Base industrielle de cybersécurité : quels acteurs et enjeux pour la Défense ?

Face aux opportunités et vulnérabilités engendrées par la numérisation croissante de la Défense - et de l'économie plus généralement - les autorités publiques soulignent l'importance de disposer d'une souveraineté numérique. Ainsi, la Revue stratégique de cyberdéfense, publiée en février 2018, rappelle les objectifs suivants : « *La souveraineté numérique peut être entendue comme la capacité de la France d'une part, d'agir de manière souveraine dans l'espace numérique en y conservant une capacité autonome d'appréciation, de décision et d'action et d'autre part, de préserver les composantes les plus traditionnelles de sa souveraineté vis-à-vis de menaces nouvelles tirant part de la numérisation croissante de la société* »[1]. A cet égard, la revue souligne que cette souveraineté passe notamment par la maîtrise de la cybersécurité et le renforcement de « *la base industrielle française et la fondation d'une base industrielle de cybersécurité européenne* »[2].

Cet article se propose de définir les acteurs qui composent cette base industrielle de cybersécurité et ce, dans le contexte des besoins liés à la Défense.

Marché(s) de la cybersécurité : quelques segmentations

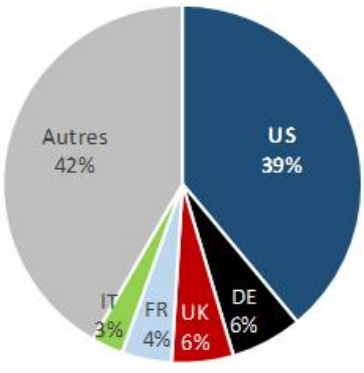
En l'absence de définition unanimement partagée et en raison d'un marché très évolutif, de nombreuses estimations du marché de la cybersécurité sont disponibles, variant considérablement en fonction du périmètre qui lui est appliqué. Par exemple, pour 2017, le cabinet Gartner évalue ce marché à 89 Mds$[3] quand il atteint les 138 Mds$ pour Markets&Markets[4].

La multitude des enjeux et des dynamiques liés au marché de la cybersécurité peut être mis avant à travers différentes segmentations. Une première est réalisée par type de solutions :

- grande famille : solutions matérielles, logicielles ou prestations de services de conseils de formation, de gestion de risques, d'audit, de test de pénétration, etc ;
- type de systèmes à sécuriser: infrastructures fixes, équipements de mobilités, bases de données, systèmes industriels, systèmes d'armes, etc. ;
- fonction de sécurité assurée : pare-feu, antivirus, chiffrement, authentification, etc. ;
- ou encore par niveau de sécurité recherché (de la technologie du paiement sans contact aux solutions de cryptographie Secret Défense).

La segmentation peut être aussi géographique : la demande en matière de cybersécurité est très hétérogène en fonction des zones et des pays. Le niveau de maturité d'un marché est étudié à l'aune de plusieurs critères, qu'ils soient liés à la situation économique, à son environnement géopolitique et cyber, la réponse à la menace cyber notamment. A titre d'exemple, selon les données communiquées par l'*European Cyber Security Organisation* (ESCO), les États-Unis représenteraient près de 40% du marché mondial en matière de cybersécurité. Les principaux marchés européens, pris individuellement, ne dépasseraient pas les 6%[5].

Marchés nationaux de la cybersécurité, en %



Source : ECSO

Une demande portée par les marchés civils

Au niveau national, une approche par type de clients « Défense » et « civils » semble nécessaire. Elle permet d'ajuster l'analyse aux enjeux propres de chaque client, que ce soit notamment en matière de :

- volume du marché ;
- maturité du marché ;
- besoins et contraintes spécifiques.

Toutefois, la distinction Défense/civil n'est pas figée et des caractéristiques communes peuvent apparaître.

La Défense renvoie à un marché très mature nécessitant les technologies les plus complexes. Liées à des domaines de souveraineté, les contraintes sont également plus fortes en termes de sécurité et les contrats portent souvent sur de petites séries (principe de différenciation des solutions). L'accès à ce type de marché est donc limité et nécessite souvent des regroupements d'acteurs industriels de tailles diverses pour répondre à des besoins techniques complexes. Pour ces raisons, la Défense reste un marché de niche pour les acteurs industriels, et ce, malgré des taux de croissance affichés substantiels.

