Groupes de défense et technologies du numérique

Recherches & Documents

N°01/2022

Kévin Martin
Chargé de recherche, Fondation pour la recherche stratégique
Janvier 2022

www.frstrategie.org

FONDATION pour la RECHERCHE STRATÉGIQUE

SOMMAIRE

Groupes de défense et technologies du numérique

Introduction

Les entreprises sont confrontées aujourd'hui aux défis liés à l'intégration croissante des technologies issues du numérique dans leurs capacités et techniques de production et dans leurs offres. Cybersécurité, *big data*, *cloud*, ou encore intelligence artificielle, ces technologies amènent à repenser le modèle d'affaires des entreprises, quels que soient leurs secteurs d'activités. Cette transformation numérique peut se traduire par des évolutions radicales en matière d'organisation du travail, de management de l'innovation (produits et technologies), d'opportunités d'affaires, notamment. Ces changements concernent également l'environnement de l'entreprise avec la redéfinition des chaînes de valeur et des écosystèmes ainsi que l'arrivée de nouveaux concurrents aux profils différents. Les groupes de défense historiques n'échappent pas à ces tendances de fond.

Les stratégies nationales de défense des grandes puissances convergent toutes sur le rôle et le recours croissant de ces technologies pour et par les armées. Leur maîtrise est considérée comme un enjeu de souveraineté. Depuis quelques années, la cybersécurité et l'intelligence artificielle (IA) font ainsi l'objet de stratégies nationales dédiées. Or, dans ces domaines technologiques, les groupes de défense se trouvent confrontés à la concurrence d'entreprises au profil d'activités à dominante civile, centré sur le développement d'offres de services web, de prestations de services informatiques et de production de matériels.

Cette note vise ainsi à explorer les différents enjeux liés au développement et au maintien d'activités liées au numérique (cybersécurité et IA) par les groupes de défense, et ce, dans un contexte d'intensité concurrentielle.

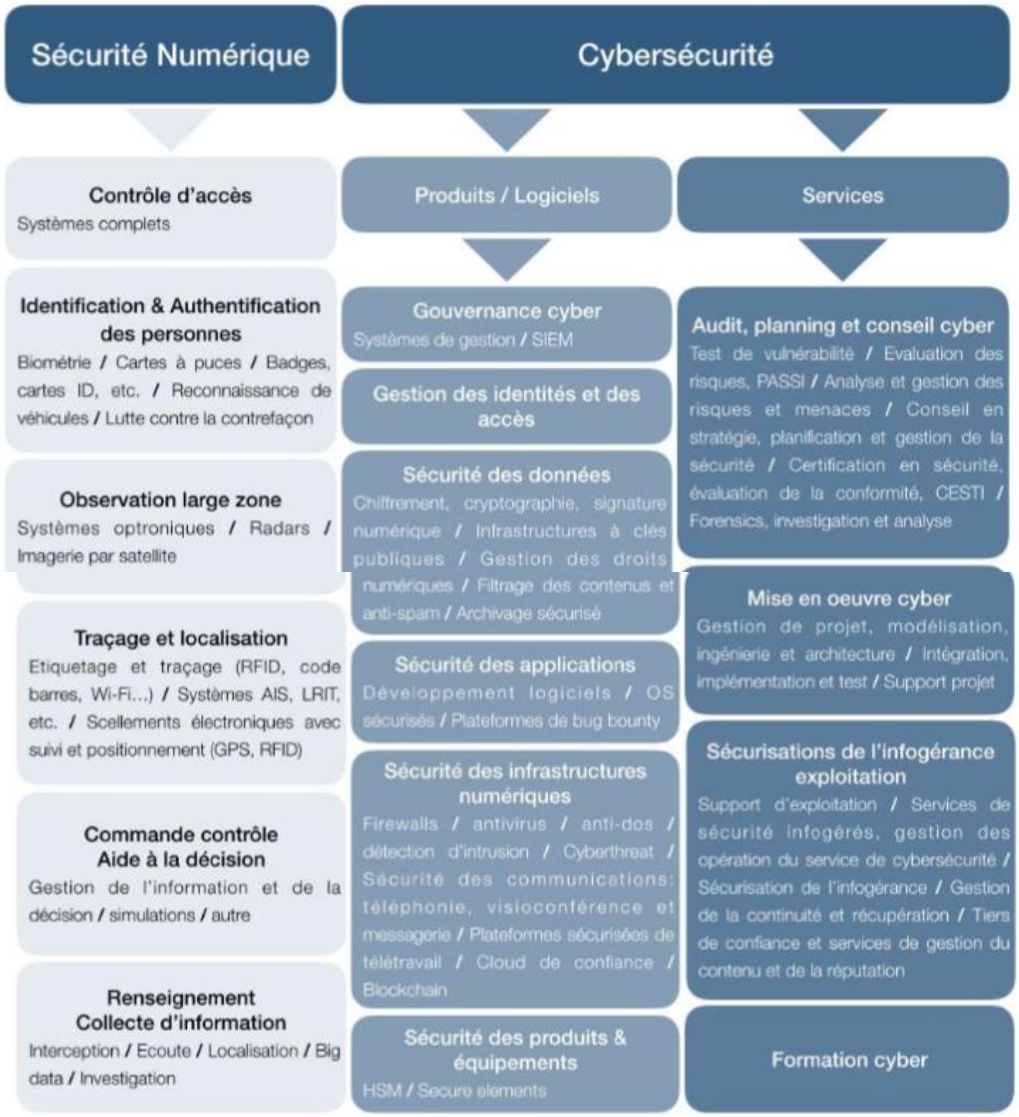
1. Spécificités des marchés liés aux solutions numériques

1.1. Des marchés dynamiques et hétérogènes

Les offres liées au numérique recouvrent des solutions très diverses quel que soit le domaine technologique étudié, rendant complexe la lecture de ces marchés. En matière de cybersécurité, on peut, par exemple, distinguer les solutions selon le type d'offres (matériels, software, services associés) ou selon les fonctions de sécurité souhaitées. L'Alliance pour la con-

fiance numérique (ACN), à travers son observatoire annuel, propose une segmentation entre les solutions de sécurité numérique et les produits et services de cybersécurité. Or, pour chacune de ces solutions, les dynamiques de marché peuvent s'avérer très différentes.

Figure n° 1 : PERIMETRE DE LA CONFIANCE NUMERIQUE, SEGMENTATION DES SOLUTIONS



Source : ACN, *Observatoire pour la confiance numérique*, 2021

En matière d'intelligence artificielle, la segmentation apparaît tout aussi problématique[1]. Le déploiement commercial de l'intelligence artificielle n'en étant qu'à ses débuts, la majorité des solutions d'IA sont des produits spécialisés dans des domaines particuliers, et le marché s'apparente pour l'heure à un ensemble morcelé de briques technologiques, que ce soit en matière de traitement du langage naturel, de la vision ou de la parole, de l'autonomisation de la robotique.

[1] Olivier Ezratty, *Les usages de l'intelligence artificielle*, Creative Commons, Edition 2021, 742 p.

Figure n° 2 : APPLICATIONS FONCTIONNELLES DE L'IA : UN EXEMPLE DE SEGMENTATION

Source : *WIPO Technology Trends 2019: Artificial Intelligence*[2]

Suivant les briques technologiques, les avancées industrielles (et commerciales) en sont à des niveaux de maturité très différents. Les principales solutions vendues se concentrent ainsi sur les technologies de *machine learning* avec différentes approches de l'apprentissage (en particulier supervisé ou en profondeur). Mais l'IA regroupe de nombreuses sous-familles technologiques ne faisant pas appel aux données de la même manière, en termes de volume et de qualité. Ainsi, la richesse du concept même d'intelligence artificielle ne transparaît-elle pas vraiment dans le panorama industriel actuel, en particulier suite à la focalisation des travaux sur les technologies d'IA connexionnistes[3].

En matière de hardware, l'attention se porte sur les processeurs et les microprocesseurs en raison notamment de l'essor des technologies d'IA liées au *machine Learning*. En effet, ces solutions reposent en grande partie sur le développement des capacités de stockage et de calculs. Là encore, des dynamiques de marché apparaissent suivant le type d'architecture (GPGPU, processeurs neuromorphiques) ou encore les infrastructures à équiper (serveur *cloud*, capteur/effecteur).

[2] WIPO, *WIPO Technology Trends 2019: Artificial Intelligence*, 2019.

[3] L'IA comprend deux branches techniques principales, l'IA connexionniste et symbolique. Comme le précise le rapport de la *task force* IA du ministère des Armées (Stratégie de l'Intelligence artificielle au service de la Défense, 2019), « *les approches symboliques* [sont] *basées sur le raisonnement (systèmes à base de règles) et les approches connexionnistes plus proches de l'empirisme, fondées sur l'apprentissage à partir de grandes bases de données (réseaux de neurones)* ».

De manière générale, ces domaines technologiques se caractérisent par une absence de définition partagée, recouvrant une multitude de familles technologiques, dont les voies sont explorées simultanément et sont à des stades de développement variés. Les analyses de marché et les perspectives de croissance dépendent alors considérablement des périmètres pris en compte. Souvent présentés comme des solutions de rupture permettant le développement de nouvelles techniques ou de nouveaux usages (s'accompagnant de nouveaux besoins de sécurité), ces domaines technologiques se particularisent par des cycles d'innovation extrêmement rapides.

