vehicle 2 , et le HCM X -51 Waverider. Un prototype de type AGM-183 ARRW développé par Lockheed Martin a été déjà testé sans succès en 2020. Puis en décembre dernier, un test du même prototype a été réalisé avec succès selon un communiqué du Président Biden.

L'**Inde**, ne semble pas en reste avec son test en 2022 de l'Agni V ICBM et de HGV-202F.

La **France** développe ses ASN4G, des missiles de croisière hypersonique (HCM) de type air-sol aéroportés par des chasseurs Rafales. Ce programme a été lancé depuis 2014 par l'ONERA et le missilier MBDA. L'ASN4G est attendu aux horizons de 2035. Par ailleurs, la France travaille également sur le développement d'un planeur hypervéloce de type VMAX confié à ArianeGroup. En outre, on compte aussi d'autres acteurs comme la DGA et THALES qui travaillent sur l'hypervélocité en France.

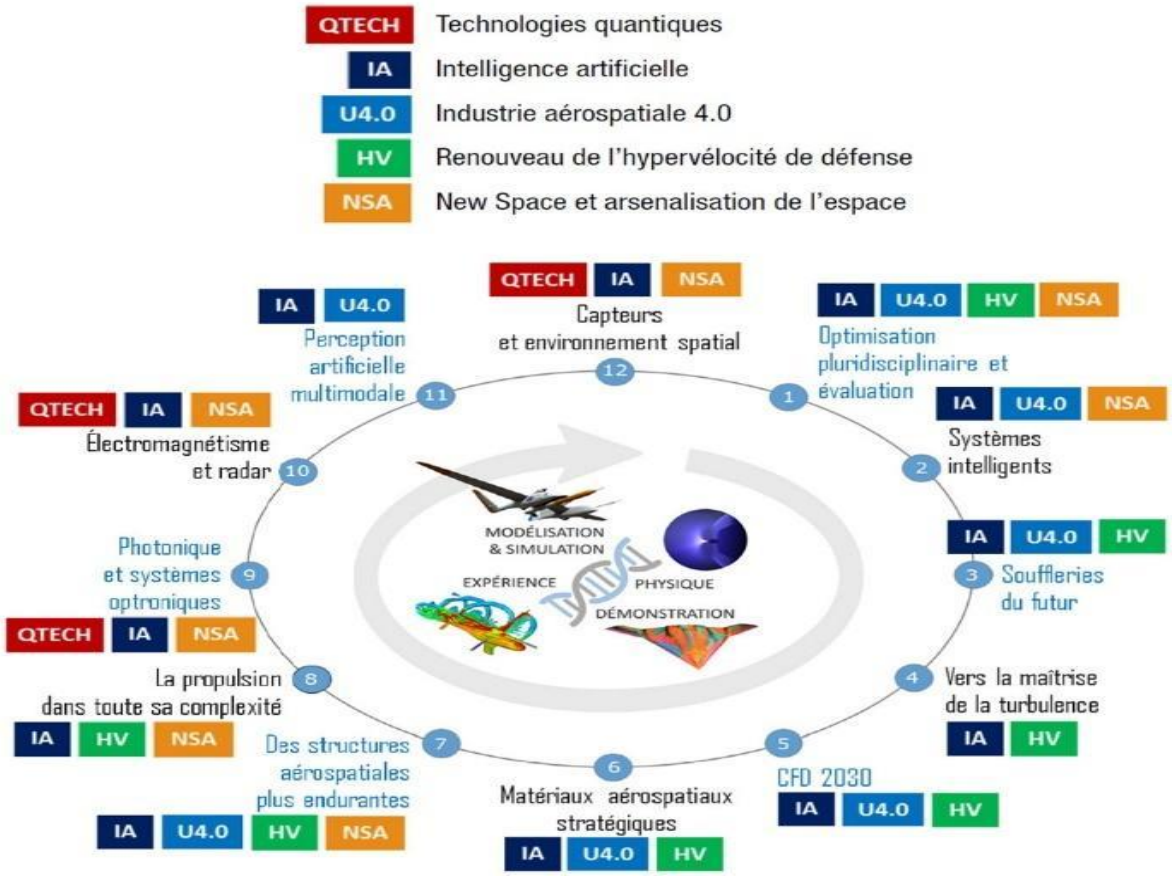
- **<u>Office National d'Études et de Recherches Aérospatiales (ONERA)</u>**

L'ONERA est un EPIC fondé en 1946 et ayant pour missions :

- De développer et d'orienter les recherches dans le domaine aérospatial.

- De concevoir, de réaliser, de mettre en œuvre les moyens nécessaires à l'exécution de ces recherches.
- D'assurer, en liaison avec les services ou organismes chargés de la recherche scientifique et technique, la diffusion sur le plan national et international des résultats de ces recherches.

En 2022, le budget de l'ONERA s'élevait à 266 Millions d'euros (dont 146 M€ de ressources propres et 110 M€ de subventions publiques) pour un effectif de 2123 collaborateurs. Depuis 2014, il est dirigé par Bruno SAINJON. Ci-dessous le plan stratégique de l'ONERA :



- **MBDA**

En France, MBDA est le fleuron dans les technologies balistiques, la production et la fourniture de systèmes de missiles et de contre-mesures opérationnelles. MBDA emploie 13000 personnes dans le monde pour un chiffre d'affaires de 4,2 Milliards d'euros (2021). Éric Béranger est son PDG.

MBDA est détenu par le groupe britannique BAE Systems (37,5 %), le franco-allemand Airbus (37,5 %), et l'italien Leonardo (25%).

Capacité de résilience en cas de crise

Entreprise multinationale, elle bénéficie *des contributions de ses filiales pour faire face à des crises pouvant impacter ses activités*. La grande quantité de contrats comme lui permettent de disposer de fonds solides qui la mettent dans les leaders de la BITD européenne.

Points forts

- ❖ Entreprise à l'internationale développée dans de nombreux pays
- ❖ Diversification de ses sous-traitants qui la rende résiliente face à des crises localisées
- ❖ Forte réputation à l'internationale par rapport à l'importance de ses contrats militaires français et étrangers

Points faibles

- ❖ Entreprise leader au niveau européen qui pourrait être la cible de prédation par des puissances étrangères.
- ❖ Les domaines RSE (Responsabilité Sociale des Entreprises) et ODD (objectifs développements durables pourraient être un angle d'attaque de la concurrence afin d'affaiblir et de ternir les activités de ce groupe à l'international. Une attention particulière peut être prise par le groupe dans ce domaine réputationnel.
- ❖ Forte dépendance aux composants électroniques étrangers qui pourraient retarder fortement les fabrications en cas de pénurie majeure.

- **Les énergies opérationnelles**

L'autonomie énergétique des Forces Armées Françaises sur ses théâtres d'opérations est un enjeu majeur. Que ce soit au niveau des bases militaires, des unités d'opérations ou même du soldat déployé, l'idée est de les rendre moins dépendants des approvisionnements extérieurs qui nécessitent des soutiens logistiques conséquents et qui peuvent être perturbés dans des environnements plus ou moins instables.

La France dispose d'un service d'énergie opérationnel dit SEO qui a pour mission :

- L'achat et la cession des produits pétroliers à travers un compte de commerce
- La mise à disposition de la ressource pétrolière au plus près du besoin, quels que soient le lieu et le délai impartis, à partir de contrats passés par les acheteurs du SEO en France ou localement sur les théâtres d'opérations ;
- Les transports amont (boucle arrière) et aval (boucle avant), optimisés en termes de coûts, de sûreté et de sécurité ;
- Une maîtrise de la « qualité produit » grâce à un ensemble de procédures reposant sur des analyses menées tout au long de la chaîne de stockage et de distribution ;
- La continuité du soutien des Forces, justifiant l'entretien de stocks réservés utilisables en situation de crise.

Les opérations de ravitaillement des aéronefs (de l'Armée de l'air et de l'espace, de la Marine Nationale et de l'ALAT) sont réalisées avec les moyens organiques du SEO en raison des enjeux liés à la sécurité des vols et des contraintes inhérentes à la maîtrise de la qualité des carburants (carburéacteurs, essence aviation). De même, le Service assure dans les dépôts de Brest et de Toulon l'avitaillement des navires de la Flotte et des moyens aéronavals embarqués (niveau 1).

En revanche, le ravitaillement des véhicules et engins terrestres relève du SCA (stations-service des GSBdD) et de l'Armée de terre (Brigade logistique et Régiments) et de l'Armée de l'air et de l'espace (EDSA), le SEO n'assurant que le niveau 2 amont.

Par ailleurs il existe d'autres solutions technologies et énergétiques modernes susceptibles d'octroyer un avantage stratégique aux forces armées françaises en théâtres d'opérations.

- **Solution n°1 : Les SMRs mobiles ou Petits Réacteurs Modulaires mobiles**

Il s'agit de solutions qui contribuent dans une certaine mesure à la lutte contre le dérèglement climatique. Les SMRs sont des centrales nucléaires miniaturisées et simplifiées, adoptées il y a une dizaine d'années par la France au travers de son programme « NuwardTM ».