Les marché civils offrent quant à eux les taux de rentabilité les plus élevés. Ils tirent donc le marché de la cybersécurité. En revanche, des spécificités se font jour entre trois catégories[6] :

- administrations publiques et gestionnaires d'infrastructures vitales : il s'agit ici de marchés faisant essentiellement l'objet de règlementation. L'accès y est donc limité et contraignant ;
- grands groupes et ETI : les exigences de sécurité sont fixées individuellement. Marchés les plus rentables mais les problématiques d'internationalisation des sites des groupes et ETI poussent ces derniers à recourir à des prestataires

en matière de cybersécurité reconnus sur le marché et disposant de solutions innovantes ;

- PME & consommateurs : les budgets mobilisables sont relativement faibles, les clients ont recours à des solutions référencées comme leader du marché.

Par ailleurs, les marchés civils peuvent être appréhendés à travers une approche métier. L'objectif est alors de prendre en compte le contexte, les règles juridiques et normes techniques spécifiques s'imposant à celui-ci (secteur bancaire, santé, e-administration, etc.).

Enfin, les intégrateurs, en plus d'être des acteurs industriels, se présentent également comme une catégorie de clients importants. Dans ce cas, ils peuvent se positionner comme intermédiaires sur de nombreux marchés.

La cybersécurité recouvre donc des solutions très variées. La demande est disparate et la Défense apparaît comme un marché de niche. Ce constat explique pourquoi, au-delà des groupes de défense, des profils variés d'acteurs industriels disposent ou développent une offre en matière de cybersécurité, notamment à destination du marché Défense ou pouvant satisfaire aux exigences des clients Défense.

Les spécificités propres à chaque acteur industriel semblent de moins en moins marquées (logique d'intégration verticale des activités), néanmoins la création d'une typologie d'acteurs offre une vision d'ensemble des écosystèmes impliqués dans la cybersécurité ainsi que des différents modèles économiques. Or, la compréhension de ces modèles par les pouvoirs publics semble déterminante pour mener des actions de soutien et de renforcement d'une base industrielle de cybersécurité.

Le positionnement des industries de défense sur le marché de la cybersécurité

Les industriels historiques de la défense figurent en tant que leaders du marché auprès du client Défense. Ils bénéficient de la relation privilégiée nouée avec ce dernier, de capacités d'intégration et de maîtrise d'œuvre de programmes complexes ainsi que d'une empreinte internationale. Les groupes de défense privilégient un mode de vente directe auprès du client Défense. Par ailleurs, en assurant une présence locale via l'adoption d'une stratégie multidomestique, ils nouent également des relations directes avec les clients étrangers. Dans ce cadre, la stratégie de pénétration de marché peut passer par la création *ex-nihilo* d'une filiale (société de droit local) ou par l'acquisition d'un acteur local, qu'il soit consultant ou éditeur. Ainsi, quand la R&D est réalisée localement, les groupes se positionnent en tant que « fournisseur domestique » des clients Défense (solutions de souveraineté).

En outre, dans un contexte de contraction des commandes d'équipements de défense au milieu des années 2000, ces acteurs avec notamment aux États-Unis, Raytheon, Lockheed Martin et Northrop Grumman (pour ne citer que les principaux), en Europe, BAE Systems, Airbus Defence & Space, Thales, Leonardo et Rohde & Shchwarz ont affiché progressivement des ambitions de positionnement sur les marchés civils (administrations publiques & OIV et grands groupes principalement), et ceci, malgré une très forte intensité concurrentielle.

Le développement d'une offre en matière de cybersécurité peut alors dériver pour ces derniers de :

- « *spin-in* » de technologies défense ;
- stratégie de croissance externe. Les groupes de défense ont été à l'origine de nombreuses opérations de rachats d'entreprises au cours de ces dix dernières années, avec pour cœur de cible les acteurs de la cybersécurité (PME, ETI et filiales de grands groupes)[7] ;
- Établissement de partenariats stratégiques avec des acteurs spécialisés.