1.2. Une demande atomisée et très segmentée

Pour l'ensemble de ces marchés du numérique, la demande est également caractérisée par une forte disparité avec des segmentations de type géographique, par typologie clients ou encore par métier.

Le marché américain apparaît incontournable pour les offreurs de solutions, quel que soit le domaine. Par exemple, en matière de cybersécurité, il représentait en 2019 près de 37 % de la demande mondiale[4], selon l'European Cybersecurity Organisation (ECSO), conférant *de facto* aux entreprises américaines un avantage compétitif lié à un « effet de grand marché ». Les marchés européens (hors Royaume-Uni) représentent quant à eux une part de 13 %. Mais il s'agit ici d'une donnée agrégée. En effet, l'Union européenne demeure encore un marché morcelé, obligeant les entreprises à adopter des approches nationales, et ce, malgré les initiatives visant à le consolider (directive NIS, *Cybersecurity act*)[5].

On peut également distinguer quatre grands types de marché en fonction du profil des clients finaux, lesquels se distinguent par un certain nombre de facteurs déterminants comme le niveau d'exigence de sécurité, les fonctionnalités et le budget dédié. Cette ventilation en quatre grandes catégories permet d'ajuster l'analyse aux contraintes et aux spécificités de chaque profil clients (taille, maturité du marché et besoins particuliers), mais elle n'est pas figée. Des caractéristiques communes peuvent en effet émerger.

- **Défense**

  Ce marché est considéré comme très mature (hors niche d'innovation), nécessitant les technologies les plus complexes et dont les solutions sont généralement produites et commercialisées par les groupes travaillant pour la défense. Souvent liées à des domaines de souveraineté, les contraintes y sont plus fortes, en termes d'exigences de sécurité, de conformité et de confidentialité des données. Si les con-

[4] Carlos Alberto Silva, « The current status of private investment in cybersecurity and effort until now at European level », Présentation ECSO au 9e Cyber Investor Days, 15 juin 2021.

[5] Adoptée par le Parlement européen en 2016, la directive NIS vise notamment à définir une série d'exigences communes en matière de sécurité des réseaux de l'information pour les acteurs désignés comme opérateurs de services essentiels (OSE). Le *Cyber Security Act*, règlement adopté quant à lui en juin 2019, va plus loin, conférant à l'ENISA (Agence européenne chargée de la sécurité des réseaux et de l'information) un mandat permanent et définissant pour la première fois un cadre européen de certification de cybersécurité. Toutefois, comme le rappelle l'ANSSI : « *Il faut noter qu'en lui-même, le Cyber Security Act définit un cadre et une gouvernance sans pour autant préciser les règles de certification. Les produits, services et processus qui auront vocation à être certifiés feront successivement l'objet de schémas thématiques.* » (cf. ANSSI, *Papiers numériques*, septembre 2021).

trats affichent souvent des montants élevés, ils sont notifiés en nombre limité (marché pluriannuel) et portent généralement sur de petites séries. L'accès à ce type de marché est donc restreint. Il voit fréquemment des regroupements d'acteurs industriels de tailles diverses à même de répondre à des besoins techniques complexes.

- **Administrations publiques**

  Ce marché requiert des niveaux d'exigences de sécurité et de conformité qui se rapprochent, à certains égards, de ceux du marché Défense. Pour les solutions de cybersécurité, de *cloud computing*, ou d'IA les besoins peuvent notamment faire l'objet d'un contrôle des autorités publiques (structures type ANSSI) et doivent respecter des normes et standards prédéfinis. La particularité de ce marché réside dans la nécessité d'une certification des produits et des solutions de cybersécurité et dorénavant de *cloud computing*. Le coût de certification peut s'avérer prohibitif pour certaines entreprises ; l'accès à ce marché est donc contraignant.

- **Grands groupes et entreprises intermédiaires**

  Les exigences sont fixées individuellement par les clients, en fonction de leurs besoins et de leurs attentes (à moins d'une règlementation sectorielle ou spécifique, comme pour les OIV). La dispersion géographique des sites de production, de gestion, et de supervision des activités industrielles ainsi que la compétitivité internationale croissante poussent les grands groupes (comme les ETI) à rechercher des solutions innovantes offrant un rapport qualité de performance/prix attractif, et ce, dans le cadre de leur transformation numérique. Il s'agit de marchés à forte rentabilité mais également plus concurrentiels.

- **Particuliers / PME**

  Ce marché est orienté vers des besoins « grand public », avec des exigences de niveau de sécurité basse en matière de cybersécurité et des attentes de solutions clés en main. Les budgets mobilisables sont généralement peu élevés et les solutions presque exclusivement orientées vers des solutions complètes. Pour les clients « privés », face à la complexité du marché, l'acquisition se porte prioritairement sur des solutions référencées comme leader sur le marché et auprès d'entreprises reconnues.

Les intégrateurs (essentiellement les entreprises de services du numérique), en plus d'être des acteurs industriels, se présentent également comme une catégorie de clients en se positionnant comme intermédiaires sur de nombreux marchés significatifs en volume.

Enfin, les marchés civils doivent également être appréhendés à travers une approche métier. Cette dernière s'avère nécessaire pour évaluer les différentes dynamiques de marché. En effet, une grande partie des solutions numériques prennent en compte les contraintes spécifiques des clients en fonction du secteur d'activités dans lequel elles opèrent (comme le *retail*, banque/finance, santé, ou la logistique). Le mode de vente privilégié étant en B2B, les offreurs adaptent leurs solutions selon le contexte, les règles juridiques et les normes techniques de leurs clients, complexifiant ainsi les logiques d'économie d'échelle.

2. Un environnement industriel marqué par le *leadership* des acteurs du numérique

Le développement de capacités nationales dans le domaine des technologies du numérique s'est généralement appuyé sur la présence au préalable d'une industrie de l'informatique hardware (PC & composants, calculateurs, cartes et puces électroniques, semi-conducteurs), de défense, des télécommunications, du logiciel et du conseil. Dans le cas de l'intelligence artificielle, des acteurs historiquement positionnés sur une offre de services web (Google, Amazon, Facebook) font aujourd'hui partie des leaders dans le domaine par l'adaptation de leur offre d'origine et en capitalisant sur la masse des données dont ils disposent.

Par ailleurs, la dispersion de la demande et les spécificités propres aux technologies du numérique – IA et cybersécurité par exemple – expliquent l'omniprésence d'acteurs industriels au profil d'activités à dominante civile.

2.1. Stratégies et profils

2.1.1. Des acteurs pivots du numérique à la stratégie d'intégration verticale

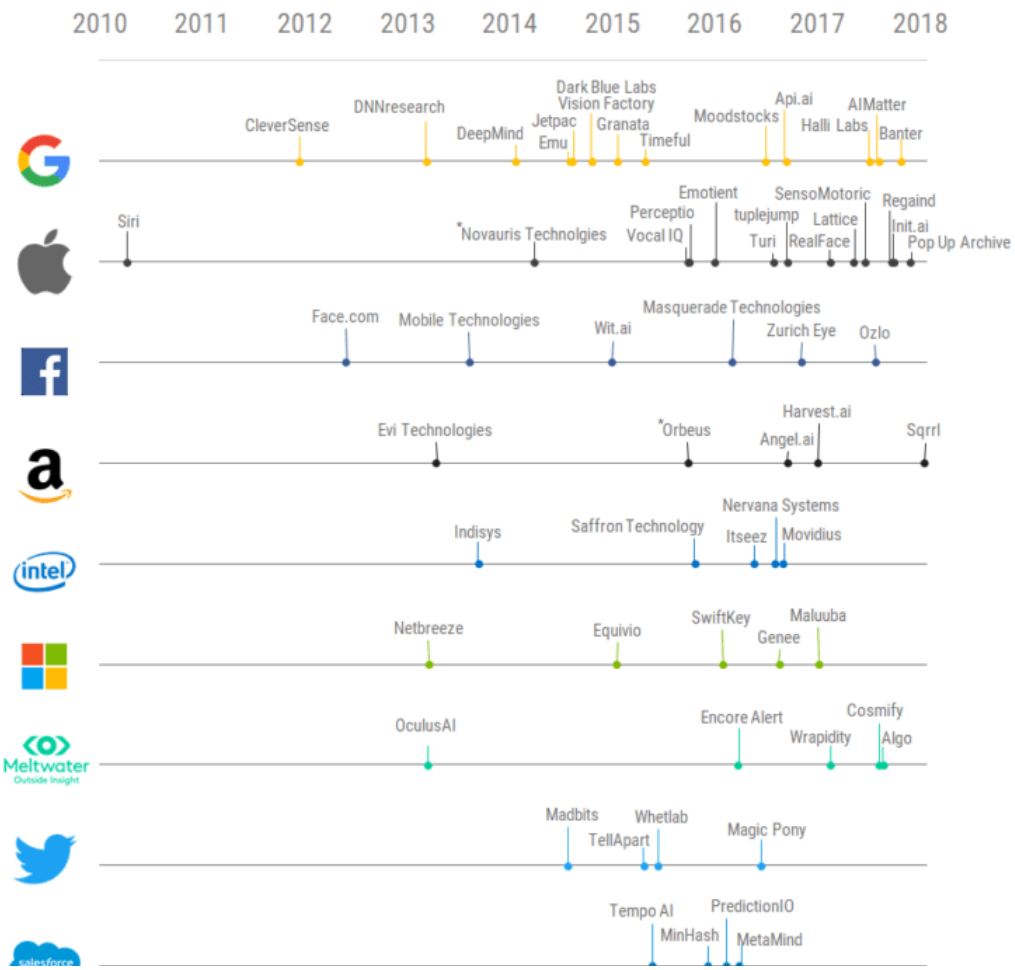
Historiquement, les premiers acteurs du numérique tels qu'IBM (création en 1911), Intel (1968), Microsoft (1976) et Apple (1976) sont issus du monde informatique (fabrication de matériels et d'équipement, développement de systèmes d'exploitation). Quasi exclusivement américains, ils ont cherché à diversifier leurs activités afin de réduire leur exposition au marché des hardwares (tendance baissière marquée de la demande et concurrence d'acteurs émergents, notamment chinois).