Des premiers travaux engagés de façon synergique par EDF, Naval Group, Le CEA et TechnicAtome. L'ambition de ce programme est de produire des versions beaucoup plus réduites et transportables au moyen de véhicules militaires dont disposent les Forces Armées Françaises. Cette solution semble être plus adaptée que les groupes électrogènes grâce à une autonomie supposée quasi éternelle.

- **Solution n°2 : Les batteries portables au Lithium par PKTRONICS**

PKTRONICS est un groupe français spécialisé dans la fabrication de batteries et autres solutions énergétiques à usage militaire. L'idée ici est de développer des batteries à usage unique ou rechargeables, surtout "empochables" dans les gilets militaires avec une autonomie maximale.



- **<u>Naval Group</u>**

Naval Group est un groupe industriel français spécialisé dans la construction navale de défense et le développement de solutions énergétique à usage civil et militaire. Le groupe emploie plus de 15 000 personnes et est présent dans 18 pays. L'entreprise est détenue principalement à hauteur de 62,49 % par l'État français et de 35 % par Thales (Français). Naval Group est dirigé par le Français Pierre Eric Pommellet. Depuis 2021, le groupe se recentre sur ses activités navales. Naval Group se positionne aussi comme un innovateur en proposant une large gamme de solutions dans l'énergie nucléaire civil et les énergies marines renouvelables. Les connaissances développées par Naval Group dans le domaine de la propulsion de systèmes navals permettent au groupe de développer des solutions dans le nucléaire civil. Il collabore ainsi avec EDF, le CEA et Areva à la construction des centrales EPR et à l'entretien de centrales nucléaires.

<u>Dépendance supply chain à l'étranger</u>

Naval Group possède des bureaux de représentation en Australie, Arabie saoudite, au Chili, aux Émirats arabes unis, en Grèce, en Inde, en Indonésie, en Malaisie, en Norvège et au Pakistan. Le groupe est également présent dans le monde à travers des filiales et joint-ventures, qu'elle possède exclusivement ou en association avec d'autres entreprises. Cette entreprise au vu de ses implantations multinationales dépend fortement de ressources fragilisés par les crises actuelles (matières premières : métaux, électronique, etc .). Sa diversification d'origine internationale de fourniture en matières premières lui permet une excellente résilience. A l'international, le groupe naval a bénéficié *"des bonnes contributions du Brésil et de l'Australie"*. Dans les services, les programmes de modernisation du porte-avions Charles de Gaulle et l'adaptation au

missile M51 du sous-marin nucléaire lanceur d'engin Le Téméraire ont été les principaux contributeurs du chiffre d'affaires.

Capacité de résilience en cas de crise

Entreprise à l'international, le groupe naval bénéficie *des bonnes contributions de ses filiales (exemple Brésil et Australie) pour faire face à des crises pouvant impacter ses activités*. La grande quantité de contrats comme dans les programmes de modernisation du porte-avions Charles de Gaulle et l'adaptation au missile M51 du sous-marin nucléaire lanceur d'engin Le Téméraire lui permettent de disposer de fonds solides qui la mettent dans les leaders de la BITD européenne.

Points forts

- ❖ Entreprise à l'internationale développée dans de nombreux pays.
- ❖ Diversification de ses sous-traitants qui la rende résiliente face à des crises localisées.
- ❖ Forte réputation à l'internationale par rapport à l'importance de ses contrats militaires français et étrangers.

Points faibles

- ❖ Entreprise leader au niveau européen qui pourrait être la cible de prédation par des puissances étrangères
- ❖ Les domaines RSE (Responsabilité Sociale des Entreprises) et ODD (objectifs développements durables pourraient être un angle d'attaque de la concurrence afin d'affaiblir et de ternir les activités de ce groupe à l'international. Une attention particulière doit être prise par le groupe dans ce domine réputationnelle

Technologie Cloud

- **Présentation et rôle dans le domaine militaire**

Dans le document "Ambition numérique du Ministère des armées" (novembre 2017), le Ministère des Armées définit ses objectifs stratégiques en matière de transformation numérique. Le *Cloud computing* correspond à un modèle de mise à disposition de ressources informatiques en tant que services infogérés et disponibles à la demande. Son intérêt principal est de déléguer les fonctions de conception, d'hébergement et d'exploitations des systèmes informatiques à un tiers dont c'est le cœur de métier, en capacité de gérer les problématiques d'échelles et d'optimisation des ressources informatiques. L'induit majeur de ce concept d'informatique en nuage est que les données manipulées sont irrémédiablement captives du fournisseur de services *cloud*.

Le Cloud est identifié un maillon essentiel dans l'atteinte de la supériorité opérationnelle sur les théâtres d'opérations en permettant notamment le traitement des données issues des nouvelles technologies et capables d'apporter un avantage informationnel : combat collaboratif, systèmes autonomes, aide à la décision, applications d'IA etc. Son rôle stratégique pour l'armée est également mis en évidence dans le rapport d'information de l'Assemblée Nationale portant sur les enjeux de la numérisation des armées : l'exemple du DOD américain, qui a initié une transition vers le Cloud est par exemple cité, avec une approche reposant d'une part sur des moyens civils (Contrat JEDI) et une approche propre de sécurisation des données.

Au-delà des aspects de gestion de la donnée (tant administrative qu'opérationnelle), l'usage du Cloud sur le théâtre des opérations dans sa fonction combattante trouve une application directe dans le "Cloud tactique" ou "Cloud de combat". La Fondation Pour la Recherche Stratégique image le cloud tactique comme la fonction de "pousser jusqu'au cockpit les capacités les plus avancées de nos réseaux numériques, selon les technologies des

cloud commerciaux, afin de renforcer l'efficacité, l'efficience et la résilience de la puissance aérienne dont il transformera les fonctions opérationnelles". En ce sens, le cloud tactique est un composant essentiel du Système de Combat Aérien du Futur (SCAF). L'enjeu est de pouvoir manipuler à des fins de supériorité informationnelle l'ensemble des données générées par les capteurs déployés sur le champ de bataille, soit un afflux constant et massif de données de nature très diverses.

Dans « Le cloud défense : défi opérationnel, impératif stratégique et enjeu de souveraineté », Focus stratégique, n° 107, Ifri, novembre 2021, Clotilde Bômont explicite les défis associés qui distinguent l'usage du cloud tactique militaire par rapport à l'usage conventionnel du cloud civil :

- Le déploiement en environnement hostile, ou contraint, induisant un impact direct sur la sécurité des données.
- La connectivité limitée sur certaines zones d'opération, réduisant les capacités d'échange même de données, et particulièrement dans des contextes de guerre électromagnétique (brouillage).
- Le besoin de mobilité de l'équipement.
- L'interopérabilité des systèmes entre les différentes armées et les différents systèmes de cloud.

Le passage au cloud dans les armées n'est pas sans risque. La principale vulnérabilité réside évidemment dans la menace des cyber-attaques et compromission de données. En déléguant des fonctions de conception, d'hébergement et d'exploitation de systèmes informatiques à un tiers, le ministère des Armées devient irrémédiablement captif du fournisseur de services *cloud* et de ses capacités à sécuriser ses infrastructures.

Aujourd'hui, les principaux fournisseurs de services Cloud sont américains (AWS, Microsoft, Google, Oracle) et chinois (Alibaba Cloud). En France, des initiatives dites hybrides reposant sur des solutions américaines mais opérées par des infogérants nationaux ont vu le jour, mais celles-ci montrent rapidement leurs limites. En termes de souveraineté et de protection des données vis-à-vis des Etats-Unis (Cloud Act), les entreprises françaises s'exposent sur les plans juridique et technique. Dans ce contexte, il apparaît nécessaire de s'appuyer sur des acteurs et solutions souveraines pour que les ambitions du ministère des Armées soient atteintes en termes de numérique et de souveraineté (Scaleway, Outscale, OVH, GAIA-X demain).

OVHCloud

OVHCloud est une entreprise française fondée en 1999. Elle est le leader français du secteur et un acteur de poids sur le marché européen, où continuent de dominer les opérateurs américains. Ses activités historiques incluent l'hébergement de serveurs et la fourniture d'accès Internet. Elle compte environ 2 700 salariés pour un chiffre d'affaires de plus de 500 M€. Cotée en bourse depuis 2021, l'entreprise possède plusieurs filiales et implantations à l'international et gère 33 datacenters sur 4 continents.

Elle est contrôlée par un consortium réunissant les membres de la famille fondatrice (famille Klaba), qui détient environ 70% du capital et des droits de vote. Deux fonds américains détiennent chacun près de 8% de la société, avec un capital flottant en bourse de près de 12,5%. La société ne dépend donc pas significativement de puissances étrangères (famille et dirigeants majoritairement français), et n'est pas particulièrement exposée à une prise de contrôle hostile de type OPA. L'extension de capital grâce à des fonds américains s'inscrit dans une logique cohérente de développement à l'international, notamment en Amérique du Nord.

