Europe et cybersécurité : quelle(s) base(s) industrielle(s) ?

Dans un contexte marqué par d'importantes évolutions technologiques, le paysage industriel européen de la cybersécurité connaît une structuration progressive, suite notamment à différentes vagues de consolidation. Cependant, une diversité des profils compose ce que l'on peut appeler une « base industrielle et technologique de cybersécurité » (BITC). La présence d'industries de défense aux côtés d'entreprises issues du monde du numérique aux *business models* différents complique ainsi la lecture du secteur. En matière de concurrence, les BITC européennes font face à l'hégémonie des groupes de cybersécurité américains, la structuration d'une filière tournée vers l'innovation en Israël et l'émergence de nouveaux acteurs (Chine notamment). Les défis européens sont alors multiples : création d'un leadership international, soutien à l'innovation, structuration d'un marché unique, etc. Fondé sur une approche comparée des bases nationales de cybersécurité en Europe et à l'étranger (Etats-Unis et Israël), cet article propose de revenir, dans un premier temps, sur les acteurs composant une base industrielle et technologique de cybersécurité ainsi que sur les éléments clés à l'origine de son développement. Dans un second temps, il tente d'éclairer les capacités européennes en la matière et ses spécificités.

Une BITC composée d'acteurs aux profils variés

L'offre de cybersécurité recouvre des solutions très diverses et la demande est caractérisée par une forte disparité, allant du citoyen-consommateur jusqu'aux ministères de la Défense. Le périmètre de la cybersécurité est en effet très large. Pour être appréhendé, il nécessite de recourir à plusieurs segmentations de marché, que ce soit selon les solutions[1] ou les clients[2].

Eu égard à ce large périmètre, plusieurs profils d'entreprises composent la BITC. Parmi les acteurs pivots, les fabricants de matériels et d'équipements informatiques et électroniques ont vu l'apparition des grands systémiers-intégrateurs (IBM, Microsoft, HP, Cisco, Dell, etc.) aux côtés d'équipementiers (Qualcomm, ST Microelectronics, Schneider Electrics, Siemens, etc.). Les éditeurs de logiciels spécialisés (Symantec, CheckPoint, Kapersky, etc.) et les entreprises de services du numérique (ESN) jouent également un rôle majeur, ces dernières profitant de la proximité clients pour déployer une large gamme de solutions de cybersécurité (Atos, Capgemini, Sopra-Steria etc.). Si une partie des opérateurs de télécommunication et des groupes de défense ont fait le choix de se positionner sur ce marché, leur entrée est plus tardive et elle s'est faite principalement par opérations de croissance externe.

Le tableau ci-après offre une vision d'ensemble des écosystèmes impliqués dans la cybersécurité et permet d'illustrer les différentes stratégies de positionnement des entreprises. On notera néanmoins, pour les acteurs pivots issus de la défense ou du monde du numérique, que les stratégies de positionnement tendent à se lisser en raison d'une logique de plus en plus partagée d'intégration verticale des activités.

BITC et quête d'innovation

Les spécialisations des BITC nationales, qu'elles soient orientées plutôt produits/solutions, spécialisées dans un sous-secteur, etc. sont héritières des politiques industrielles spécifiques menées dans différents secteurs (défense, électronique, semi-conducteurs, informatique, etc.), essentiellement dans les années 1970-2000. Ainsi, le développement d'une capacité nationale de cybersécurité s'appuie-t-elle d'abord sur la présence au préalable d'une industrie de défense, du logiciel, de l'informatique hardware (PC & composants, calculateurs, cartes et puces électroniques, etc.), des télécommunications, du conseil, etc.

Les stratégies nationales dédiées à la cybersécurité, et incluant un volet industriel, sont quant à elles assez récentes. Une analyse de ces dernières, menée dans les principaux pays leaders du secteur, nous permet de retenir des conditions de succès communes :

- Prise de conscience des risques cyber par les acteurs publics ;
- Maturité des marchés domestiques de la cybersécurité (public et privé) ;
- Grands groupes leaders, têtes de pont de filière ;
- Adoption d'un arsenal juridique contraignant (objectif de susciter la demande) ;

*Article publié dans la revue *RDN*, avril 2019.