Tous ont privilégié une stratégie d'intégration verticale à travers une politique de rachats d'actifs, ciblant prioritairement des éditeurs de logiciels et des prestataires de services informatiques. Ils proposent aujourd'hui des offres complètes, signalant le passage d'un modèle de ventes de produits et de services informatiques à celui de solutions[6]. Par le biais notamment d'une politique dynamique de croissance externe – ces acteurs fondent leur expertise sur leur capacité à suivre les évolutions technologiques et d'usages affectant leurs marchés (produits et clients). Les années 2000 ont ainsi vu ces entreprises se positionner en tant que gestionnaires de données et prestataires de services numériques, cédant le cas échéant des activités historiques de fabrication de matériels[7]. En ce sens, leur stratégie se rapproche de celle déployée par des entreprises comme Amazon, Google et Facebook. Ils ont intégré des solutions de cybersécurité dans leurs offres classiques sans pour autant se positionner sur ce marché en tant que tel. En revanche, l'IA apparaît comme une évolution naturelle de leur cœur de métier, voire un virage incontournable pour conserver leur place dans la chaîne de valeur en tant qu'acteurs pivots de la transformation du numérique des organisations.

[6] Par exemple, passage de la suite Office à Office 365 chez Microsoft.

[7] Par exemple, en 2005, IBM a cédé ses activités PC à Lenovo. En 2014, le groupe a entrepris de se séparer de ses activités de serveur x86 (rachetées par Lenovo) et d'une partie de ses activités historiques de production de semi-conducteurs type puces ex-PowerPC pour Apple, Xbox, etc. (reprises par Global Foundries).

Figure n° 3 : EXEMPLE D'ACQUISITIONS DE *START-UPS* IA PAR DIFFERENTS GROUPES AMERICAINS



Source : CB Insight

Dans ce contexte, l'axe stratégique principal semble reposer sur le développement de systèmes de gestion multiplateformes ou multidomaines fondés sur des technologies utilisant le *machine learning*. En proposant ces briques fondamentales, ils sont à même d'intégrer de nombreuses solutions spécifiques adaptées à chaque secteur ou client.

Par exemple, Microsoft a modifié en profondeur sa stratégie, un mouvement illustré par la place prise par son offre de *cloud computing* « Azure AI » au sein de laquelle l'IA joue un rôle central. Azure AI se fonde plus spécifiquement sur les capacités d'hébergement du groupe – ainsi que sur les données qu'il détient – pour proposer une IA *Platform-as-a-service* (PaaS) capable d'accueillir différentes bibliothèques *open source* ou non comme TensorFlow[8], ainsi que des applications logiciels développées en interne. L'objectif est de positionner le groupe comme un cœur de réseau d'entreprises/institutions en matière d'intelligence artificielle aux applications multiples. Ainsi, le système de Microsoft est plutôt semi-fermé, avec la volonté d'agréger des applications développées hors de l'entreprise sur une plateforme propriétaire en *cloud*.

[8] Outil *open source* dédié au *machine learning* développé par Google.

Figure n° 4 : ÉVOLUTION DE LA CHAINE DE VALEUR DE L'INFORMATIQUE

CHAINE DE VALEUR TRADITIONNELLE : DU PROCESSEUR AU SERVICE

NOUVELLE CHAINE DE VALEUR : DE L'INFRASTRUCTURE A LA SOLUTION

Source : Gérard Roucairol, Pierre Bitard, « Pour une politique industrielle du numérique », *Les cahiers Futuris*, mars 2018, pp. 31-33

Par ailleurs, les acteurs pivots du numérique ont publié en *open source* des briques logicielles de base de l'IA offrant à de très nombreuses *start-ups*, PME voire grands groupes un cadre de développement de solutions métiers (TensorFlow notamment). Ils « *adoptent une double approche de plateforme pour attirer des développeurs d'applications avec des frameworks le plus souvent en open source et générer des économies d'échelle et d'intégration verticale pour capter une partie aussi grande de la valeur ajoutée* »[9]. Dès lors, il en résulte une architecture faussement ouverte où le contrôle de bout en bout de la chaîne induit *de facto* une sorte d'écosystème entre les mains d'un seul acteur[10].

Ces acteurs pivots disposent également de capacités de R&D leur permettant de maintenir ou créer des activités de développement de processeurs (spécifiques aux applications IA). Sur ce segment, leur stratégie industrielle se rapproche de celle des équipementiers *pure players* (dans une logique d'intégration verticale).

2.1.2. Des éditeurs de logiciels au centre de l'attention

Les éditeurs de logiciels représentent les acteurs les plus importants en nombre. Si les leaders mondiaux sont des grands groupes, *pure players*, historiquement positionnés sur le marché de la cybersécurité, généralement non européens et cotés en bourse, cette catégorie d'acteurs comprend également une myriade de *start-ups* et de PME. Ce sont ces dernières qui concentrent aujourd'hui l'attention grâce à une stratégie de communication et marketing offensive. Elles sont souvent très spécialisées, sur un secteur (par exemple finance, santé, commerce électronique) et/ou sur une application (reconnaissance vocale/traitement de la parole, vision par ordinateurs, fouille de données, optimisation, calculateurs dédiés IA, etc.).

Traditionnellement, *start-ups* et PME sont considérées comme les plus porteuses d'innovation, nouant des partenariats avec les autres catégories d'acteurs ou étant elles-mêmes la cible d'opérations d'acquisition. Toutefois, en grande majorité, et particulièrement pour les entreprises positionnées sur des segments applicatifs, il s'agit d'une approche mar-

[9] Olivier Ezratty, *Les usages de l'intelligence artificielle*, ebook Blog Opinions libres, octobre 2017, chapitre « Acteurs de l'intelligence artificielle », p. 242.

[10] Par exemple, pour Google/Alphabet qui commercialise le processeur TPU, des services autour de TensorFlow et ses nombreuses banques de données.

ché spécifique. Dans ce cas, les éditeurs de logiciels intègrent de nombreuses briques logicielles et puissances de calculs disponibles sur étagère et développés/maîtrisés par les groupes pivots du numérique.

Pour ces acteurs, la confiance clients représente une problématique majeure (capacité de l'entreprise à déployer une solution à grande échelle, pérennité de la stratégie industrielle, etc.). Au stade de *start-up* ou PME, l'objectif primordial pour les éditeurs de logiciel est de disposer de capacités de financement suffisantes en vue d'assurer leur phase de croissance. Cette phase apparaît déterminante pour obtenir une position dominante dans une économie marquée par des logiques d'hyper-croissance. Cependant, la réalisation de multiples levées de fonds peut s'avérer à double tranchant[11]. Si elle peut se présenter comme un indicateur de l'attractivité d'une *start-up* (et donc du potentiel d'accès au marché de ses solutions et/ou innovations), elle peut aussi être synonyme d'une perte de contrôle (dissolution du capital) et d'une réorientation de la stratégie d'entreprise.

Rappel des différentes étapes de besoins en capitaux des *start-ups* innovantes

De manière générale, les besoins en capitaux pour une *start-up* se décomposent en cinq phases en fonction de la maturité du projet :

- **Idéation du projet**. À ce stade, les financements sont généralement assurés par les fondateurs. À titre d'exemple, ils atteignent en moyenne entre 50 k€ et 100 k€ pour une *start-up* de cybersécurité européenne.
- ***Seed* ou amorçage** : étape marquée par la création d'une structure juridique de l'entreprise. Les fonds d'amorçage sont, en général, de 100 k€ à 500 k€ et ont pour vocation d'accompagner la *start-up* dans son industrialisation/commercialisation.
- ***Early-stage*** représente la phase où la *start-up* commence à disposer de clients et réalise un chiffre d'affaires. Les levées de fonds, appelées Série A et Série B, atteignent en moyenne 0,5 M€ à 5 M€. La mise en place d'un management expérimenté joue un rôle clé dans l'attractivité des fonds d'investissement en capital-risque.
- ***Late-stage*** constitue le point où la *start-up* a démontré la viabilité de son projet grâce à une forte présence commerciale. Les levées de fonds sont alors plus importantes (>5 M€).
- **IPO ou introduction en bourse**. Pour arriver à ce stade, l'entreprise doit d'abord atteindre une taille critique, ce avant de rechercher la rentabilité. Les fonds obtenus en *Late-stage* assurent à la *start-up* un financement des investissements en marketing et R&D pour y parvenir.