OVHCloud maîtrise l'ensemble des étapes de production, de la fabrication des baies de serveurs (incluant l'assemblage des composants informatiques) jusqu'à la mise à disposition des ressources informatiques via les datacenters, ce qui constitue un avantage concurrentiel sur le marché. L'approvisionnement en composants clés (puces, semi-conducteurs notamment) reste toutefois un point de vigilance important.

Ses dirigeants se montrent sensibles aux enjeux d'intelligence économique, notamment sur l'extraterritorialité du droit américain (filiale locale): la structure juridique d'OVHCloud reflète une séparation des activités strictes entre les filiales européenne et américaine afin d'y circonscrire la zone d'application aux seuls Etats-Unis. OVHCloud contribue par ailleurs à des initiatives liées à la souveraineté des données : rédaction du livre blanc « Protéger ses données et services stratégiques dans le cloud : enjeux, principes et solutions »), et participation à l'initiative de développement d'infrastructure Cloud européenne sécurisée et fiable, GAIA-X.

OUTSCALE

Outscale est une entreprise française fondée en 2010, également spécialisée dans le Cloud et filiale de Dassault Systèmes, créée afin de répondre à la problématique de souveraineté des données. Elle compte aujourd'hui un peu moins de 200 salariés pour près de 40M€ de chiffre d'affaires.

Elle se positionne uniquement sur le segment « *Infrastructure As A Service* », c'est à dire le socle de base permettant la mise à disposition de systèmes d'exploitation et l'orchestration de ressources associées et la création de solutions type (« *Platform As A Service* », et « *Software As A Service* »). Outscale développe à cet effet son propre système d'exploitation sur la base notamment de briques Open-Source.

En tant que filiale du groupe Dassault, elle joue un rôle auprès d'autres industriels du secteur de la Défense et est déjà sensible aux enjeux d'intelligence économique et de souveraineté. Outscale participe également à l'initiative en projet de développement d'infrastructure Cloud européenne sécurisée et fiable, GAIA-X.

- **Contribution à l'émergence de solutions souveraines et sécurisées d'hébergement**

OVHCloud et Outscale contribuent à la stratégie de souveraineté impulsée par l'ANSSI, l'agence nationale française de cybersécurité, au travers de la mise en conformité de services d'hébergement avec le référentiel Cloud de confiance (SecNumCloud) : celle-ci garantit aux utilisateurs des services qualifiés respectant un certain nombre d'exigences qui contribuent à la sécurité du traitement de la donnée.

- **Limitations dans le développement économique du Cloud**

Le rapport de KPMG *« Le Cloud européen : de grands enjeux pour l'Europe et cinq scénarios avec des impacts majeurs d'ici 2027-2030 »* éclaire sur les difficultés à développer un Cloud européen pérenne. Ce marché est dominé par trois « *hyperscalers* » américains, et la grande majorité (~70 %) des dépenses d'infrastructures cloud des entreprises européennes est captée par des fournisseurs de cloud non-européens.

L'offre souveraine est jugée trop limitée : "les fournisseurs internationaux dominent le marché grâce à des pratiques d'acquisition client agressives » auxquelles s'ajoutent « des conditions complexes de sortie" qui rendent captifs le client. Et sans réelles possibilités de négociation des conditions contractuelles. Ces facteurs impactent fortement les opportunités de croissance d'hébergeurs nationaux comme OVH et Outscale.

- **Intrants vulnérables**

Outscale ou OVHCloud (comme toute la filière Cloud) dépendent directement ou indirectement de l'approvisionnement en micro-processeurs et puces électroniques, qui sont fabriqués par de grands industriels américains (Intel, AMD) ou asiatiques (TSMC).

La crise du Covid-19 a mis en lumière cette dépendance accrue en l'absence de constructeurs européens majeurs, et déclenché le lancement du European Chips Act : le plan de relance de l'Europe pour regagner son autonomie stratégique dans le domaine. OVHCloud documente d'ailleurs ce risque dans son document d'enregistrement auprès de l'AMF à l'occasion de son entrée en bourse en 2021.

Intelligence Artificielle et champ de bataille

« Celui qui deviendra leader en ce domaine sera le maître du monde » disait Vladimir Poutine en 2017.

Présentation de la technologie et son rôle dans le domaine militaire

L'Intelligence Artificielle (IA) peut être définie comme un ensemble d'algorithmes conférant à une machine des capacités d'analyse et de décision lui permettant de s'adapter intelligemment aux situations en faisant des prédictions à partir de données déjà acquises. Les applications possibles sont multiples dans les domaines économique, médical, informatique et militaire.

« La croissance de la puissance de calcul, la disponibilité des données et les progrès réalisés dans les algorithmes ont fait de l'IA l'une des technologies les plus stratégiques du XXIe siècle. Les enjeux ne sauraient être plus élevés. Notre approche de l'IA définira le monde dans lequel nous vivons. ». Par cette déclaration (début 2018), la Commission Européenne montre que l'Europe se saisit du sujet après les ambitions affichées par la Chine, la Russie et les États-Unis. En effet, l'IA permet des gains substantiels de compétitivité ou de productivité dans tous les secteurs de l'économie et dans les services publics. La science des données, l'apprentissage machine et la robotique forment ainsi la matrice de la « 4° révolution industrielle ».

Le gouvernement français s'est lancé dans une stratégie nationale pour l'IA afin de faire émerger des talents et d'accélérer la R&D dans la filière Ainsi, en 2019, la ministre des armées Florence Parly soulevait la question de l'IA dans l'armée française. La France a choisi de donner à ses armées les moyens de mener à bien leurs missions dans un environnement opérationnel de plus en plus difficile, l'IA faisant l'objet d'une compétition stratégique entre puissances technologique, économique et militaire. Malgré ses efforts, l'armée française accuse un retard important contre les 3 puissances dominantes, et alors que l'IA s'apprête à révolutionner le champ de bataille.

Certains s'interrogent sur la disparition progressive des Etats-Majors au profit de l'IA, capable de mieux appréhender les milliers de paramètres qui influent sur le champ de bataille en temps réel. Aujourd'hui, la technologie ne permet pas encore la création d'une IA « forte », autonome et polyvalente, pouvant supplanter la totalité des capacités cognitives humaines des états-majors militaires. Cependant, après une maturité suffisante, elle pourrait devenir un véritable atout et même minorer les vulnérabilités militaires. On peut ainsi souligner 4 grands principes qui sont suivis par les armées françaises dans ce domaine :

- Liberté d'action et interopérabilité: afin de maintenir la supériorité face à tout type d'adversaire, il s'agit d'intégrer, dès à présent, des modules IA dans les SIOC tout en s'assurant de rester interopérables avec les alliés

- IA de confiance, maîtrisée et responsable: combiner jugement humain et puissance des algorithmes pour décider et agir avec clairvoyance dans des tempos opérationnels toujours plus élevés
- Résilience et évolutivité : la robustesse, la résilience sans connexion et l'évolutivité des algorithmes, doivent être pris en compte dès la phase de conception

- Cœur de souveraineté : alors que l'écosystème mondial de l'IA est dominé par des acteurs étrangers, le maintien d'un cœur de souveraineté technologique est indispensable.

Les domaines d'application sont vastes et les apports de l'IA au sein des armées est très prometteuse. Contribuant au processus de réflexion des états-majors (Observation, Orientation, Décision, Action), l'IA accélérerait le cycle opérationnel en aidant à mieux maîtriser le tempo des opérations et à renforcer la performance et l'agilité du C2.

De plus l'IA est d'une redoutable efficacité pour analyser l'environnement des opérations, en planification comme en conduite. Nourrie par l'abondance des données en sources ouvertes, elle excelle dans l'analyse systémique qui combine de multiples domaines : militaire, économique, logistique, politique, idéologique, social.

Dans le domaine du renseignement, les données OSINT pourraient être recoupées automatiquement et instantanément, améliorant la connaissance de l'adversaire et le suivi en temps réel de son évolution. La reconnaissance d'images et l'analyse comportementale (infrastructures et équipements, troupes) permettent de détecter des activités particulières et de fournir du renseignement précieux.

Enfin l'IA est déjà utilisée en simulation constructive à des fins de préparation opérationnelle des état-major. Dans l'armée de Terre, le système SOULT (Simulation pour les Opérations des Unités interarmes et de la Logistique Terrestre), permet de simuler un affrontement terrestre et son impact sur des unités qui suivent des principes militaires bien connus. Son usage pourrait être étendu à la conception de la mission réelle en cours.

La maintenance des matériels militaires offre aussi un champ d'application intéressant, de manière prédictive, périodique ou après une panne. Elle mobilise un volume de pièces important, y compris en déploiement opérationnel, et du temps pour que les techniciens réalisent des opérations de contrôle d'usure et de maintenance. L'objectif de la maintenance prédictive est d'exploiter les données enregistrées par les matériels puis d'utiliser l'IA pour déterminer, à l'avance, le moment optimum auquel une pièce doit être changée.