Cette extension de leur gamme de solutions permet aux groupes de défense d'atteindre de nouveaux marchés, en diversifiant leur portefeuille clients vers des administrations civiles, voire des acteurs privés (grands groupes). La consolidation de leur offre de cybersécurité passe ensuite par les axes stratégiques suivants :

- Création d'une ligne d'activités (Business Unit, BU) dédiée à la cybersécurité. Par cette stratégie, les groupes visent en priorité le marché domestique de la Défense, les administrations civiles (nationales et internationales) et les opérateurs d'importance vitale (OIV). L'intégration de solutions sur étagère, via le développement de partenariats avec les leaders mondiaux de la cybersécurité, permet de renforcer cette ligne d'activités.
- Mise en place d'une filiale cybersécurité dédiée, laquelle consolide les activités des acteurs spécialisés rachetés par le groupe de défense. Il peut ainsi bénéficier de leurs canaux de ventes, mais, si ces entités nouvellement acquises disposent d'une « marque » forte (très bonne visibilité auprès des clients finaux), celle-ci peut être préservée. Les acquisitions d'entreprises spécialisées ciblent généralement des acteurs positionnés sur les marchés civils, permettant au groupe de défense de diversifier son portefeuille client et se positionner sur les marchés les plus attractifs (grands groupes).

A l'inverse, les groupes de défense sont de plus en plus confrontés à la concurrence des entreprises issues du secteur du numérique et des télécommunications. Dans ce contexte, ils doivent notamment être en mesure de résoudre les problématiques liées à l'absence de synergie avec leur cœur d'activités. Plus particulièrement, ils doivent adapter leur stratégie en prenant en compte les caractéristiques propres à la cybersécurité tel que le cycle court de l'innovation.

Ainsi, plusieurs acteurs défense ont opéré un retrait des marchés civils[8]. Par exemple, avec la vente de sa filiale Morpho à Oberthur, le groupe Safran a opté pour une stratégie de recentrage autour de ses activités dans l'aéronautique et la défense[9]. Aux États-Unis, Lockheed Martin a notamment fait le choix de sortir des marchés administrations publiques et IT après la cession en 2016 des activités IT & Technical Services à Leidos.

Marchés de la cybersécurité et de l'armement : approche comparée

	Cybersécurité	Armement
Demande (principaux clients)	Disparate	Limitée aux clients gouvernementaux
État de la concurrence	Forte intensité concurrentielle	Variable selon les segments
Barrières à l'entrée	Faibles	Fortes
Cycle d'innovation	Court	Long
Ruptures technologiques (fréquences)	Élevée	Modérée

Le groupe américain a néanmoins conservé ses activités cyber les plus critiques[10].

La montée en puissance des entreprises issues du numérique

Depuis quelques années, les entreprises issues du secteur du numérique (au sens large, électronique inclue) affirment leurs ambitions sur le marché de la cybersécurité, dont client Défense. Celles-ci disposent de plusieurs avantages concurrentiels :

- base clients très importante sur le marché civil (grands groupes et administrations publiques) ;
- positionnement sur des activités à forte rentabilité (intégration, conseils et services associés) ;
- capacités d'investissement élevées (politique de fusion-acquisition) ;
- politique de partenariat dédiée avec les start-ups et PME spécialisées ainsi que les incubateurs, laboratoires collaboratifs, etc. Les structures des grands groupes sont trop lourdes pour répondre à l'exigence du cycle court de l'innovation qu'impose la cybersécurité, amenant ces derniers à coopérer avec des structures innovantes et agiles (start-ups et PME). Or, les entreprises du numérique disposent ici d'un avantage par rapport aux groupes de défense dans la coopération avec ces start-ups et PME car elles sont pleinement intégrées dans leur écosystème.

Même si leur catalogue d'offres tend à se « lisser » en raison notamment du développement des activités d'infogérance et de services de *cloud computing*, des disparités subsistent entre les différents acteurs du numérique. Ces disparités, liées au positionnement d'origine sur le marché, permettent de comprendre les stratégies actuellement mises en œuvre.