Parmi les éditeurs spécialisés en IA, relevons le cas de l'entreprise Palantir, qui a réalisé un CA 2020 de 1,1 Md$. Positionnée sur le segment de la fouille et de l'analyse de données structurées et non structurées, elle propose deux solutions logicielles. La première, « Gotham », son offre historique, cible les clients Défense et du monde du renseignement ; elle représente 56 % de son activité. La seconde (44 % du CA 2020), « Foundry », s'adresse plus spécifiquement aux marchés civils. Fondée en 2004, Palantir a réalisé son introduction en bourse en 2020. L'émergence et la croissance de l'éditeur américain reposent sur différents facteurs, parmi lesquels une expérience forte de ses dirigeants dans l'entrepreneuriat et le

[11] Présentation de Nextflow à l'occasion de la conférence organisée par Atlanpole, « Peut-on développer sa start-up sans lever des fonds ? », 14 juin 2016.

domaine du numérique, et sa proximité avec la communauté du renseignement américain (influence du fonds IN-Q-TEL, accès aux RH spécialisées, débouchés commerciaux). Relevons également que son offre commerciale a été parmi les pionnières sur ce segment d'activités (avec le britannique i2 notamment) et que Palantir a réalisé des levées de fonds importantes et régulières (pour un total 2,6 Mds$[12]), déterminantes dans l'accompagnement de sa croissance et venant soutenir ses activités de marketing, R&D et de rachats d'actifs stratégiques. En effet, Palantir a procédé à l'acquisition de plusieurs entreprises dont les capacités sont venues consolider les équipes RH spécialisées (Voicegem en 2013[13]) et apporter des briques technologiques complémentaires. Tel est le cas des opérations menées sur la période 2014-2016 et ciblant Propeller (*app-making*), Poptip (analyse en temps réel des données issues des réseaux sociaux), Silk (visualisation de données) et Kimo-no Labs (outils de *web-craping*). Rappelons également que Palantir a conclu un accord amiable en 2011 avec le britannique i2 suite à des poursuites judiciaires ouvertes par ce dernier pour détournement de propriété intellectuelle[14].

Pour les *start-ups* européennes, notamment celles spécialisées dans l'IA ou la cybersécurité, l'accès aux financements privés en capital-risque est régulièrement considéré comme un point bloquant, en particulier lors des dernières phases du projet (*Late Stage* et IPO)[15]. La question de l'*exit* est en effet cruciale pour les *start-ups*. Pour rappel, celle-ci peut se réaliser selon trois modalités :

- rachat de la *start-up* par un grand groupe du secteur ;
- entrée dans le capital de *private equity* et de fonds d'investissements spécialisés ;
- introduction en Bourse.

En Europe, la première option semble privilégiée. À l'inverse, il existe encore peu d'exemples d'introduction en bourse ou de capitaux français/européens positionnés sur le financement des dernières phases de croissance des *start-ups*. Il s'agit d'un frein connu au développement de cet écosystème industriel mais sur lequel les politiques publiques nationales ou européennes mettent de plus en plus l'accent.

2.1.3. Entreprises de services du numérique (ESN), un poids renforcé dans la chaîne de valeur

Les prestataires de services impliqués dans l'IA sont principalement les entreprises de services du numérique (ESN, ex-SSII) de taille mondiale. Ils tirent profit de leurs références clients de type « grands comptes » pour déployer des solutions au sein des systèmes d'information. Un des enjeux majeurs des ESN à rayonnement mondial réside dans la capacité de ces dernières à créer une relation de confiance et de proximité avec les clients finaux. Pour ce faire, elles doivent assurer un maillage du territoire, réalisé en partie grâce à l'établissement de sites de services rattachés au groupe. À l'international, où les probléma-

[12] « Palantir Technologies », *Crunchbase*, consulté le 8 septembre 2021.

[13] « Palantir Acqhires Team behind YC Voice Email Startup Voicegem », *Techcrunch,* 16 février 2013.

[14] « Palantir's third black eye: i2 lawsuit settled », *Reuters,* 17 février 2011. I2 a été rachetée en août 2011 par l'américain IBM.

[15] « Web conférence : Financement et développement des startups évoluant dans le domaine de la défense », Fondation pour la recherche stratégique, 9 juillet 2020.

tiques restent similaires, les grandes ESN privilégient une stratégie multidomestique, condition d'une proximité suffisante avec le client final. Dans ce cadre, les ESN sont en mesure d'intervenir en tant qu'intégrateur. Elles se positionnent pour certaines dans le domaine de l'IA afin de renforcer leur offre liée à la transformation digitale à destination de leurs clients historiques (grands comptes privés et publics), multipliant les acquisitions et partenariats avec les acteurs pivots du numérique et les éditeurs de logiciels.

2.2. Des compétiteurs affirmés sur des marchés Défense ?

Les grands groupes mondiaux issus des différentes vagues technologiques de l'informatique et du numérique (IBM, Microsoft, Apple, Amazon, Google, Facebook) apparaissent aujourd'hui comme les acteurs pivots du numérique. Ils se caractérisent par :

- une base clients très importante et variée sur le marché civil ;
- un positionnement sur des activités et des marchés à forte rentabilité (intégration, conseils et services associés) ;
- des investissements significatifs en matière de R&D ;
- pour les plus grands, un *cash-flow* permettant de mener des politiques ambitieuses de rachats d'actifs stratégiques.

À leurs côtés, de très nombreux acteurs spécialisés se sont positionnés sur une partie de la chaîne de valeur à travers le développement d'une offre de services. Or, en plus d'une croissance externe dynamique, les acteurs pivots du numérique mettent en œuvre une politique de partenariats dédiée avec les *start-ups* et PME (par exemple, incubateurs ou laboratoires collaboratifs). Leurs structures internes jugées trop lourdes pour répondre à l'exigence de cycle court de l'innovation, les grands groupes sont amenés à coopérer avec des entités considérées innovantes et plus agiles. Dans ce cadre, les « *digital natives ont été aussi les précurseurs dans la création ou la mise en place de partenariats avec des structures telles que des incubateurs, accélérateurs (…). Elles entretiennent ainsi leur capacité d'exploration de domaines connexes à leur cœur de métier, et favorisent la mise en concurrence régulière de leurs équipes de R&D internes* »[16]. Les *start-ups* et PME apparaissent ainsi pleinement intégrées dans l'écosystème de ces grands groupes. De plus, si les acteurs pivots du numérique sont partenaires de *start-ups* et PME en matière de R&D (*via* la mise en place des systèmes d'innovation adaptés et déployés à l'international tels que des *innovation centers*, *labs*), ils sont également clients et intégrateurs de solutions développées par celles-ci, voire investisseurs *via* des *corporate ventures* spécialisés et reconnus.

La recomposition de la chaîne de valeur en informatique, résultant des évolutions technologiques numériques, amène des acteurs spécialisés du numérique (groupes pivots, éditeurs, ESN) à capter une partie toujours plus importante de la valeur ajoutée réalisée par des entreprises présentes sur des secteurs d'activités dits « traditionnels ». Dans certains cas, ils viennent concurrencer des industries historiques sur leur cœur de métier grâce à l'adoption

[16] Sébastien Tran, « Comment les digital natives sont-elles devenues les entreprises les plus innovantes du monde », *The Conversation*, 10 avril 2018.

d'une organisation « nativement numérique ». Les cas de SpaceX dans le secteur des lanceurs spatiaux ou de Tesla dans celui de l'automobile en sont une parfaite illustration.

Les opérateurs de télécommunication sont aussi confrontés à cette nouvelle concurrence[17]. Principalement acheteurs de solutions sur étagère, notamment dans le cadre de leur relation client (comme les *chatbots* ou services reconnaissance vocale) ou de la maintenance prédictive et de l'optimisation du réseau, les opérateurs de télécommunication pourraient voir leur modèle d'affaire évoluer, en particulier dans le contexte de la place centrale prise par les services informatiques en nuage (et les infrastructures *cloud*) et du déploiement du réseau 5G (opportunités commerciales associées dans le domaine des objets connectés).