La France possède une stratégie claire en matière d'IA, présentée dans le rapport de la Task-Force IA, qui a défini une feuille de route ministérielle et des principes directeurs pour une IA de défense maîtrisée. Sept axes d'efforts sont prioritaires : aide à la décision en planification et en conduite, combat collaboratif, cyberdéfense et influence, logistique, soutien et maintien en condition opérationnelle, renseignement, robotique et autonomie, administration et santé.

La France dispose de talents et de pépites pour développer, dès à présent, des savoir-faire dans ce vaste domaine. Impulsées par l'Agence de l'innovation de Défense (AID), les premières initiatives commencent à voir le jour au sein des armées françaises dans plusieurs domaines : ressources humaines, maintenance, formation et même au cœur du commandement des opérations. Une technologie essentielle pour accroître la souveraineté du pays dans tous les domaines.

Preligens

Créée en 2016 par deux ingénieurs français, Arnaud Guérin et Renaud Allioux, la société utilise l'IA pour automatiser l'analyse de données multi-sources des professionnels du renseignement et orienter les analystes vers des événements inhabituels nécessitant leur expertise. Depuis sa création, Preligens a levé 23 millions d'euros, signé des contrats avec 5 pays et agences internationales. L'entreprise compte aujourd'hui plus de 150 employés et a ouvert des filiales au Royaume-Uni, aux États-Unis, en Allemagne, en Belgique et à Singapour. Elle travaille notamment avec la DRM dans le cadre des études d'analyses d'images d'origine satellitaire (GEOINT, IMINT). Elle a réalisé un chiffre d'affaires de plus de 6 millions d'euros en 2022.

Concrètement, Preligens développe des logiciels, algorithmes et outils dans le domaine de l'observation et de la surveillance par satellite ou autres moyens aéroportés incluant, mais non limités aux Drones, avions, ballons sondes pour des missions d'observation et de surveillance d'infrastructures industrielles ou militaires.

Dépendance supply chain à l'étranger

Preligens s'appuie sur une architecture de serveurs sécurisés accrédités par l'ANSSI et ce afin d'assurer la sécurité des données et limiter la dépendance aux acteurs du marché informatique international.

Capacité de résilience en cas de crise

La société diversifie ses achats de matériels et composants informatiques pour ne pas dépendre d'un seul fournisseur. Elle multiplie par ailleurs les serveurs de sauvegardes afin de limiter l'impact d'attaques Cyber. Par ailleurs, elle se dote d'une Politique de protection informatique très stricte afin de limiter les retombées sur les activités de l'entreprise. Enfin, une grande partie des données récoltées et des analyses fournies sont classifiées afin de limiter l'accès à des ayants droits préalablement identifiés.

Points forts

- Capacité d'innovation importante grâce aux nombreux clients au niveau mondial (5 pays) et à sa R&D interne.
- Forte capacité à trouver de nouveaux marchés grâce à l'excellente des programmes proposés.
- Recrutement de Grégoire de Saint-Quentin, ancien GCOS comme SVP Advanced Projects, qui fait bénéficier la société de son expertise et de son réseau dans la sphère sécuritaire et renseignement.
- Travail actuellement avec de nombreux services de renseignement français et étrangers. Efficacité des applications de reconnaissance reconnues.

Points faibles

- Dépendance aux matériels informatiques non français.
- Vulnérabilité aux menaces provenant du cyberespace.
- Forte consommation d'énergie pour alimenter l'ensemble des machines.
- Développement des activités de l'entreprise à l'étranger impliquant une augmentation de son exposition aux vols de données par d'autres pays.
- Entreprise utilisant des données militaires classées. Le danger d'un rachat par une entreprise étrangère pourrait créer des vulnérabilités.

ATHEA

ATHEA est une joint-venture créée autour de deux groupes français leaders mondiaux des hautes technologies, Thales et Atos en 2021. Cette société a développé une plateforme souveraine associant traitement de données massives et intelligence artificielle pour les secteurs de la défense, du renseignement et de la sécurité intérieure et qui s'adresse tant aux acteurs publics que privés. Dirigée par Philippe GASC, elle a réalisé un chiffre d'affaires de plus de 20 millions d'euros en 2022.

La Société a pour objet, en France et à l'étranger, les activités de création, définition et validation d'actifs technologiques et de services informatiques, consistant en la création et l'exploitation d'infrastructures informatiques spécialisées, la création, la définition et la validation d'un produit commun nouveau de traitement « big data » souverain, comprenant une infrastructure, une « infostructure », des cas d'usage et des applications clients.

Athéa met à disposition du client le support nécessaire pour l'analyse de données massives au travers d'algorithmes d'intelligence artificielle. Les solutions développées par ATHEA comprennent alors l'ingestion (connexion à tout type de source donnée), le traitement (processing) et le stockage (data lake) des données multi-sources et multiformes.

Applications militaires sur champ de combat

Responsabilité du ministère des Armées (DGA, DRM) : différents champs d'application en maturité (DRM) ou en prospective (SSA, maintenance, etc), et différents portages (installation lourde, embarquée).

Dépendance supply chain à l'étranger

Athea s'appuie sur une architecture de serveurs sécurisés accrédités par l'ANSSI (label secNumCloud) et localisés en France, ce afin d'assurer la sécurité des données et limiter la dépendance aux acteurs du marché informatique à l'international.

Capacité de résilience en cas de crise

ATHEA dispose d'une culture de sécurité forte issue de Thalès et ATOS. Nous relevons les éléments suivants :

- Couche de sécurité apposée sur la donnée par labellisation, permettant d'assurer un contrôle renforcé de l'accès à la donnée.
- Diversification des achats de matériels IT.
- Multiplication des serveurs de sauvegardes afin de limiter l'impact d'attaques Cyber
- Politique de protection informatique très stricte.
- Classification des données afin de limiter les ayants droits.

Points forts

L'entreprise rencontre un vif succès commercial et peut s'appuyer sur les éléments suivants :

- JV entre grands leaders de l'industrie de défense française.
- Capacité d'innovation et R&D importante grâce à l'appui des sociétés du groupe.
- Capacité à trouver des marchés en France et en Europe grâce à son excellente réputation et à la base client ATOS et Thalès.

Points faibles

Nous relevons néanmoins des points de vigilance :

- Dépendance des matériels informatiques non français.
- Vulnérabilité aux dangers du cyberespace car cible de très fort intérêt.

Informatique quantique

L'informatique quantique offre de belles promesses pour les gouvernements et entreprises. Si le domaine d'étude n'est pas nouveau (R. Feynman dès 1982, algorithme de Shor, 1994), ses avancées récentes ont provoqué un regain d'intérêt alors que les applications pratiques se démocratisent. Sur le plan militaire, ses apports pourraient s'avérer décisifs pour casser les codes ennemis et sécuriser ses propres communications. La capacité du quantique à apporter une suprématie totale en fait un sujet de premier ordre pour les armées.

Nous pouvons en retenir la définition d'IBM : "*une technologie qui exploite les lois de la mécanique quantique (le comportement des particules à un niveau microscopique) pour résoudre des problèmes trop complexes pour les ordinateurs classiques.*" Son unité de mesure, le Qubit, varie de l'unité informatique traditionnelle, le bit, en ce qu'il peut prendre une infinité d'états entre 0 et 1, offrant des capacités de calcul parallélisées exponentielles.

Plusieurs méthodes de calcul quantique sont actuellement en concurrence :

❖ **Supraconducteurs** à base de silicium (Iiria, Alice & Bob, Intel, IBM, Google, CEA-Leti) ou de graphène, qui pose des questions sur les approvisionnements en terres rares. Si le silicium est très répandu, le gallium, issu de mines de bauxite, est plus rare et peu extrait en France.

❖

❖ **Ions piégés** (Honeywell, IonQ), moins plébiscitée et qui pose la question d'autres terres rares, mais où le leadership européen de l'Autriche dans ce domaine pose des enjeux de souveraineté moins cruciaux.

Applications

Les applications de l'informatique quantique sont nombreuses dans le domaine scientifique et nécessitent des capacités dites HPC (Calcul de Haute Performance): cryptographie, IA, prévisions financières, météo, énergie, sciences des matériaux, spatial, télécommunications, santé (médecine personnalisée et biologie notamment).

Sur le plan militaire, le quantique soulève de nouveaux enjeux que les armées se doivent d'explorer dans leurs domaines d'activité traditionnels : simulations nucléaires, communications sécurisées (cryptographie post-quantique), planification et conduite des opérations (scénarios de guerre et de stratégie selon des milliers de paramètres temps réel), détection (guerre navale et sous-marine, spatial, aérien, balistique), navigation :

■ **Navigation**: Accéléromètres, magnétomètres et gravimètres quantiques pourraient répondre à la dépendance des systèmes de navigation critiques à l'égard du GPS, qui peuvent être brouillés ou usurpés. Un avion pourrait faire un vol transocéanique et arriver à destination avec une précision de quelques mètres sans utiliser le GPS.