Principales stratégies de positionnement	Marchés ciblés
Groupes de défense	
Entrée sur le marché : diversification des activités au profit de la cybersécurité, dans un contexte de contraction des commandes via *« spin-in »* de technologie de défense et politique de croissance externe. Consolidation des activités : création d'une B.U. cyber et/ou création d'une filiale cyber pour conserver/créer une « marque » forte (via regroupement des activités et/ou croissance externe). Logique de partenariat : intégration de solutions leaders sur le marché/développement conjoint d'offres avec les acteurs leaders mondiaux (systémiers intégrateurs, éditeurs de logiciels, prestataires de services).	Marché : Défense (marché et activités historiques) + Diversification des clients au profit des acteurs « civils » : administrations publiques et grands groupes. Ventes directes, en qualité de systémiers-intégrateurs.
Fabricants de matériels et d'équipements	
Systémiers intégrateurs Entrée sur le marché : presque exclusivement tous américains, des fabricants ayant privilégié une diversification des activités au profit d'une offre de services, suivant une stratégie d'intégration verticale. Fourniture d'offres packagées. Consolidation des activités de services et édition logicielle via une stratégie d'acquisition agressive. Le cas échéant, intégration des solutions de sécurité reconnues comme leaders du marché.	Marchés : Grands comptes prioritairement (administrations publiques, grands groupes).
Equipementiers – pure player Entrée sur le marché : sécurisation *by-design* et développement d'offres de services de sécurité associées. Développement de solutions sécurisées *by design* grâce à une politique de R&D soutenue. En recherche de taille critique pour réaliser des économies d'échelles. Logique de partenariats : services et intégration de solutions sécurisées.	Marchés : intermédiaires (systémiers-intégrateurs) via partenariats + Renforcement de la relation directe avec les clients finaux.
Éditeurs de logiciels	
Grands groupes Acteurs historiques positionnés sur le marché de la cybersécurité, presque tous non européens et cotés en bourse. Intégration permanente de mécanismes et solutions de sécurité dans leur offre. D'une logique de licence à une offre SaaS. Très forte logique marketing (référencement des solutions, etc.). Croissance externe via l'acquisition ciblée d'éditeurs de logiciels disposant de briques technologiques, soutenue par des réserves de cash importantes.	Canaux de ventes indirects *via* ESN et systémiers-intégrateurs. Vers le développement de relations directes avec les clients finaux (vente de services associés).
Start-ups, PME Recherche d'une croissance interne rapide soutenue par la quête de financement (levées de fonds, cotation en bourse, etc) en vue d'assurer une bonne commercialisation des solutions (certification, catalogage, marketing, etc.).	Développement des canaux de vente indirects en B2B *via* les ESN.
Prestataires de services	
Entreprises de services du numérique (ESN) à rayonnement mondial Entrée sur le marché : proximité clients assurée grâce à la multiplication d'établissements secondaires et/ou croissance externe. Logique d'intégrateur : sélection des offres de sécurité les plus réputés du marché (bénéficiant d'une reconnaissance auprès du client final grâce à un bon catalogage/référencement) et/ou des acteurs en mesure de déployer des solutions à l'échelle mondiale. Développement d'offres de sécurité managées autour de SOC.	Marchés : Grands comptes prioritairement et administrations publiques. + Développement vers les marchés Défense (liés principalement aux activités de soutien général).
Cabinets de conseil à rayonnement local/régional Proximité Client/Offre en matière d'audit et de conformité : accent mis sur le développement des ressources humaines (consultants).	Marchés : PME-ETI et collectivités territoriales.
Prestataires de services de R&D Entrée sur le marché : généralement issus de laboratoires de recherches publics ou privés (spin-off). Modèle basé sur la licence de brevets. Concentration des efforts RH dans la R&D et multiplication des projets de recherche menés dans l'écosystème local.	Marchés : Fabricants de matériels et d'équipements essentiellement, en vente directe et indirecte (royalties issus des brevets).
Opérateurs télécom	
Entrée sur le marché : Intégration de solutions de sécurité au sein des offres « classiques » de communication via des partenariats avec des entreprises spécialisées et/ou développement de solutions en interne. Développement d'une offre de cybersécurité en interne (création d'une B.U.) ou par croissance externe ciblant des prestataires de services spécialisés.	Clients historiques + Marchés liés aux prestations de services en matière de cybersécurité (en concurrence avec les ESN notamment).