Fabrication de matériels et d'équipements : les acteurs *pure-players*, c'est-à-dire les entreprises spécialisées dans la production de matériels et d'équipements, offrent des solutions sécurisées *by design*. Dans ce cadre, ils privilégient le développement en interne de technologies de sécurité (brevets) tout en établissant des partenariats stratégiques avec des acteurs spécialisés de la cybersécurité. Toutefois, la sécurité est aujourd'hui encore majoritairement perçue par les clients finaux comme un coût supplémentaire, et non comme un avantage compétitif. A terme, ce constat devrait évoluer, les produits sécurisés *by design* constitueront un élément déterminant de différenciation de l'offre (intégration de clauses de sécurité). En effet, le développement des réglementations nationales et internationales sur plusieurs marchés spécialisés semble inéluctable (systèmes industriels connectés et objets connectés notamment).

Aujourd'hui, l'accès aux marchés pour les fabricants de matériels et d'équipements est principalement réalisé en B2B (*Business to Business*) et se traduit par des accords négociés entre les systémiers-intégrateurs mondiaux ainsi que par la vente indirecte (solutions intégrées dans le catalogue d'intermédiaires spécialisés). Néanmoins, la volonté des fabricants de matériels et d'équipements de diversifier leurs activités au profit d'une offre de services a tendance à faire évoluer la relation avec les systémiers-intégrateurs : d'un canal de vente historique, celle-ci tend dorénavant vers un partenariat (avec pour certains cas des ambitions de croissance externe).

Les systémiers-intégrateurs, presque exclusivement américains, cherchent quant à eux à diversifier leurs activités. Dans ce cadre, une stratégie d'intégration verticale est largement privilégiée, avec pour cible les éditeurs de logiciels et les prestataires de services informatiques. Ils profitent ainsi d'une situation dominante grâce à leurs activités IT à partir desquelles ils proposent des solutions de cybersécurité dédiées mais aussi des services associés.

Édition logicielle : les grands groupes mondiaux *pure-player* historiquement positionnés sur le marché de la cybersécurité, hormis SAP et Sophos, sont non-européens et cotés en bourse.

En phase de croissance externe, ils profitent d'importantes réserves de *cash*. Leur objectif est d'intégrer en permanence des mécanismes et des solutions de sécurité dans leur offre et de disposer d'une main d'œuvre qualifiée en nombre suffisant.

À leur côté, les PME disposant de technologie(s) de niche représentent dans ce contexte des cibles privilégiées des éditeurs de logiciels, mais aussi des fabricants de matériels et d'équipements ainsi que des groupes de défense. Pour ces acteurs, la confiance client représente une problématique majeure. Malgré un coût élevé, ces derniers ont ainsi largement recours aux processus nationaux de certification et de qualification, afin de garantir un niveau de sécurité auprès des clients.

De plus, à leur stade (start-up ou PME), l'objectif primordial des éditeurs spécialisés est de disposer de capacités de financement élevées (capital-risque, fonds publics, entrée en bourse, etc.) en vue d'assurer une croissance interne importante et disposer le plus rapidement possible d'une visibilité critique sur le marché. En effet, la vente indirecte en B2B constitue le canal de vente privilégié. Dans ce cadre, l'entreprise doit tisser un réseau composé de systémiers-intégrateurs, de revendeurs et de grossistes. Or, pour intégrer des solutions dans leur catalogue, ces derniers s'appuient essentiellement sur :

- la réputation commerciale de la solution (référencement, qualification, certification, etc.);
- la capacité de l'entreprise à déployer la solution à grande échelle.

Dans une moindre mesure, les éditeurs disposent également du canal de vente *online* dont la qualité dépend principalement du référencement web.

Prestation de services : les prestataires de services sont principalement les entreprises de services du numérique (ESN). Parmi les ESN, les groupes de taille mondiale tirent profit de leurs références clients type « grands comptes » pour déployer des solutions de sécurité des SI. Ces entreprises développent notamment des offres de services de sécurité managés autour de SOC/CERT. À leur côté, subsistent les ESN à rayonnement local, principalement positionnées sur les marchés des ETI/PME et administrations (collectivités territoriales par exemple).

Un des enjeux majeurs des ESN réside dans leur capacité à créer une relation de confiance et de proximité avec les clients finaux. Elles doivent ainsi assurer un maillage du territoire, en partie réalisé grâce à la création de sites de services locaux rattachés au groupe. À l'international, les problématiques restent similaires. Les ESN privilégient une stratégie multidomestique, condition d'une proximité suffisante avec le client final. Elles sont alors en mesure d'intervenir en tant qu'intégrateur, aux côtés des systémiers-intégrateurs historiques (catégorie fabricants de matériels et d'équipements informatiques).