La défense n'échappe pas à ces évolutions. Une *partie* des acteurs civils du numérique est entrée dans une logique affirmée de pénétration du marché Défense, réussissant à remporter des contrats majeurs. Palantir se hisse désormais dans le cercle des principaux fournisseurs du DoD, venant concurrencer les acteurs historiques. C'est ainsi qu'en mars 2019, l'entreprise a été sélectionnée dans le cadre du programme de modernisation *Distributed Common Ground System* (DCGS-A) de l'US Army au détriment de Raytheon (un marché évalué à 800 M$)[18]. En 2021, Palantir a remporté la phase 2 de ce programme face à BAE Systems (823 M$)[19]. Bien qu'annulés en juillet et octobre 2021, les contrats *Joint Enterprise Defense Infrastructure* – JEDI (qui a vu s'opposer Amazon à Microsoft) et *Integrated Visual Augmentation System* – IVAS (remporté par Microsoft), évalués respectivement à 10 Mds$[20] et 21,9 Mds$[21], rappellent une nouvelle fois que les acteurs pivots du numérique sont devenus incontournables pour les armées.

En France, relevons l'intérêt croissant des entreprises de service du numérique (ESN) pour le marché Défense. C'est ainsi que les entreprises Atos ou Sopra-Steria sont impliquées à des degrés divers dans le programme Artemis du ministère des Armées. Dans ce cadre, Atos, dont le positionnement sur les marchés Défense résulte en partie de la reprise des activités historiques de Bull[22], a créé une coentreprise avec Thales[23].

Ces évolutions font émerger des problématiques nouvelles pour le client Défense. Le cas du projet MAVEN, impliquant Google et le DoD, et relatif à l'utilisation d'algorithmes de reconnaissance de formes dans le ciblage des drones armés américains, en offre un bon exemple. La médiatisation du projet puis son abandon par Google, sous la pression de ses ingénieurs, sont le reflet des tensions internes consécutives au développement de solutions destinées

[17] « Comment les GAFA s'invitent sur le terrain des télécoms », *Le Monde,* 27 septembre 2021.

[18] « Palantir – who successfully sued the Army – has won a major Army contract », *Defense News,* 29 mars 2019.

[19] « Palantir captures another Army battlefield intell system award », *Washington Technology*, 6 octobre 2021.

[20] « Le Pentagone ouvre à la concurrence le contrat *cloud* JEDI remporté par Microsoft contre Amazon », *L'usine digitale*, 7 juillet 2021.

[21] « U.S. Army pushes back date on Microsoft goggles, affirms commitment to deal », Reuters, 14 octobre 2021.

[22] En mai 2014, Atos a annoncé une OPA sur Bull, valorisant l'entreprise à 620 M€. Cette opération permet au groupe d'étendre ses activités à la fabrication d'équipements et de matériels informatiques (HSM, disques durs, HPC, etc.) dont une partie est dédiée à la Défense, tout en étoffant son offre dans le domaine de l'infrastructure *cloud* et en consolidant sa position dans le domaine de l'intelligence artificielle.

[23] « Thales et Atos officialisent la création d'Athea, 'champion' de l'intelligence artificielle pour la Défense », *Opex360*, 27 mai 2021.

au monde militaire[24]. À ces difficultés s'ajoutent d'autres contraintes inhérentes au marché Défense et venant limiter son attractivité : demande limitée aux clients nationaux, mise en conformité et sécurisation des solutions, logique de différenciation.

3. Groupes de défense : entre clients, partenaires et offreurs de solutions numériques

L'intégration et la maîtrise des nouvelles briques technologiques liées au numérique sont devenues des enjeux majeurs pour les groupes de défense. Celles-ci apparaissent indispensables dans le cadre des plans internes de transformation numérique engagés depuis plusieurs années, visant notamment à moderniser l'outil industriel. Mais elles le sont également au regard de l'évolution des besoins de leurs clients traditionnels et, le cas échéant, de leur positionnement (activités duales). Les groupes de défense sont donc à la fois clients et potentiels offreurs de solutions numériques.

3.1. Une intégration incontournable des technologies numériques

Dans le cas des activités de défense, et en raison des contraintes propres au client étatique, différents enjeux peuvent être distingués en fonction du niveau d'intégration des solutions numériques :

- les solutions numériques génériques disponibles sur le marché civil et qui peuvent concourir à renforcer la productivité d'un groupe de défense ;
- les solutions numériques adaptées aux besoins Défense ;
- les solutions numériques conçues spécifiquement pour les besoins Défense et intégrées dans les programmes d'armement.

IA : la problématique de la gestion et de la valorisation des données pour les groupes de défense

Les acteurs dominants en termes d'intelligence artificielle (AWS, Google, Facebook, par exemple) ont développé des compétences fortes, souvent en capitalisant sur leurs capacités à accéder à des masses de données de natures variées. La gestion et le traitement de ces données leur ont ainsi offert un avantage déterminant eu égard aux types actuels d'IA proposés sur le marché, fondés sur le *machine learning*.

Dans le domaine de la défense, la gestion des données suscite plusieurs problématiques parmi lesquelles : accès (confiance du client étatique à les partager) ; gestion et stockage (protection de données classifiées) ; volume de données (effets « petites séries » des systèmes d'armes déployés).

[24] « Google Hedges on Promise to End Controversial Involvement in Military Drone Contract », *The Intercept*, 1er mars 2019. Cela n'empêche pas Google d'avoir plusieurs contrats avec le DoD (« Forget project Maven. Here are a couple other DoD projects Google is working on », *C4ISRnet*, 13 mars 2019).

En tant que client ou partenaire, les options stratégiques prises par les entreprises se concentrent principalement sur les aspects liés à l'organisation, au management et aux ressources humaines ainsi qu'à l'intégration de solutions sur étagère au sein de l'outil industriel. Les actions mises en œuvre peuvent se résumer ainsi :

- Identification et évaluation des opportunités de création de valeur grâce aux jeux de données disponibles au sein de l'entreprise et mise en place d'une nouvelle gouvernance autour de la donnée (amélioration de son accès en décloisonnant différentes sources de données au sein de l'entreprise et sécurisation de son patrimoine numérique).
- Intégration de solutions sur étagère. Il s'agit d'adopter des solutions destinées avant tout à améliorer/protéger son activité, principalement les fonctions soutien (infrastructure de la société, RH, achats, R&D) et de base (logistique, fabrication/production, distribution, marketing/ventes, services).

Selon cette logique, les groupes de défense déploient les solutions de partenaires ou de fournisseurs et les adaptent selon leurs besoins et leurs contraintes internes. En outre, les groupes de défense sont confrontés à l'intégration croissante d'une main d'œuvre spécialisée sur ces nouvelles technologies. Il s'agit là aussi d'un enjeu majeur, dans un contexte de pénurie et de concurrence exacerbée avec les acteurs pivots et autres groupes au profil d'activités à dominante civile.

Au-delà des usages internes, les actions mises en œuvre par les groupes de défense visent à adapter ou compléter leur catalogue solutions, au risque de voir leur position dans la chaîne de valeur dévaluée, voire d'être évincés de nouveaux marchés de défense d'envergure (liés en partie à l'évolution des architectures en *cloud* des systèmes d'information et de communication). Dans ce contexte, les groupes de défense peuvent être amenés à développer de nouvelles solutions spécifiques en mettant l'accent sur la R&D. Les groupes de défense peuvent également souhaiter se positionner sur d'autres marchés (diversification des activités et ou clients), *via* le rachat d'entreprises spécialisées (politique de croissance externe), et/ou adopter une approche visant à mutualiser les risques et partager les efforts de financement en nouant des accords avec d'autres acteurs, spécialisés ou non (politique de partenariats).

L'expérience des stratégies menées dans les années 2010 par les groupes de défense aux États-Unis et en Europe en matière de cybersécurité offre un premier retour sur les enjeux d'un positionnement sur ces nouveaux domaines. Les dernières stratégies mises en œuvre notamment dans les domaines de l'IA et du *big data* laissent suggérer une approche partenariale privilégiée ayant pour double objectif de consolider un écosystème d'entreprises innovantes autour des groupes de défense et d'intégrer les mécanismes « civils » liés au développement de technologies numériques.

3.2. Positionnement sur les marchés du numérique : retour d'expériences en matière de cybersécurité

Les industriels de la défense ont progressivement pénétré les marchés liés au numérique avec, au milieu des années 2000, la cybersécurité. Identifié comme potentiel relais de croissance, dans un contexte de contraction des commandes d'équipements de défense, le mar-

ché de la cybersécurité a vu l'entrée en force des fournisseurs de la Défense, tels que Raytheon, Lockheed Martin, Northrop Grumman, General Dynamics, BAE Systems, Airbus Defence & Space, Thales, Safran, Leonardo ou encore Rohde & Schwarz. Cette pénétration s'est faite en privilégiant une stratégie de croissance externe, avec pour objectif d'étendre leur portefeuille de produits/services (nouveaux marchés spécifiques) et de clients (acteurs privés et administrations publiques)[25]. Mais en élargissant leur offre de telle sorte à atteindre le marché civil, les groupes de défense se sont retrouvés en concurrence directe avec les acteurs historiques du numérique (acteurs pivots du numérique, éditeurs de logiciels spécialisés et ESN). Par ailleurs, ils se sont positionnés sur un marché dont le modèle économique est différent de leurs activités historiques et qui nécessite des investissements importants en capital-risque.

3.2.1. Aux États-Unis, un retrait progressif des groupes de défense des marchés cyber

Dans ce contexte, après avoir constitué des filiales ou *business units* spécialisées (au fil des rachats successifs), la majorité des groupes de défense américains ont opéré une marche arrière, en cédant ces dernières.