- Mise en place d'une politique de R&D dédiée (plan d'investissements, feuilles de routes industrielles) ;
- Formations universitaires adaptées de qualité et en nombre suffisant (accompagnant la croissance du secteur) ;
- Soutien au développement des entreprises technologiques à travers l'afflux de financements privés adaptés (capital-risque) ;
- Regroupement des activités de cybersécurité au sein de clusters réunissant l'ensemble de l'écosystème (industriels, centres de R&D, laboratoires de recherche, pôles de formation, clients finaux, capitaux-risqueurs).

La pérennisation de l'activité des start-ups, et plus généralement des acteurs innovants en matière de cybersécurité, est aujourd'hui une des priorités des Etats qui affichent une ambition dans le secteur. Le regroupement sous forme de cluster est désormais privilégié dans l'ensemble des stratégies nationales avec pour objectif, entre autres, d'attirer les financements privés en capital-risque. En effet, l'émergence des start-ups est marquée par une phase de développement de solutions adaptées à des défis de sécurité spécifiques. Avantage compétitif déterminant dans le secteur, cette stratégie de niche peut leur offrir une forte croissance (identification sur le marché en tant que pionnier). Ces start-ups font alors souvent l'objet d'acquisition par des grands groupes (systémier-intégrateur et éditeurs de logiciels essentiellement). Pour accompagner cette hyper-croissance, la présence en nombre et en volume des différents investissements en capitaux-risques, encouragés par des fonds d'investissements publics amorceurs adaptés, est donc primordiale.

Parmi les leaders mondiaux, le cas israélien illustre bien cette problématique. Avec près de 420 entreprises[3] (contre 148 en 2011), la BITC israélienne profite de la présence d'acteurs têtes de pont, notamment dans les secteurs de l'édition logicielle (CheckPoint et CyberArk) et de la défense (Elbit Systems). Mais elle se distingue par le nombre de créations de start-ups (depuis 2014, moyenne >65 start-ups cyber par an) et de PME récentes positionnées sur des segments relais de croissance (SCADA industriels, Objets connectés, Renseignement d'origine cyber, etc.). Ces start-ups bénéficient, pour réussir leurs levées de fonds, de l'accompagnement par de très nombreux investisseurs. En 2018, elles ont ainsi capté plus de 1 Md$ d'investissements en capital-risque, soit près de 20 % du total mondial réalisé dans le secteur de la cybersécurité[4] (2e place derrière les États-Unis qui en concentrent ~50 %). Ce montant, qui a augmenté de manière exponentielle ces dernières années, coïncide avec l'inauguration du cluster CyberSpark situé à Beersheva. Signe de son attractivité, le cluster accueille près d'une cinquantaine de centres de R&D étrangers tels qu'IBM, Intel, Microsoft, Siemens, etc., qui profitent notamment de l'écosystème national de recherche et de soutien publics[5].

Quelles actions européennes en matière de renforcement des capacités industrielles de cybersécurité ?

La Commission européenne s'est emparée des sujets numériques et *in fine* de la cybersécurité, ses initiatives s'inscrivant dans le cadre de la « Stratégie de cybersécurité de l'Union européenne »[6]. Elle affiche parmi ses objectifs le développement de ressources industrielles et technologiques en matière de cybersécurité. La communication relative à la création d'un « marché numérique unique »[7] rappelle également ces enjeux. Elle montre surtout que les initiatives de la Commission européenne visent une meilleure structuration du marché européen, et ce, à travers une évolution du cadre réglementaire[8]. Sur le plan de la structuration de l'offre, les avancées paraissent plus modestes. La mise en place d'un partenariat public-privé pour la cybersécurité (PPP) est toutefois notable. Il s'est matérialisé en juin 2016 par la création de l'*European Cybersecurity Organisation* (ECSO), composée d'acteurs et associations d'industriels, clusters, administrations publiques, clients et opérateurs. L'ECSO est censée générée, d'ici 2020, 1,8 Md€ d'investissements dans le secteur de la cybersécurité, l'UE s'engageant à consacrer 450 M€ dans le cadre du programme cadre de recherche et développement H2020 (financement qui doit susciter en théorie des investissements 3 à 4 fois supérieurs par les membres d'ECSO).

En Europe, des capacités concentrées en France, au Royaume-Uni et en Allemagne

A l'image du marché, les BITC européennes restent fragmentées. Une analyse des principales bases industrielles (françaises, britanniques et allemandes) fait par ailleurs ressortir la problématique de l'ancrage des BITC à un domaine d'action public plus large (sécurité, industrie 4.0, numérique, etc.).