Enfin, la sélection par les clients finaux dépend également des solutions intégrées. Dans ce cadre, les ESN multiplient les partenariats et accords de distribution avec les acteurs mondiaux dans leur domaine, essentiellement américains, car mieux reconnus par les clients finaux, en partie grâce à leur

présence au sein de *benchmarks* réalisés par des cabinets anglo-saxons tels que ceux du cabinet Gartner[11].

La catégorie des prestataires de services recouvre aussi les acteurs industriels spécialisés dans les travaux de R&D. Leur modèle économique repose sur la licence de brevets (royalties). Ces acteurs sont pleinement insérés dans l'écosystème de recherche local en prenant part à de nombreux projets de recherche (et menés bien souvent en partenariat). Ce modèle économique impose de détenir de nombreux brevets (problématiques liées aux dépôts) qu'il convient ensuite de revendre, principalement aux acteurs relevant de la catégorie fabrication de matériels et d'équipements. L'entreprise peut aussi développer son modèle économique sur la vente de services associés au développement d'un produit. Dans ce cas, celle-ci a aussi recours au réseau de vente indirect.

Les opérateurs de télécommunication

Grâce à leurs moyens techniques et financiers, les opérateurs de télécommunication ont pénétré progressivement le marché de la cybersécurité par le biais d'offres de solutions de sécurisation des données et de services de cloud. Maîtrisant les « tuyaux » d'information, l'axe de développement privilégié consiste à sécuriser l'information qui y circule.

L'acquisition d'entreprises prestataires de services et l'établissement de liens de partenariats avec les fournisseurs spécialisés (systémiers-intégrateurs, éditeurs de logiciels et fabricants de matériels et d'équipement) forment le socle de développement de leurs activités de cybersécurité.

Le rachat d'activités industrielles de cybersécurité permet aux opérateurs de télécommunication de créer ou renforcer une nouvelle BU cyber. Celle -ci peut alors étoffer les offres historiques de communication des opérateurs par l'intégration de solutions et de services de cybersécurité, ou opérer directement sur le marché de la cybersécurité (solutions dédiées). La multiplication des partenariats avec les entreprises spécialisées du secteur a pour objectif d'intégrer des solutions de cybersécurité reconnues par les clients au sein des offres historiques et/ou intégrer une brique technologique dans le développement d'une offre 100% de cybersécurité (*via* la BU cyber).

Une filière de cybersécurité européenne ?

Le secteur industriel français de la cybersécurité a connu d'importantes mutations au cours des dernières années. Les pouvoirs publics français ont notamment multiplié les initiatives visant à renforcer ce secteur[12]. En parallèle, le paysage industriel français de la cybersécurité a vu l'entrée de nouveaux acteurs (issus de la Défense, sécurité numérique, etc.). Enfin, de nombreuses opérations de fusion-acquisition[13] ont participé à la consolidation des activités de cybersécurité des entreprises tête de pont de la filière (Thales-Gemalto, Atos-Bull, Airbus Cybersecurity, Sopra-Steria, Idemia, etc.).

Malgré ces évolutions, le secteur industriel de cybersécurité français semble toujours atomisé[14]. Or, l'environnement déjà hautement concurrentiel voit l'émergence de filières nationales en Chine, en Israël, au Royaume-Uni, ou encore en Allemagne. Rappelons par ailleurs que les États-Unis disposent du tissu industriel le plus dense dans le domaine de la cybersécurité. Bénéficiant notamment de la taille du marché domestique, la base industrielle de cybersécurité américaine comprend les principaux acteurs mondiaux : systémiers-intégrateurs (Cisco, FireEye, IBM, Microsoft, HP Dell), éditeurs de logiciels *pure-player* (Symantec, etc.), ou encore groupes de défense disposant d'une offre cyber (Raytheon, Lockheed Martin, General Dynamics, etc.).

Dans ce contexte, la Commission européenne s'est emparée des sujets numériques et *in fine* de la cybersécurité. Les initiatives prises par cette dernière s'inscrivent dans le cadre de la Stratégie de cybersécurité de l'Union européenne[15], laquelle affiche notamment les objectifs de développement de capacités industrielles et technologiques en matière de cybersécurité. Ainsi, la communication relative à la création d'un « marché numérique unique » (*Digital Single Market*)[16] rappelle ces enjeux et illustre la volonté de la Commission européenne d'influencer la structuration du marché européen de la cybersécurité à travers une évolution du cadre réglementaire et des initiatives public-privé.