■ **Interception électromagnétique**: Les capteurs à base d'impuretés dans le diamant pourraient permettre de réaliser des analyses spectrales des signaux électromagnétiques de plusieurs ordres de grandeurs plus fines que les technologies actuelles. Dans un contexte de guerre électronique, ces dispositifs pourraient multiplier les performances des systèmes d'interception.

■ **Télédétection**: Le radar quantique est une technologie de télédétection émergente fondée sur l'illumination quantique qui permettrait de détecter les avions furtifs, de filtrer les tentatives délibérées de brouillage et de fonctionner dans des zones où le bruit de fond est élevé.

Place de la France

Plusieurs puissances de première importance scientifique et militaire sont en course : Etats-Unis, Canada, Grande-Bretagne, France, Allemagne, Suisse, Russie, Chine, Israël, Japon et Inde dans une moindre mesure.

Si le bassin d'emploi est relativement faible (16.000 à horizon 2030), les budgets commencent à devenir assez conséquents (autour de 30 Milliards de dollars en 2022).

La France s'est ainsi dotée d'une "stratégie nationale d'accélération quantique", portée par Neil Abroug, au sein du SGPI rattaché à Matignon. Celle-ci prévoit une enveloppe de 1,815 milliards d'euros et une régionalisation des efforts autour de pôles d'excellence : Saclay, Grenoble (QuantAlps), Occitanie, Strasbourg, Bordeaux. Les acteurs sont issus du monde public (CEA, CNRS, INRIA, ANR, ANSSI, OPECST, Matignon, DGA/AID) et privé (TOTAL, Airbus, EDF et ATOS, Thalès, SOITEC, STMicroelectronics, Orano, Air Liquide, concours d'acteurs plus petits).

Par ailleurs, l'un des enjeux du quantique repose sur la maîtrise et la souveraineté de technologies "habilitantes" (cryostats, lasers, ultravide, matériaux supraconducteurs etc.) pour faciliter leur déploiement. La France compte un leader mondial (Air Liquide) et des ETI et PME bien positionnés sur ce créneau (iXblue, Alice & Bob, SOITEC, Syrlink, AUREA Technology, PASQAL, Quandela etc.) qui, en fournissant les assembleurs de calculateurs quantiques ou en construisant le leur, fournissent directement ou indirectement les armées françaises.

Sur le plan militaire, le quantique est identifié comme une priorité par l'Etat-Major de l'Armée de Terre et le SGDSN dans des livres blancs distincts. A ce titre, la protection des opérateurs privés apparaît absolument nécessaire pour conserver une souveraineté nationale dans la filière. Si certaines entreprises sont soumises à un contrôle strict des investissements étrangers par Bercy, d'autres rentrent directement dans la BITD française, dont la DRSD assure le suivi et la protection (espionnage, normes et standards, M&A agressif). L'ANSSI est également prépondérante sur le volet cybersécurité. Assurer le maintien en conditions opérationnelles des équipements par la sécurisation des approvisionnements en matières premières est donc une priorité. Toutefois, ces technologies habilitantes sont nombreuses, et il apparaît difficile pour la France d'assurer seule sa souveraineté dans tous les segments concernés.

Au risque, sinon, de se retrouver dans la position de l'Allemagne, qui accueille à bras ouverts IBM et D-Wave (Canada) dans ses laboratoires de recherche, faute de capacités propres.

Enfin, sur la partie logicielle, la souveraineté française n'apparaît pas particulièrement à risque dans la mesure où d'une part, la Recherche française dispose de ses propres capacités, et d'autre part que la plupart des algorithmes fondateurs sont en open source et donc librement accessibles.

Cryptographie (post)-quantique

Parmi les différentes applications militaires au quantique, celui de la cryptographie (cryptage, déchiffrement) et donc de la sécurité des communications, ressort comme l'enjeu majeur. Pour construire des solutions suffisamment robustes et avancées, les opérateurs doivent s'appuyer sur les qubits photons, sur lesquels la

France semble accuser un certain retard. L'algorithme de cryptographie le plus utilisé au monde dans les protocoles de chiffrement, le RSA, est ainsi menacé par les technologies quantiques, et la solution pourrait être pour la France de développer sa propre Quantum key distribution (QKD), ou au niveau européen a minima.

"*A plus long terme, la France pourrait envisager de proposer, dans les 5 ans, la première solution de distribution quantique de clés de chiffrement, déployable à coût d'infrastructures marginal et résistant aux attaques par canaux auxiliaires et par déni de service (rapport Forteza)"* selon Olivier Ezratty. *"Le club très fermé des pays dotés de la technologie pourrait décider d'interdire l'exportation des machines les plus performantes. Une telle rétention technologique offrirait à ces pays des gains de plusieurs points de leur balance commerciale et de leur PIB, tandis que le reste du monde se trouverait sous la menace d'une compromission généralisée de ses communications avec l'obligation de déployer dans l'urgence des moyens de chiffrement plus sûrs. Elle pourra également s'affirmer comme la première nation à disposer d'une filière complète productrice de Si 28 industriels pour les besoins de la production de qubits sur Silicium."*

Risques principaux

Les entreprises françaises en pointe dans ce domaine attirent l'attention de plus gros acteurs ou d'acteurs étrangers avec des intentions parfois masquées. ATOS est par exemple sujet à des tentatives d'OPA hostiles de la part de DxC et de fonds britanniques, et même de grands groupes français. La start-up Muqans a quant à elle été rachetée par iXblue, un autre acteur français.

La capacité des entreprises françaises du secteur à atteindre une taille critique n'est donc pas suffisante et la filière doit pouvoir compter sur la vigilance des opérateurs de l'Etat spécialisés en intelligence économique pour éviter la perte de technologies et de savoir-faire clés.

La souveraineté passe aussi par la maîtrise de l'approvisionnement en matières premières critiques. Ainsi, Orano annonçait en 2021 se lancer dans la production d'isotopes rares (silicium 28), indispensables pour les qubits silicium, jusqu'à présent approvisionnés par la Russie. Air Liquide annonçait en décembre 2021 un contrat d'approvisionnement en hélium 3 au Canada sur 10 ans (gaz indispensable pour les cryostats à dilution dans les processeurs quantiques). Côté logiciel, la France dispose de capacités propres grâce à un haut niveau académique mais compte moins de 10 acteurs de référence dans le domaine, souvent de petite taille (startups).

Côté hardware, la France compte des acteurs de belle taille dans la photonique (Azur Light Laser Systems), le câblage (Radiall, Atem) ou les modules HSM (ATOS), utilisés pour le cryptage de données. Dans le cas d'une guerre à haute intensité, le risque porte donc sur la capacité des acteurs privés servant les armées à assurer leurs approvisionnements, en matière premières (terres et métaux rares) ou en composants de haute technologie (semi et supra-conducteurs, puces). En cas de cyberattaque majeure, le risque porte sur la capacité de ces acteurs à protéger leurs secrets techniques (codes source, résultats, projets, ressources et moyens).

Le cas d'ATOS

Parmi les entreprises françaises actives dans le quantique, ATOS est de loin l'acteur le plus important en France. Groupe de 110.000 employés, de 11,7 milliards € de CA, dont 542 M$ sur le HPC ; 3ème acteur mondial derrière Lenovo et HPE, et fabricant du supercalculateur Leonardo et des modules HSM. Il occupe ainsi une place quasi-

systémique dans la filière industrielle quantique française, grand donneur d'ordre auprès de PME et ETI spécialisées (lasers, ultravides, cryogénie, puces) et fournisseur pour de grands groupes privés, laboratoires publics et des armées au côté du CEA-Leti.

Ainsi, cette entreprise doit faire l'objet de toutes les attentions de la part des autorités car une perte de savoir-faire et technologies clés aurait des impacts en cascade sur tout l'écosystème quantique français et rendrait la France dépendante d'autres pays et d'entreprises étrangères dans un domaine d'avenir aux applications militaires de première importance. ATOS est par ailleurs un membre important de GAIA-X au niveau européen et fournit de grands industriels de défense cherchant à se défaire de l'extra-territorialité du droit américain.

Nous relevons ainsi des tentatives d'OPA hostiles sur le groupe, fragilisé financièrement par un contexte difficile et une structuration de son capital défavorable (flottant à 97%). La restructuration en cours du groupe (qui accusait 3 milliards € de pertes en 2021), amènera à une scission en deux entités, Evidian et New Atos, qui risque de le fragiliser d'autant plus. Mené par une direction bicéphale, qui génère de l'inertie, ATOS va par ailleurs perdre en taille critique, ce qui le met davantage à la merci de concurrents plus importants ou d'acteurs aux intentions hostiles. Dans ce contexte, l'agence de notation Standard & Poors a jugé que l'investissement dans les titres d'Atos était devenu spéculatif, abaissant sa notation de BBB+ à BB. Le titre perdait 80% en bourse en 2021, le rendant davantage vulnérable.