Figure n° 5 : OPERATIONS D'ACQUISITIONS / CESSIONS D'ACTIVITES CYBER ET IT PAR LES PRINCIPAUX GROUPES DE DEFENSE AMERICAINS

	Principales acquisitions activités cyber et associées	Cessions activités cyber et IT
Lockheed Martin	Eagle Group International LLC (2009), Amor Group (2013), Industrial Defender (2014)	Activités IT & Technical Services (2016)
General Dynamics	Vangent (2011), Fortress Technologies (2011), Fidelis Security (2012), Open Kernel Labs (2012), CSRA (2018)	Fidelis Security (2015)
Boeing	Narus (2010), SMSi (2011), Inmedius (2012), Ventura Solutions (2014)	Narus (2015)
Northrop Grumman	M5 Network Security (2012)	Activités IT & missions *support services* (2021)
Raytheon	Oakley Networks (2007), SI Government Solutions (2008), Telemus Solutions (2008), BBN Technologies (2009), Compucat Research (2010), Technology Associates (2010), Trusted Computer Solutions (2010), Applied Signal Technology (2011), Pikewerks Corporation (2011), Hengeller Computer Consultant (2011), Teligny (2012), Blackbird Technologies (2014), Websense (2015), Stonesoft (2016), Sidewinder (2016), RedOwl (2017), Skyfence Network (2017)	Forcepoint (2020)

Par exemple, Lockheed Martin a vendu en 2016 ses activités *IT & Technical Services* à Leidos, se désengageant ainsi des marchés liés aux administrations publiques. Le groupe américain a néanmoins conservé ses activités cyber les plus critiques. Dan Nelson, *VP Corporate commu-*

[25] Kévin Martin, « Cybersécurité : ambitions israéliennes et positionnement des acteurs défense », *Défense & Industries*, n° 6, février 2016.

nication, résumait ainsi les raisons de cette cession : « *The main factors driving the spin-off or sale of our IT and technical services businesses (which include cybersecurity) are changing market dynamics, shifting government priorities, increased competition and industry trends that have led us to believe that these businesses may achieve greater growth, and create more value for our customers by operating outside of Lockheed Martin* »[26]. La situation est similaire pour Boeing avec la vente de sa filiale Narus, cinq ans après son acquisition. Plus récemment, ce sont Northrop Grumman et Raytheon qui ont cédé leurs activités IT ou cyber (entité *IT & Mission support services* pour Northrop Grumman, filiale de cybersécurité Forcepoint pour Raytheon).

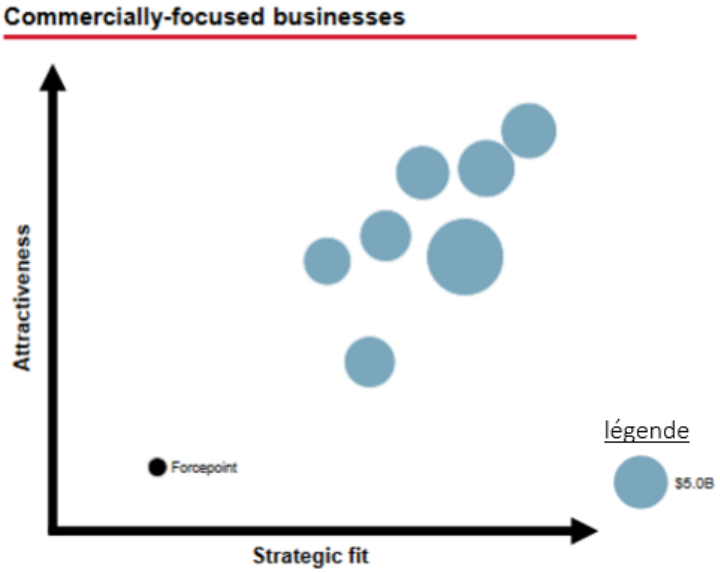
Rappelons qu'avant sa fusion avec UTC, Raytheon fut l'un des rares groupes de défense historiques américains à mener à bien une stratégie de diversification vers les marchés civils de la cybersécurité. Le groupe a su renforcer son offre de solutions existantes avec des capacités cyber (missiles, radars, ISR, C2, etc.) tout en diversifiant ses activités à destination des marchés liés à la transformation numérique (détection et gestion des menaces notamment). Pour ce faire, Raytheon a mené une politique de croissance externe soutenue entre 2007 et 2016 avec 15 acquisitions, pour un montant cumulé supérieur à 3,5 Mds$. Parmi les principales opérations, on peut citer le rachat de l'un des pionniers de l'informatique, BBN Technologies (2009), d'un acteur spécialisé dans la défense et le renseignement, Blackbird Technologies (2014), et d'une entreprise positionnée sur les marchés civils, Websense (2015). Cette politique a donné lieu, dans un premier temps, à une consolidation des activités de cybersécurité au sein d'une division dédiée, Raytheon Cyber Products. Puis, en mai 2015, avec le rachat de Websense, Raytheon franchit un nouveau cap, consolidant au sein d'une filiale de cybersécurité toutes les offres du groupe destinées au marché civil (fusion des actifs de la branche Raytheon Cyber Products avec ceux de Websense au sein de Forcepoint).

La cession de sa filiale commerciale de cybersécurité Forcepoint était toutefois une hypothèse avancée dès 2018-2019. Le rapport annuel 2018 du groupe donnait déjà les éclairages suivants : « *In order to compete effectively, Forcepoint must successfully execute on its growth strategy, including the development of new products and services. If Forcepoint is unable to compete successfully, it may divert financial and management resources that would otherwise benefit our other operations* ». Cette cession interviendra finalement en janvier 2021. En effet, le groupe n'avait plus d'intérêt à poursuivre les investissements nécessaires dans le domaine en raison, notamment, de dépenses d'exploitation élevées liées aux coûts marketing et de ventes (43 % du CA 2019). De plus, les résultats de la filiale cyber apparaissaient très en deçà des autres activités, pénalisant ainsi les performances du groupe ; la marge d'exploitation de Forcepoint atteignait à peine 1,2 % en 2019 contre, en moyenne, 16,4 % pour le groupe[27]. Or, les activités de Forcepoint étaient marginales, représentant seulement 2,25 % du CA total du groupe (soit 658 M$).

[26] « Lockheed Martin Corp. To Exit Commercial Cybersecurity, Double-Down on Helicopters and Combat Jets », *Forbes*, 4 décembre 2015.

[27] Rapport Annuel 2020 Raytheon.

Figure n° 6 : ÉVALUATION DU PORTEFEUILLE DES ACTIVITES COMMERCIALES DE RAYTHEON TECHNOLOGIES



Source : Raytheon Technologies Investor Day[28]

La cession de Forcepoint est également le signe que Raytheon a intégré l'ensemble des technologies liées à la cybersécurité dans ses activités cœur de métier et diversifié le profil de ses RH (effet de bord). En outre, cela traduit un repositionnement sur les marchés du numérique (besoin de concentration des investissements) à l'heure de la fusion entre Raytheon et UTC. Après avoir annoncé en 2018 avoir été sélectionné, *via* son centre R&D BBN Technologies, par la DARPA dans le cadre du programme *Explainable Artificial Intelligence* (XAI), le groupe a noué en 2021 un accord stratégique avec IBM portant sur le co-développement de technologies liées à l'IA et au quantique.

De son côté, General Dynamics semble conserver une approche duale de ses activités cyber et IT, une position unique parmi les principaux fournisseurs de défense américains. L'acquisition fin 2018 de CSRA pour un montant de 9,7 Mds$ confirme cette tendance[29]. Plus généralement, malgré les désinvestissements réalisés sur les marchés civils, tous les acteurs ont conservé des compétences cyber et des offres à destination des clients Défense ou directement intégrés dans leurs offres historiques.

3.2.2. En Europe, une présence consolidée des groupes de défense sur les marchés cyber

En Europe, avec la vente en 2016 de sa filiale Morpho à Oberthur, seul le groupe Safran a opté pour une stratégie de recentrage sur ses activités cœur de métier dans l'aéronautique et la défense. À l'inverse, structurant des capacités sur plusieurs segments, les autres

[28] Greg Hayes (CEO Raytheon Technologies), « Raytheon Technologies Investor Day », 27 juillet 2021.

[29] « General Dynamics completes CSRA acquisition », *Defense News*, 3 avril 2018.

groupes de défense européens sont devenus progressivement des acteurs pivots au sein des bases industrielles et technologiques nationales de cybersécurité[30].