Des avancés concrètes ont eu lieu *via* notamment l'adoption de règles européennes, avec l'objectif de construire un véritable marché européen de la cybersécurité. Par exemple, l'adoption du règlement EIDAS, abrogeant la directive 1999/93/CE relatif à la signature électronique en Europe[17], permet d'harmoniser les normes européennes sur le segment de l'identification électronique. De plus, l'adoption, le 6 juillet 2016, de la directive *Network and Information Security* (NIS)[18], devrait permettre de renforcer la sécurité des réseaux et des systèmes d'information européens. Cette dernière est également susceptible d'avoir des effets sur la structuration du marché.

Les avancées vers un marché unique européen de la cybersécurité semblent tangibles. Néanmoins, plusieurs problématiques demeurent en raison de divergences entre États membres. Premièrement, la mise en place de schémas de certification de solutions de cybersécurité à l'échelle européenne s'annonce délicat[19]. Deuxièmement, l'absence de définition partagée entre États membres en matière d' « industrie de cybersécurité européenne » représente un point dur majeur [20].

Quelle politique industrielle de défense en matière de cybersécurité ?

La compréhension des enjeux industriels propre aux différents acteurs offre un premier aperçu des dynamiques actuellement à l'œuvre. Il ressort de ce constat la difficulté d'adopter des mesures de soutien à grande échelle tant les problématiques et modèles économiques des acteurs industriels de cybersécurité divergent. De plus, le développement d'une capacité nationale de cybersécurité, et plus spécifiquement cyberdéfense, est inhérent à la présence au préalable d'une industrie de défense et du numérique ainsi qu'à l'adoption d'une stratégie nationale spécifique, intégrant un volet industriel. Quelques pays, dont la France, ont pour l'heure mis en œuvre une politique industrielle dédiée à la constitution d'une base industrielle et technologique de cybersécurité (BITC). Ainsi une première lecture de ces orientations de politiques publiques fait ressortir les points suivants :

- développement de formations universitaires adaptées permettant de disposer de ressources humaines en qualité et nombre suffisant (à même d'accompagner la croissance du secteur) ;

- politique de R&D dédiée (plan d'investissements, feuilles de route industrielles) ;
- Adoption de nouvelles règlementations contraignantes en matière de cybersécurité avec pour objectif de stimuler la demande et conséquence de structurer de nouveaux marchés ;
- multiplication de mesures incitatives en vue d'attirer les investissements en capital-risque ;
- mise en place de clusters régionaux réunissant notamment les acteurs industriels et leurs centres de R&D, les pôles de formation, les laboratoires de recherche, les clients finaux et les capitaux-risqueurs.

En outre, l'orientation civile des acteurs industriels de la cybersécurité impose au ministère des Armées de repenser le dialogue Etat-Industries dans ce domaine. Ce constat pose d'ailleurs plus généralement la question de la capacité des Armées à intégrer les innovations venues du civil, en particulier dans les domaines liés à la cybersécurité et à l'intelligence artificielle. C'est notamment l'objectif affiché par la LPM 2019-2025 : « *capter en cycle court l'innovation issue du marché civil, en tirant partie de la révolution numérique (…). Cette démarche s'appuiera largement sur la construction d'un écosystème d'innovation, interne au ministère des armées et connecté avec les écosystèmes d'innovation civils* »[21]. La création d'une agence de l'innovation placée au sein de la DGA est censée apporter une première réponse à cette problématique, comme le rappelle, Florence Parly, ministre des Armées : « *La nouvelle agence de l'innovation aura donc pour mission d'organiser les échanges avec cet écosystème de l'innovation, qui est plutôt civil* »[22].

Dans ce contexte, le renforcement de la base industrielle de cybersécurité française et européenne, nécessaire pour garantir un niveau de souveraineté numérique, dépasse le seul cadre d'une politique industrielle de défense. Celle-ci semble devoir s'inscrire dans une action plus transversale afin de bénéficier d'effets de levier pour la structuration du secteur. La prise en compte, dans cette approche transversale, des besoins spécifiques liés à la Défense apparaît essentielle pour atteindre les objectifs affichés.