Si des acteurs français se sont montrés à un moment intéressé (Orange, Thalès, Onepoint, Capgemini), ce sont plutôt les tentatives d'acteurs étrangers qui inquiètent : Lutech en Italie, le consortium DxC (ESN américaine), des fonds anglo-saxons (ICG Partners, Cerberus, Apollo) dont les avances sont alléchantes pour les actionnaires du groupe. Le fonds d'investissement de Siemens franchissait le seuil de 5% du capital du groupe et des droits de vote en novembre 2022.

ATOS peut toutefois compter sur une propriété intellectuelle étoffée (brevets) des équipes R&D de haut niveau, une base de très grands clients demandeurs de services informatiques et d'expertise quantique et du soutien des pouvoirs publics. Toutefois les crises successives du COVID-19, la guerre en Ukraine et la crise énergétique ont affaibli le groupe, qui voit ses coûts augmenter et ses chaînes d'approvisionnement s'allonger et se fragiliser (puces et cartes, CPU, ASIC, composants clés). Ainsi, les routes d'approvisionnement désorganisées en Asie à la suite de la crise du COVID-19 ont ralenti la production de matériels clés au détriment de concurrents régionaux.

Enfin, en cas de crise cyber majeure, le groupe semble bien positionné avec ses propres solutions et savoir-faire en termes de cyberdéfense, même si sa surface (110 000 employés) le rend vulnérable à une faille humaine.

Indices de souveraineté

	indice général Contribution à la souveraineté économique française	**Indice 1** Force d'innovation technologique	**Indice 2** Contribution à la puissance économique française	**Indice 3** Contribution au rayonnement de la France	**Indice 4** Indépendance vis-à-vis de puissances étrangères	**Indice 5** Indépendance financière
ATOS						
MBDA						
Naval Group						
Outscale						
OVHCloud						

Preligens						
Athea						

IV) Dispositifs de soutiens français et européens

Des solutions existent déjà pour assurer la souveraineté de la France dans ces filières et protéger ces entreprises, mais elles peuvent être complétées ou rénovées pour davantage d'efficacité.

Dispositifs en France

Création des plans de relance de la souveraineté économique française

Cinq plans thématiques pour reconstruire la souveraineté économique de la France ont été récemment proposés par la Commission des Affaires Economiques du Sénat. Les thèmes abordés sont les suivants :

- L'approvisionnement en intrants
- Les infrastructures énergétiques et numériques
- Les compétences et métiers de demain
- La politique commerciale
- La protection des entreprises françaises

Plan d'action ministériel « achat d'innovation 2021-2024 » :

Un décret de décembre 2018 avait permis d'expérimenter pour 3 ans l'achat sur devis de produits ou solutions innovantes d'un montant inférieur à 100 000 € HT. Le retour d'expérience a porté sur l'ensemble du périmètre d'achat du ministère, armement et hors armement réunis, ce qui a permis de conclure à l'intérêt réel de ce dispositif. Désormais inscrite dans le code de la commande publique, cette disposition facilite et accélère l'acquisition d'innovations.

Les organismes sous tutelle jouent un rôle particulier au sein de l'écosystème de l'innovation de défense. Référents dans leurs domaines de compétences, ils animent leurs propres réseaux d'acteurs et forment des amplificateurs de l'orientation en matière d'innovation de défense. Au-delà des axes d'efforts tirés par les besoins de la Défense, ils orientent la recherche exploratoire pour répondre aux besoins futurs.

Services de protection économique des entreprises

Le Service de l'information stratégique et de la sécurité économiques (Sisse) a été chargé d'animer, sous l'autorité du Commissaire à l'information stratégique et à la sécurité économiques (également Directeur général des entreprises), la politique de sécurité économique française. Créé en 2016, c'est un service à compétence nationale, à vocation interministérielle et rattaché à la DGE à Bercy. Les entreprises françaises peuvent s'appuyer sur le Sisse pour être conseillées et faire face aux nombreux défis économiques du moment.

En termes de renseignement, la DRSD et la DGSI jouent un rôle de premier plan en termes de contre-ingérence.

France 2030

Le ministère des Armées doit pouvoir s'appuyer sur une base industrielle performante, pérenne et dotée d'une forte capacité d'innovation. Elle est constituée de grands groupes industriels de défense et de milliers d'ETI, PME et start-up que le ministère soutient Le PIA (20 milliards d'euros sur 5 ans) jusqu'à récemment, et aujourd'hui le plan d'investissement France 2030 sont des atouts majeurs pour atteindre cet objectif.

France 2030 vise un double objectif : positionner l'industrie française sur les marchés stratégiques en soutenant les acteurs émergents et transformer des innovations en projets industriels. Doté de 34 milliards d'euros, France 2030 identifie 10 objectifs prioritaires (nucléaire, hydrogène décarboné et EnR, décarbonation de l'industrie, premier avion bas-carbone, 2 millions de véhicules électriques et hybrides, alimentation saine, 20 bio-médicaments et dispositifs médicaux innovants, contenus culturels et créatifs, nouvelle aventure spatiale, grands fonds marins) et des conditions resserrées de sélection des projets (50% des crédits seront en faveur de la décarbonation, 50% du plan pour les acteurs émergents).

Dispositifs européens

L'intérêt structurel des coopérations, notamment européennes, réside dans une interopérabilité et une interchangeabilité avec les partenaires mais aussi dans la recherche de coûts d'échelle en mutualisant les besoins, la fédération d'une industrie globalement plus efficiente, robuste et intégrée et l'accès à des projets ou études que la France ne pourrait pas financer seule.

Hub for European Defence Innovation (HEDI)

Consolider la souveraineté de l'Europe passe par la construction d'une stratégie d'innovation. Dans le contexte de la PFUE, la France a donné une impulsion forte à la mise en place par l'Agence européenne de défense du dispositif HEDI (*Hub for European Defence Innovation*) qui permettra d'animer des travaux et des projets d'innovation dont l'origine est extérieure à l'écosystème de défense, dans l'optique de constituer des projets davantage orientés vers des usages militaires.

Fonds européen de défense (FED)

Le FED encourage la coopération entre États membres dans les domaines de la R&T de défense et du développement capacitaire. Il fait suite aux deux programmes pilotes, l'action préparatoire pour le volet recherche et le programme de développement industriel de défense. Il contribue à l'approfondissement de l'autonomie stratégique de l'UE à travers deux aspects : le renforcement de la BITDE, afin de limiter la dépendance technologique de l'UE et le développement de capacités, qui permettra aux Etats membres de mener des opérations avec une plus grande efficacité et une plus grande autonomie d'action.

Un montant de près de 8 milliards d'euros a été validé pour le cadre 2021-2027. La France soutient 40 projets, dont la plupart s'inscrivent dans le cadre d'une réponse aux projets de la coopération structurée permanente, de R&D de fond, et de soutien aux PME de la filière.

Quantique européen

Si la France maîtrise donc une partie importante de la chaîne de valeur quantique, le meilleur partenaire semble être l'Allemagne, mieux financée, et disposant notamment du centre de calcul allemand Jülich ou de l'EuroHPC Jupiter permettant d'atteindre l'exascale.

D'autres dispositifs ou ressources communes existent comme le JU ECSEL, EuroHPC, HPCQS H2020 ou ERC, Quantum Flagship Européen ou QLSI. Des calculateurs HPC voient leurs ressources partagées au niveau européen, comme HELMI et LUMI : *"Les travaux quantiques sont transmis à HELMI de manière sécurisée via HTTPS et le backend de HELMI contrôle l'électronique matérielle pour effectuer le calcul quantique réel. Le résultat est renvoyé du côté de LUMI au programme qui a fait l'appel. Il peut alors combiner le résultat avec tout calcul classique qu'il a pu effectuer. Il peut ensuite lancer l'itération suivante ou afficher les résultats à l'utilisateur* », détaille à *ComputerWeekly* Ville Kotovirta, chef de l'équipe des algorithmes quantiques au VTT.

DIANA (Defence Innovation Accelerator for the North Atlantic) de l'OTAN

La diminution des contraintes sanitaires a permis la consolidation des liens avec nos alliés et partenaires désireux d'explorer l'innovation non originellement dédiée à la Défense. Les USA, le Canada, les Pays- Bas, Singapour (avec la prochaine mise en place d'un laboratoire commun d'IA) ou le Royaume-Uni offriront des possibilités d'échanges et de collaboration concrètes dans la captation d'innovations d'opportunité.

Lorsque la crise du Covid-19 a conduit à un verrouillage de toutes les activités, le manque de culture numérique du personnel de la défense a révélé à la fois une nouvelle menace et une opportunité. Conscients de cette situation, les membres de l'OTAN ont décidé en juin 2020 de lancer l'Accélérateur d'innovation de défense de l'Atlantique Nord (DIANA), dont l'objectif est d'atteindre les pleines capacités opérationnelles d'ici 2023. DIANA est la version OTAN de la DARPA et renforcera la coopération transatlantique dans le domaine des technologies essentielles pour assurer la sécurité et la culture numérique de défense.