Figure n° 7 : OPERATIONS D'ACQUISITIONS / CESSIONS D'ACTIVITES CYBER ET IT PAR LES GROUPES DE DEFENSE EUROPEENS

	Principales acquisitions activités cyber et associées	Cessions activités cyber et IT
Safran	L-1 Identity (2011), Dictao (2014)	Morpho (2016)
Thales	Sysgo (2012), activités cyber Alcatel-Lucent (2014), Vormetric (2015), Guavus (2017), Gemalto (2019), Ercom (2021)	-
Airbus D&S	Netasq (2012), Arkoon (2013)	-
BAE Systems	Detica (2008), Stratesc (2010), ETI A/S (2010), pôle Intelligence de L-1 Identity, Norkom (2011), Silversky (2014)	-
Leonardo	Vitrociset (2019)	-
Rohde & Schwarz	GateProtect (2014), Adyton Systems (2014), Sirrix (2015), R&S Cybersecurity HSM (2016), DenyAll (2017), Camero-Tech Ltd (2019)	-

Ils profitent d'un environnement concurrentiel plus favorable sur leur marché domestique (présence essentiellement de PME ou d'acteurs pivots du numérique étrangers). Par exemple, en France, selon l'observatoire national de la confiance numérique, Thales et Airbus Defence and Space sont les deux principaux acteurs du secteur, avec des chiffres d'affaires réalisés dans le domaine respectivement de 1,66 Md€ et 520 M€[31]. Ils se placent devant des entreprises spécialisées telles qu'Atos, Idemia ou IBM France.

Cette position a été acquise principalement au travers d'opérations de rachats d'entreprises menées au cours des dix dernières années. Les groupes Thales, BAE Systems et Rohde & Schwarz se distinguent par leur dynamisme en la matière. Le britannique BAE Systems a ainsi investi entre 2008 et 2014 près de 1 Md£ dans le rachat de six entreprises lui permettant de créer une branche « Cyber & Intelligence » (8 % du CA 2020). Le groupe allemand Rohde & Schwarz, qui affiche un CA total de 2,34 Mds€ en 2020, a pour sa part mené sa politique d'acquisition entre 2014 et 2019, ciblant six entreprises. Durant cette période, le groupe a connu une croissance de son CA >20 %, de ses effectifs > 30 % et a réorganisé ses activités en 4 *business units* (Sécurité de l'aérospatiale et de la défense, Cybersécurité, Test & Mesure, Broadcast et médias).

En 2016, Thales s'est engagé dans une démarche de transformation numérique. La cybersécurité, l'IA, le *Big Data* et l'IoT/connectivité sont explicitement identifiés comme les 4 piliers technologiques structurant de cette transformation[32]. Le groupe affirme ses ambitions *via*

[30] Kévin Martin, « Europe et cybersécurité : quelle(s) base(s) industrielle(s) ? », *Revue Défense Nationale*, 2019/4, n° 819, pp. 107-113.

[31] ACN, Observatoire pour la confiance numérique, 2021, p. 3.

[32] « Thales présente ses grandes priorités stratégiques 2018-2021 lors de sa journée investisseurs », *Communiqué de presse Thales*, 6 juin 2018.

une approche sécurité. Outre des réorganisations internes[33], cette politique s'est concrétisée par une vague de rachats d'actifs stratégiques en France et aux États-Unis. Thales a notamment repris en 2014 les activités cyber d'Alcatel Lucent puis réalisé deux acquisitions successives aux États-Unis, visant Vormetric (2015) et Guavus (2017). Le rachat de Gemalto pour 4,8 Mds€, initié en 2017 et finalisé en 2019, marque l'aboutissement de cette politique avec la création d'un nouveau domaine d'activités duales, « Identité et Sécurité numériques ». Celui-ci représente 18 % du CA 2020.

Airbus Defense & Space (deux acquisitions consolidées au sein de la filiale Stormshield) et Leonardo (rachat de l'électronicien Vitrociset) ont plutôt regroupé leurs activités classiques de cybersécurité au sein de divisions dédiées, reflétant leur positionnement ancré dans la défense. Pour Airbus Defence & Space, celles-ci sont concentrées au sein de l'entité Connected Intelligence[34] et, pour Leonardo, au sein de la division Cyber Security rattachée à la Business Unit « Defence, Electronics & Security ».

Figure n° 8 : PLACE DES ACTIVITES DE CYBERSECURITE AU SEIN D'AIRBUS D&S ET LEONARDO[35]

Airbus D&S

Leonardo

[33] Depuis 2011, le groupe poursuit une réorganisation interne de ses activités liées au numérique (cybersécurité, identité, etc.). En 2011, Thales Communications & Security est créé, résultat de la consolidation des entités Thales Communication (spécialisé dans les produits et systèmes d'information et de communications sécurisés) et Thales Security Solutions and Services (systèmes de sécurité des citoyens, des infrastructures critiques et des voyageurs). L'année 2013 est marquée par une réorganisation des activités du groupe autour d'un nouveau modèle reposant sur six Global Business Units (GBU), elles-mêmes regroupées en trois secteurs opérationnels (Défense&Sécurité, Aéronautique, Transport). Dans ce cadre, la branche « Système d'information et de communications sécurisées » relève du secteur Défense&Sécurité. En 2014, Thales a intégré ses compétences en matière de sécurité des systèmes d'information et systèmes d'information critiques pour former un nouveau segment d'activités, « Systèmes d'information critiques et Cybersécurité ».

[34] Relevons qu'Airbus D&S a conservé sa filiale Stormshield, préservant ainsi son canal de ventes spécifique.

[35] Issue des présentations et documents de référence 2020 d'Airbus SE et Leonardo Company.

3.3. Une politique de partenariats désormais incontournable ? Les exemples des technologies liées à l'intelligence artificielle et au big data

Cette stratégie de croissance externe a semble-t-il été privilégiée par les groupes de défense dans le domaine de la cybersécurité au cours de la période 2010-2017, offrant de nouveaux débouchés commerciaux (conservés ou non). Avec la vague technologique liée à l'IA, dont les solutions apparaissent incontournables pour optimiser les performances des solutions existantes, les actions mises en œuvre par les groupes de défense visent davantage un renforcement de leurs capacités internes. Aux États-Unis, les principaux groupes de défense historiques ont renforcé leurs activités de R&D sur les thématiques d'autonomie et de robotisation, profitant du lancement de nombreux programmes du DoD en la matière.

L'accent est également mis sur les partenariats. Les groupes de défense ont modifié ces dernières années leurs structures et leur système d'innovation afin de créer un cadre de coopération adapté avec les acteurs spécialisés de l'écosystème industriel et de recherche dans le domaine du numérique, tel que l'IA. Cette stratégie, qui s'inscrit dans des logiques d'*open innovation*, vise à attirer des *start-ups* du numérique et permet d'assurer une veille technologique dans le domaine (mise en place d'accélérateurs, incubateurs, *challenges* technologiques). Toutefois, les relations nouées en amont ne débouchent pas nécessairement sur un partenariat industriel et commercial pérenne.

Ces initiatives s'appuient sur des structures de type *corporate venture*. Si la pratique est ancienne[36], celle-ci semble de nouveau avoir le vent en poupe auprès des groupes de défense, en particulier dans le contexte du foisonnement des technologies du numérique[37]. Le rôle du *corporate venture* pour un groupe de défense est résumé par Chris Moran, responsable de Lockheed Martin Ventures, comme un outil de détection des technologies émergentes essentiellement à caractère dual et de prise de participation dans des *start-ups* innovantes. L'entrée dans le capital, uniquement sous forme minoritaire, a pour objectif d'orienter la *start-up* vers des solutions répondant aux problématiques défense tout en préservant son *business model* et ses potentiels débouchés commerciaux[38]. Aux États-Unis, Lockheed Martin Ventures a été mis en place dès 2007 (mais le fonds est réellement actif depuis 2016[39]) quand Horizon X (Boeing) et Honeywell venture Capital étaient inaugurés en 2017. En Europe, la dynamique est comparable. Si des *corporate ventures* existent depuis plusieurs an-

[36] « Why defense giants tie in with start-ups. 'Partnering' gives high-tech access or paths apart from Pentagon », *The Christian Science Monitor*, 16 avril 1986.

[37] « Defense Industry Adds Venture Capital to Its Arsenal », *Wall Street Journal*, 5 juillet 2018.

[38] Chris Moran : « *At Lockheed Martin Ventures, the first thing we do is screen the emerging technology we're looking at against the business interests of the corporation. We are looking for what we call "dual use" technologies. However, we're not a huge fund. We're a $200 million fund, and we aim to be a minority shareholder in technology startups. Lockheed Martin Ventures wants to tap into these startups, and ultimately serve as a [market/ bridge] for the emerging technology being created outside the walls of the defense industry. Being a minority shareholder means companies will have the space to sell to the entirety of the aerospace and defense sector. That's a scenario where everyone wins* » (« Lockheed Martin seeks investments not acquisitions in dual-use technology startups », *Lockheed Martin,* juillet 2020).

[39] Cela résulte d'une nouvelle organisation marquée par la nomination de Chris Moran à la tête de la structure (« With new hire at helm, Lockheed Martin Ventures readies to make first investment », *Inside Defense*, 9 septembre 2016).

nées au sein des principaux groupes de défense[40], ceux de Safran et Airbus Group Ventures ont été lancés en 2015. MBDA a mis en place une approche similaire en 2017[41].