KÉVIN MARTIN
Chargé de recherche
Pôle Défense & Industries, FRS
k.martin@frstrategie.org

Notes

1.Secrétariat général de la défense et de la sécurité nationale (SGDSN), *Revue stratégique de cyberdéfense*, 12 février 2018.

2. *Ibid*.

3. « Gartner Forecasts Worldwide Security Spending Will Reach $96 Billion in 2018, Up 8 Percent from 2017 », *Gartner,* 7 décembre 2017.

4. « Cybersecurity Market worth 231.94 Billion USD by 2022 », *Markets&Markets*, juillet 2017.

5. ECSO, *European cybersecurity industry proposal for a contractual public-private partnership*, juin 2016.

6. Cette segmentation s'appuie sur celles adoptées par diverses études : TechUK, *Assessing Cyber Security Exports Risks,* November 2014 ; Pierre Audoin Consultants, *Competitive analysis of the UK cybersecurity sector*, juillet 2013 ; AFDEL, *Livre Blanc cybersécurité : hisser les acteurs français au niveau de la compétition mondiale*, juin 2014.

7. En Europe on peut, par exemple, évoquer les acquisitions d'Airbus (Arkoon, Netasq), de Thales (activités cyber d'Alacatel Lucent, Vormetric, Guavus, Gemalto), BAE Systems (Detica, Stratesc, ETI A/S, Norkom, SilverSky) ou Rohde & Schwarz (GateProtect, Adytom Systems, Sirrix AG, DenyAll).

8. « Top five U.S. defense contractors bungle commercial cybersecurity market opportunity », *CSO*, 28 janvier 2016.

9. Cession de Morpho par le groupe Safran, réponse du Ministère de la défense à la question écrite n°23397, *JO Sénat* , 23 février 2017, p. 737.

10. « Lockheed Martin Successfully Closes Transaction to Separate and Combine IT and Technical Services Businesses with Leidos» *Communiqué de presse Lockheed Martin,* 16 août 2016.

11. Cf. Gartner Magic Quadrant.

12. D'Elia Danilo, « La cybersécurité, entre bien public et marketing de la peur », *in Quelles stratégies face aux mutations de l'économie mondiale ?* , Etude de l'IRSEM, n°38, avril 2015.

13. Depuis 2011, l'auteur dénombre près de 100 opérations de fusions-acquisition dans le domaine de la cybersécurité impliquant des acteurs industriels français.

14. Alliance pour la confiance numérique, *L'observatoire de la filière de la confiance numérique en France*, 2017.

15. Communication de la Commission européenne, *Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé*, 7 février 2013.

16. Communication de la Commission européenne, *Stratégie pour un marché unique numérique en Europe*, 6 mai 2015.

17. Parlement européen et Conseil de l'Union européenne, *Règlement N° 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur*, 23 juillet 2014.

18. Parlement européen et Conseil de l'Union européenne, *Directive 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union*, 6 juillet 2016.

19.Mazucchi Nicolas, *2018, une année charnière pour l'Europe dans le cyber ?*, Note de la FRS, 22 janvier 2018.

20. Cf. Secrétariat général de la défense et de la sécurité nationale (SGDSN), *Revue stratégique de cyberdéfense*, 12 février 2018 : « *La construction d'une base industrielle de cybersécurité et cyberdéfense [européenne] se heurte aujourd'hui à deux difficultés (…) La seconde difficulté est une certaine différence de conception entre États membres de l'Union européenne sur la nature d'une entreprise européenne »,* p.120.

On notera que cette problématique n'est pas spécifique à la cybersécurité, la question renvoyant à celle de la BITD européenne. Voir à ce sujet Hélène Masson (ed.), Christian Mölling, Keith Hartley, Martin Lundmark, Krzysztof Soloch, *Defining the « European Defence Technological and Industrial Base »: Debates & Dilemmas (I)*, Note de la FRS, 26 juillet 2013.

21. Ministère des Armées, *Projet de loi de programmation militaire 2019/2025—Rapport annexé*, 2018, p. 54.

22. « Entretien de la ministre des Armées », *Usine nouvelle*, 31 mai 2018.