Propositions d'actions transverses:

- Création d'un comité interministériel destiné à se prononcer sur les questions des nouvelles technologies militaires nécessitant un effort de souveraineté
- Développement d'un vivier d'experts en nouvelles technologies appliquées au militaire (quantique, IA, CYBER, nucléaire, missilerie) au sein du ministère de l'économie et en lien avec les autres ministères (Armées, éducation nationale, transition écologique, affaires étrangères) et en souveraineté économique
- Mise en place d'une politique interministérielle de la donnée qui doit garantir une exploitation optimale des données tout en respectant les exigences de sécurité et de conformité
- Mise en place d'une gouvernance de l'action ministérielle des nouvelles technologies souveraines, avec la création d'une Cellule de Coordination au sein de chaque ministère concerné
- Mise en place de mécanismes entre les contrats de recherche et l'acquisition de solutions pour faciliter le passage à l'échelle industrielle
- Le développement de coopérations internationales, en particulier au niveau européen, afin de porter les positions stratégiques de la France et de peser dans l'établissement des normes techniques ou des régulations sur l'exportation des nouvelles technologies

- **Cloud**

❖ Apporter un soutien plus fort à la migration vers le cloud, avec des politiques publiques normalisées, une politique de dépenses dédiées au Cloud.

❖ Allocation de dépenses publiques massives sur le long-terme pour soutenir la montée en puissance de fournisseur de cloud européens, en contrepartie d'une trajectoire cible de développement visant à imposer l'interopérabilité entre fournisseur cloud

- **Quantique**

Les dispositifs existants au niveau français et européen, ainsi que l'existence d'une stratégie dédiée semblent convaincants. Il faut toujours faire mieux !

❖ Montée de l'Etat au capital d'ATOS pour éviter une OPA hostile.

❖ Création d'un incubateur dédié aux applications quantiques militaires, supervisé par DefInvest (BPI), la DGA et le CEA-Leti. CEla permettrait de rassembler les savoir-faire scientifiques, militaires et financiers au sein d'une structure commune ayant vocation à "aimanter" la création de startups innovantes.

V) Comment garder ces entreprises comme grands groupes mondiaux ?

- **Actions majeures à réaliser ou à poursuivre :**

Afin de pouvoir garder nos entreprises de pointe à leur niveau de compétitivité actuelle tout en ayant pour but final de les développer dans un temps plus long, les actions suivantes sont nécessaires au niveau de l'Etat français :

❖ Amélioration de la capacité de la France à produire certains **biens stratégiques** dans les domaines dits critiques (IA, quantique, etc)

❖ Recherche d'une plus grande **diversification** des fournisseurs et des sources en priorisant la BITD européenne

❖ Constitution de stocks stratégiques (nécessité d'avoir un contrôle périodique de la qualité et de la quantité des stocks stratégiques) et l'attraction d'investisseurs étrangers sur le territoire français

❖ Développement de la **protection des brevets** à l'instar de la protection américaine

❖ Poursuite et amélioration de la protection des entreprises face à un **rachat par un pays étranger**

❖ Augmentation **des instances de contrôles des investissements** étrangers en France et au niveau européen

❖ Développement de **mesure politiques fortes généralisées au niveau national mais surtout au niveau européen** (ex : Plan de résilience économique et sociale / chips act aux USA 5 (37 milliards de dollars)) ;

❖ Développement des systèmes de **protection et des sensibilisations** des grands groupes en matières de sécurité économique

- **Contrôle des investissements étrangers en France :**

L'Etat français a depuis un certain temps pris en compte les possibles menaces des investissements étrangers sur les entreprises françaises

Bruno Le Maire a déclaré : *« Le contrôle des investissements étrangers en France qui a été complété par la loi PACTE est un instrument essentiel de la souveraineté économique, industrielle et numérique du pays. La publication de lignes directrices relative au contrôle des IEF permettra de renforcer la prévisibilité et la sécurité juridique des opérations envisagées par les investisseurs étrangers et ainsi contribuer à renforcer davantage encore l'attractivité de la France ».*

A l'initiative de Bruno Le Maire, ministre de l'Economie, des Finances et de la Souveraineté industrielle et numérique, **la loi PACTE** a permis de renforcer le régime français de contrôle des investissements étrangers et de l'adapter aux enjeux économiques actuels. Cet effort doit être encore davantage développer et renforcer afin de muscler les systèmes de protection et de sauvegarde de nos entreprises de pointe.

Focus investissements étrangers en France (IEF) :

Le gouvernement français renforce, le dispositif de contrôle des investissements étrangers en France (IEF). Les technologies dites "critiques" - dont la cybersécurité, l'intelligence artificielle, les semi-conducteurs ou le stockage de l'énergie - font l'objet d'une attention particulière des pouvoirs publics. De plus, le gouvernement peut désormais bloquer une acquisition dès lors que la participation envisagée par un investisseur étranger porte sur un minimum de **25%** du capital, contre **33%** auparavant.

❖ Pour des entreprises travaillant dans des domaines critiques, il serait nécessaire de continuer à diminuer le taux de blocage. On pourrait même arriver à 10%. Les champions technologiques français et européens ne peuvent plus être grignotés par la concurrence internationale.

- **<u>Propositions :</u>**

❖ Développer la capacité, pour la France, à faciliter l'émergence des start-up innovantes à forte performance économique (capitalisation boursière et création d'emplois aux effets multiples sur la consommation, le pouvoir d'achat et le développement du capital humain).

❖ Développement d'une Silicon Valley à la Française afin de créer un bassin industriel de recherche, de production mais aussi d'éducation pour promouvoir les interactions des nouvelles technologies.
Comme pour le cas américain, où les interactions entre l'Université de Stanford, de l'Armée américaine, et enfin de la communauté des affaires, en particulier les fonds d'investissements ont permis l'avènement de la Silicon Valley, ce même processus pourrait être développé (par exemple POLYTECHNIQUE, armée française et communauté des affaires).

❖ A l'avenir, une solution du type "**Proxy Agreement**" à la française, à l'image de ce qu'impose l'administration américaine à des investisseurs étrangers lors d'un rachat d'une société considérée comme stratégique pour les États-Unis devra peut-être voir le jour afin de lutter contre la violence de la guerre économique qui fait rage. Ce dispositif limiterait drastiquement les droits de l'investisseur étranger au sein même de sa société, de même que la désignation des dirigeants de la société.

❖ Acquisition d'un petit nombre d'actions avec un droit de vote préférentiel dans des sociétés hautement stratégiques. Le bénéfice de cette opération :

- Coût d'acquisition peu élevé grâce à la petite quantité d'actions achetées.
- Le droit de vote préférentiel confère un droit de vote double, triple quadruple selon les statuts…De ce fait, l'Etat bénéficie d'un pouvoir plus grand en assemblée.
- La société reste attractive pour les investisseurs car malgré la diminution de leurs droits de vote, les dividendes restent identiques.