Une note du Center for Security and Emerging Technology (CEST) confirme que les groupes de défense disposant d'un *corporate venture* ont plutôt tendance, sur les technologies IA, à réaliser des prises de participation minoritaire que des acquisitions[42]. Par cette approche partenariale, les *corporate ventures* des groupes de défense trouvent leur place aux côtés des fonds spécialisés, bien que leurs capacités financières et leurs objectifs d'investissement diffèrent[43]. Mais des alliances restent possibles, comme le prouve la décision prise par Boeing, en août 2021, de s'associer avec AE Industrial Partners. Son *corporate venture* est ainsi devenu un spin-off, dans le cadre d'un accord conclu avec le fonds d'investissement spécialisé[44]. Cette décision permet à Horizon X de disposer d'un capital plus important (et donc de capacités d'investissements renforcées), Boeing conservant une part majoritaire dans la structure. Les groupes de défense peuvent aussi participer à des fonds d'amorçage spécialisés, comme par exemple Naval Group (PSL Innovation Funds)[45].

[40] Par exemple Saab Coporate Venture a été inauguré en 2001.

[41] Voir MBDA, *Corporate & Social Responsibility Report 2017,* mai 2018. Page 18 : « *In 2017, we increased our engagement in Open Innovation. We set up a corporate-venture capital activity and started to invest in new promising technologies developed by start-ups and small and medium-sized enterprises (SMEs*) ».

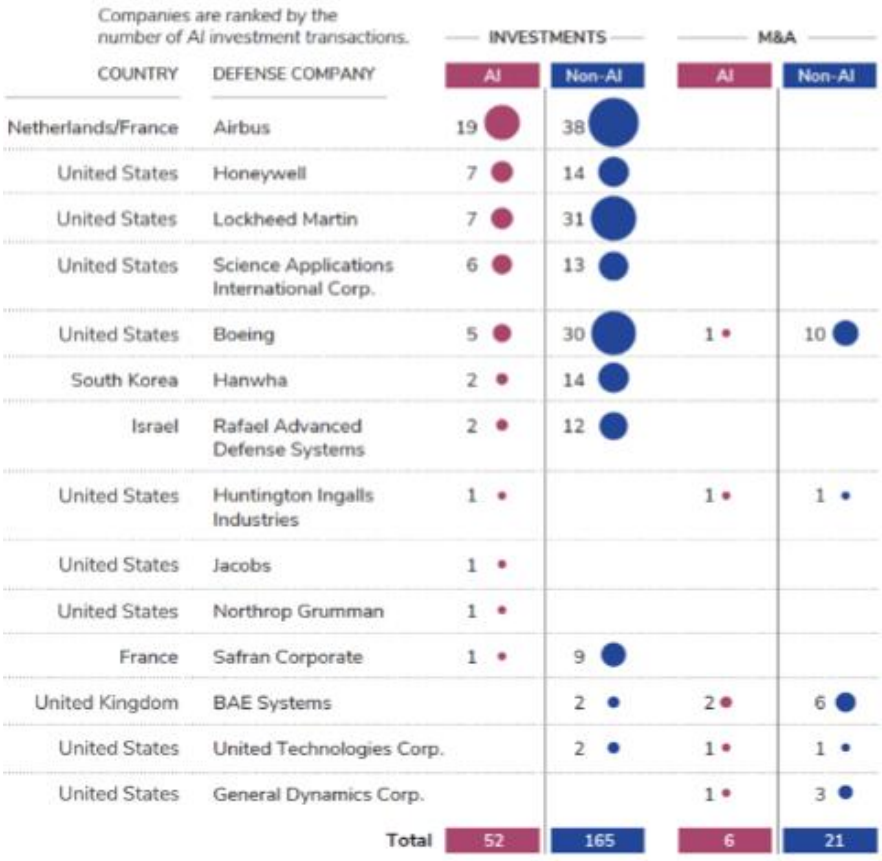
[42] Ngor Luong, Rebecca Gelles, Melissa Flagg, « Mapping the AI Investment Activities of Top Global Defense Companies », *CSET Issue Brief,* Center for Security and Emerging technology, octobre 2021.

[43] « How corporate defense venture funds fit into the VC ecosystem », *Defense News,* 30 janvier 2020.

[44] « Boeing to spin off venture capital arm HorizonX », Reuters, 5 août 2021.

[45] « Naval Group soutient le lancement d'un fonds d'amorçage dédié aux startups », *Mer et Marine*, 29 juin 2018.

Figure n° 9 : PLACE DES INVESTISSEMENTS ET ACQUISITIONS EN MATIERE D'IA PAR LES GROUPES DE DEFENSE : EXEMPLE SUR UNE SELECTION D'ENTREPRISES (2013-2020)



Source : Center for Security and Emerging technology (CSET)

De manière plus classique, les groupes de défense ont engagé une politique de partenariats auprès d'acteurs spécialisés. L'objectif est ici de développer conjointement une offre intégrant des capacités IA ou *big data* et qui sera commercialisée par le groupe de défense. Ce partenariat, qui s'inscrit dans un projet industriel et commercial défini, peut être mené selon deux logiques complémentaires :

- avec des groupes pivots du numérique, participant à la transformation numérique du groupe et de ses activités.
- avec des acteurs de toutes tailles (grands groupes, ETI, PME et *start-ups*), spécialisés majoritairement sur des segments applicatifs.

Tel est le cas du groupe Airbus qui s'est lancé dans la collecte de données lui permettant de s'adjoindre de nouveaux services associés en matière de gestion de flottes et de maintenance prédictive. Il en ressort les nouvelles offres « Skywise » (destinée aux plateformes aéronautiques civiles) et « Smartforce »[46] (destinée aux plateformes aéronautiques militaires), toutes deux développées en partenariat avec des acteurs spécialisés comme Palantir et Alten. En 2018, Lockheed Martin et Amazon Web Services ont noué un partenariat straté-

[46] « Airbus launches SmartForce – services bringing the power of data to military operations », *Airbus Defence and Space*, 16 juillet 2018.

gique dans le domaine des activités de services de station au sol suite à la création d'AWS Ground Station[47].

Par ailleurs, dans le cadre du développement d'une offre de *cloud* sécurisé à destination des armées et des institutions publiques, les groupes de défense européens se sont rapprochés des acteurs pivots du domaine. Thales[48], Leonardo[49] et Fincantieri[50] se sont associés respectivement à Google Cloud, Microsoft et Amazon Web Services pour se positionner sur leur marché national de *cloud* public. Thales et Microsoft sont également partenaires dans le cadre du développement d'une solution de *cloud* de défense, « Nexium Defence Cloud »[51].

Conclusion

Les actions déployées par les groupes de défense dans le domaine du numérique répondent à la fois aux besoins internes de transformation numérique et à une évolution de leurs activités (cœur de métier ou dans un but de diversification). Avec cette adaptation, plusieurs problématiques se font jour, au premier rang desquelles une concurrence particulièrement intense venue d'acteurs au profil d'activités à dominante civile, qu'ils soient acteurs pivots du numérique ou nouveaux entrants. Il s'agit d'une nouvelle donne liée à la place prise par les innovations du numérique dans la définition de nouveaux besoins de défense et dans l'optimisation des performances des systèmes et équipements de défense existants.

Dans certains domaines technologiques matures, comme les infrastructures *cloud* et les services associés, l'avance des acteurs pivots du numérique et l'importance des efforts de financement impliquent *a minima* pour les groupes de défense de mener une stratégie partenariale en vue de proposer des offres conjointes à destination de leurs clients traditionnels (forces armées et institutions publiques). Mais le risque d'être évincé de nouveaux marchés d'envergure est désormais bien réel.

Pour les domaines au niveau de maturité technologique plus faible, par exemple les activités IA hors *machine learning* (IA « explicable » par exemple) ou l'informatique quantique, les groupes de défense mettent l'accent sur la R&D tout en multipliant les interactions avec les écosystèmes civils porteurs des principales innovations. Leur objectif est de bénéficier au plus tôt des avancées technologiques civiles sans dépendre des acteurs pivots du numérique. Cependant, cela présuppose de redéfinir les relations classiques maître d'œuvre / sous-traitants, avec des entreprises qui ne sont pas toujours issues des bases industrielles et technologiques de défense traditionnelles. C'est également un enjeu majeur pour les Armées et les ministères de la Défense nationaux, lesquels cherchent à capter les innovations

[47] « Amazon-Lockheed venture casts shadow on ground station startups », *Spacenews,* 29 novembre 2018.

[48] « Thales et Google Cloud annoncent un partenariat stratégique pour développer conjointement un 'Cloud de Confiance' en France », Communiqué de presse, *Thales Group*, 6 octobre 2021.

[49] « Leonardo and Microsoft: a new partnership for a secure digitization of public administration and national infrastructures », Communiqué de presse, *Leonardo company*, 26 mai 2021.

[50] « Fincantieri and Amazon Web Services team up to power the digitization and competitiveness of Italy with cloud computing », Communiqué de presse, *Fincantieri*, 13 mai 2021.

[51] « Thales and Microsoft partner to develop a unique Defence Cloud solution », Communiqué de presse, *Microsoft*, 12 juin 2018.

auprès de ces nouveaux acteurs, afin d'en faire bénéficier les programmes d'armement *via* une démarche incrémentale.

Les opinions exprimées ici n'engagent que la responsabilité de leur auteur.