Sources

- https://www.researchgate.net/figure/Sketch-of-quantum-warfare-utilising-various-quantum-technology-systems_fig1_355975604
- https://www.oezratty.net/wordpress/2022/strategie-quantique-francaise-un-an-apres/
- https://www.lesechos.fr/tech-medias/hightech/thales-ferme-la-porte-a-une-position-minoritaire-dans-le-spin-off-datos-1895791
- https://www.ibm.com/fr-fr/topics/quantum-computing
- https://en.wikipedia.org/wiki/Quantum_cryptography
- https://portail-ie.fr/analysis/4149/atos-risque-une-opa-hostile-menace-pour-la-souverainete-numerique-francaise
- https://epjquantumtechnology.springeropen.com/articles/10.1140/epjqt/s40507-021-00113-y
- https://medium.com/uvc-partners-news/the-european-quantum-computing-startup-landscape-a115ffe84ad8
- https://www.latribune.fr/technos-medias/informatique/atos-le-geant-francais-de-l-informatique-en-negociations-exclusives-avec-l-italien-lutech-941110.html
- https://www.lemondeinformatique.fr/actualites/lire-atos-a-l-heure-de-la-restructuration-87069.html
- https://www.nouvelobs.com/economie/20220623.OBS60061/atos-la-chute-d-un-colosse-aux-pieds-d-argile.html
- https://www.challenges.fr/entreprise/les-plantages-en-serie-qui-menacent-atos_787561
- https://atos.net/fr/2022/communiques-de-presse_2022_02_16/atos-devoile-son-nouveau-supercalculateur-hybride-de-classe-exascale-au-coeur-de-la-souverainete-numerique-et-economique
- Livres Blancs
- https://www.lemonde.fr/economie/article/2022/10/06/les-predateurs-rodent-autour-d-atos_6144659_3234.html
- https://atos.net/wp-content/uploads/2022/02/La-souverainete-numerique-selon-Atos.pdf
- https://www.cairn.info/revue-defense-nationale-2021-HS4-page-241.htm
- https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657
- https://www.opex360.com/2022/09/08/m-lecornu-met-en-garde-les-industriels-de-larmement-contre-les-risques-de-sabotage-et-despionnage/
- https://www.ege.fr/sites/ege.fr/files/uploads/2020/06/IndustriesdeD%C3%A9fenserisquesinformationnels.pdf
- https://www.ifri.org/sites/default/files/atoms/files/044_051_cyberguerre-2.pdf
- Agence de l'innovation de défense | ministère des Armées (defense.gouv.fr)
- Preligens | Pioneering AI for a safer world
- Athea – La solution européenne de big data souverain
- Pappers : Toute l'information gratuite sur les entreprises en France
- Societe.com : RCS, siret, siren, bilan, l'information gratuite sur les entreprises du Registre du Commerce des Sociétés (RNCS)
- https://www.economie.gouv.fr/plan-de-relance
- https://www.economie.gouv.fr/dae/innovation
- https://sisse.entreprises.gouv.fr/fr
- https://www.gouvernement.fr/actualite/france-2030-un-plan-d-investissement-pour-la-france-de-demain
- Création d'un pôle pour l'innovation de défense de l'UE au sein de l'AED (europa.eu)
- https://welcomeurope.fr/13-milliards-deuros-pour-le-futur-fonds-europeen-de-la-defense-2021-2027/
- https://finabel.org/defence-innovation-accelerator-for-the-north-atlantic-diana
- #focus - Loi n° 2019-486 du 22 mai 2019 dite LOI PACTE / Réforme de l'assurance vie - JurisCampus - Institut de formation professionnelle
- Investissements étrangers en France | Direction générale du Trésor (economie.gouv.fr)
- Les stratégies de défense anti-OPA en droit français et américain des sociétés | Institut de Droit Comparé (u-paris2.fr)
- Baromètre Vélite 2022 : la seconde édition de l'étude sur la souveraineté économique des groupes du CAC 40 (cabinet-velite.com)
- Les stratégies de défense anti-OPA en droit français et américain des sociétés | Institut de Droit Comparé (u-paris2.fr)
- Rapport de Cédric Villani : donner un sens à l'intelligence artificielle (IA) | enseignementsup-recherche.gouv.fr
- Chocs futurs | Secrétariat général de la défense et de la sécurité nationale (sgdsn.gouv.fr)
- France 2030 : un plan d'investissement pour la France | economie.gouv.fr
- Intelligence artificielle et armées françaises : une technologie du présent à mettre en œuvre immédiatement | Cairn.info
- Innovations de rupture : enjeux et défis pour la souveraineté française | Cairn.info
- 20200108-NP-Rapport de la Task Force IA Septembre.pdf (defense.gouv.fr)
- https://www.defense.gouv.fr/sites/default/files/dgnum/Ambition%20Num%C3%
- A9rique%20-%20Minist%C3%A8re%20des%20Arm%C3%A9es.pdf
- https://www.assembleenationale.fr/dyn/15/rapports/cion_def/l15b0996_rapport-information.pdf
- https://www.defense.gouv.fr/sites/default/files/aid/Report%20of%20the%20AI

- %20Task%20Force%20September%202019.pdf
- https://www.gartner.com/doc/reprints?id=1-271OE4VR&ct=210802&st=sb
- https://www.ncsc.nl/documenten/publicaties/2022/augustus/16/cloud-actmemo
- Le Cloud européen - KPMG France (home.kpmg)
- https://www.cairn.info/revue-vie-et-sciences-de-l-entreprise-2007-3-page-43.htm
- Repenser la place des entreprises dans la société_Comment concrétiser les ambitions de la loi PACTE (www.cci.fr)
- https://www.defense.gouv.fr/energie-ops/nos-missions/energie
- https://www.naval-group.com/fr/gouvernance
- https://www.defense.gouv.fr/dga/adaptation-au-m51-snle
- https://www.defense.gouv.fr/cesm/actualites/breves-marines-ndeg254-missiles-hyperveloces-technologie-strategique-immature
- https://www.onera.fr/fr/actualites/actualisation-du-plan-strategique-scientifique-2015-2025
- https://www.onera.fr/fr/missions-et-objectifs
- https://www.defense.gouv.fr/dga/rafale
- https://www.defense.gouv.fr/sites/default/files/aid/Report%20of%20the%20AI
- %20Task%20Force%20September%202019.pdf
- https://www.gartner.com/doc/reprints?id=1-271OE4VR&ct=210802&st=sb
- https://www.ncsc.nl/documenten/publicaties/2022/augustus/16/cloud-actmemo
- Le Cloud européen - KPMG France (home.kpmg)
- https://www.cairn.info/revue-vie-et-sciences-de-l-entreprise-2007-3-page-43.htm
- Repenser la place des entreprises dans la société_Comment concrétiser les ambitions de la loi PACTE (www.cci.fr)
- Ambition numérique du ministère des Armées
- [2] Rapport d'information en conclusion des travaux d'une mission d'information
- sur les enjeux de la numérisation des armées - https://www.assembleenationale.
- fr/dyn/15/rapports/cion_def/l15b0996_rapport-information.pdf
- [3] Report of the AI Task Force September 2019 - Artificial intelligence in support of defence -
- https://www.defense.gouv.fr/sites/default/files/aid/Report%20of%20the%20AI
- %20Task%20Force%20September%202019.pdf
- [4] Gartner - Magic Quadrant for Cloud Infrastructure and Platform Services -
- https://www.gartner.com/doc/reprints?id=1-271OE4VR&ct=210802&st=sb
- [5] Rapport d'analyse commandité par le gouvernement néerlandais sur
- L'applicabilité du Cloud Act américain -
- https://www.ncsc.nl/documenten/publicaties/2022/augustus/16/cloud-actmemo
- Prestataires de service d'informatique en nuage (SecNumCloud)
- Le Cloud européen : de grands enjeux pour l'Europe et cinq scénarios avec des impacts majeurs d'ici 2027-2030 - https://assets.kpmg/content/dam/kpmg/fr/pdf/pdt/fr-mv-1204-lcege.pdf
- EU Chips Act : le plan de l'Europe pour redevenir leader mondial des semi-conducteurs
- https://ec.europa.eu/commission/presscorner/detail/fr/STATEMENT_22_891
- https://www.ovhcloud.com/fr/datacenters-ovhcloud/
- https://www.ovh.com/fr/blog/comment-ovh-resout-lequation-developpement-aux-usa-et-identite-europeenne/
- Document d'enregistrement d'OVHCloud auprès de l'autorité des marchés financiers (AMF) français - https://corporate.ovhcloud.com/sites/default/files/2021-12/ovh-groupe-deu-2021-vdef.pdf
- https://corporate.ovhcloud.com/fr/sustainability/supply-chain/
- Protéger ses données et services stratégiques dans le cloud : enjeux, principes et solutions
- https://www.ovhcloud.com/fr/lp/how-protect-your-data-cloud/
- https://www.bfmtv.com/economie/entreprises/industries/les-super-pouvoirs-des-nouveaux-satellites-espions-que-la-france-envoie-dans-l-espace_AN-201812170119.html
- https://sifted.eu/articles/western-armies-technical-edge/
- https://nam12.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.senat.fr%2Fnotice-rapport%2F2021%2Fr21-755-notice.html&data=05%7C01%7C%7Ce552a6ec76fc46d0064a08da626ad942%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C637930508318553080%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=CRQ9pZkwfmEF4blHJZyY3lnyrkeUQxszE6%2Bz7cv4Htc%3D&reserved=0
- https://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/pourquoi-naval-group-est-la-societe-la-plus-solide-de-son-secteur-en-europe-808157.html
- Ambition numérique du ministère des Armées
- Clotilde Bômont, « Le cloud défense : défi opérationnel, impératif stratégique et enjeu de souveraineté », Focus stratégique, n° 107, Ifri, novembre 2021. - https://www.ifri.org/sites/default/files/atoms/files/bomont_cloud_defense_2021.pdf

- Le "cloud tactique", un élément essentiel du système de combat aérien futur - https://www.frstrategie.org/publications/notes/cloud-tactique-un-element-essentiel-systeme-combat-aerien-futur-2019
- Rapport d'information en conclusion des travaux d'une mission d'information sur les enjeux de la numérisation des armées - https://www.assembleenationale.fr/dyn/15/rapports/cion_def/l15b0996_rapport-information.pdf
- Report of the AI Task Force September 2019 - Artificial intelligence in support of defence -
- https://www.assemblee-nationale.fr/dyn/15/rapports/resinat/l15b5119_rapport-information.pdf
- https://www.assemblee-nationale.fr/dyn/15/rapports/cion_afetr/l15b4822_rapport-information
- Quelle stratégie de résilience dans la mondialisation ?
- https://www.cae-eco.fr/quelle-strategie-de-resilience-dans-la-mondialisation
- Quels intrants vulnérables doit-on cibler ?
- https://www.cae-eco.fr/quels-intrants-vulnerables-doit-on-cibler
- Etude DG Trésor
- Analyse de la vulnérabilité des approvisionnements français
- https://www.tresor.economie.gouv.fr/Articles/2021/12/15/analyse-de-la-vulnerabilite-des-approvisionnements-francais
- Echanges dans le cadre de l'étude avec du personnel des sociétés : PRELIGENS, ATHEA ministère des Armées (AID, Force terrestre, STAT)