En France, les dernières données communiquées par l'association d'industriels ACN[9], font état d'une BITC composée de près de 850 acteurs, principalement des PME et microentreprises. Elle réalise un chiffre d'affaires (CA) national hors export cumulé de 9 Mds€ pour environ 60 000 emplois. Ces données intègrent les activités issues de la sécurité numérique et ce, au sens très large, avec la vente de matériels et d'équipements tels que ceux liés à la biométrie, détection, terminaux de paiement, etc. Les leaders en la matière sont par exemple Idemia (ex Morpho - Oberthur Technologies), Gemalto ou Ingenico. La BITC française se trouve ainsi écartelée entre le monde du numérique et celui de la sécurité.

En Allemagne, la BITC est caractérisée par la position dominante d'entreprises intervenant en particulier sur le segment des infrastructures réseaux (Siemens, Deutsche Telekom, Secunet, etc.), et plus généralement, par la présence d'un tissu dense de PME et ETI. Représentée par les associations *Bitkom* et *Teletrust*, la BITC allemande fait partie intégrante du projet d'industrie 4.0, lancé en 2011 par le gouvernement.

Selon la dernière étude publiée par les autorités nationales[10], la BITC britannique regroupe 846 acteurs dont Sophos, le premier éditeur de logiciel spécialisé en Europe (CA total de 641M£ ; 3 300 employés). L'ensemble des entreprises du secteur emploie 31 000 personnes pour un CA cumulé de 5,68 Mds£. Pleinement intégrée au monde du numérique, la BITC est représentée par l'association d'industriels *TechUK*, qui agit comme interface privilégiée avec le gouvernement dans le cadre des initiatives de partenariat public-privé en la matière.

Des acteurs de niche sont également présents en Italie, Finlande, Espagne, Suède ou encore en Estonie.

Les groupes de défense européens, acteurs pivots des BITC nationales ?

Structurant des capacités sur plusieurs segments, les groupes de défense européens sont devenus progressivement des acteurs pivots au sein des BITC nationales.

Ce positionnement privilégié des principaux groupes de défense européens est principalement le fruit d'opérations de rachats d'entreprises menées au cours des dix dernières années, avec pour cœur de cible les acteurs spécialisés de cybersécurité, généralement des PME, ETI ou filiales de grands groupes. Le britannique BAE Systems a ainsi initié une politique de croissance externe particulièrement dynamique entre 2008 et 2014, investissant près de 1 Md£ dans l'acquisition de six entreprises spécialisées (Detica, Stratesc, ETI A/S, pôle Intelligence Service Group de L-1 Identity Solutions, Norkom Technologies, Silversky). Airbus a réalisé en 2012-2013 les acquisitions successives d'Arkoon et Netasq, quand le français Thales procédait au rachat des activités cyber d'Alcatel Lucent (2014), Vormetric (2015), Guavus (2017) et Gemalto (initié fin 2017). L'allemand Rohde & Schwarz a repris cinq entreprises entre 2014 et 2017 (GateProtect, Adyton Systems, Sirrix AG, R&S Cybersecurity HSM et DenyAll). En revanche, Leonardo a essentiellement tiré profit de technologies de défense pour développer son offre de cybersécurité, à travers notamment les activités de sa filiale électronicienne Selex[11]. Le groupe italien va aussi renforcer ses activités de cybersécurité à travers l'acquisition de l'entreprise de défense Vitrociset (janvier 2019).

La stratégie de croissance externe déployée par les principaux groupes de défense aura permis d'étoffer rapidement leur portefeuille de solutions de cybersécurité et d'étendre leur positionnement vers les marchés civils (administrations publiques et grands groupes). Leur CA généré dans le secteur de la cybersécurité les place désormais parmi les leaders nationaux. Ce rôle d'acteurs pivots au sein des BITC leur offre une place prédominante dans l'écosystème d'innovation, plutôt porté par des entreprises au profil civil[12]. Dans ce cadre, les groupes de défense ont multiplié les alliances stratégiques avec les leaders mondiaux, grands groupes civils et acteurs spécialisés (Airbus-Atos, Thales-Cisco, BAE Systems-02, Rohde&Schwarz-Radisys etc.). En structurant leur coopération, ils nouent également des relations privilégiées avec les start-ups spécialisées. A titre d'exemple, Thales est devenu, en 2017, partenaire référent de l'incubateur Station F pour la cybersécurité quand BAE Systems a étendu, fin 2016, son partenariat avec le cluster londonien CyLon puis lancé en 2018 *The Intelligence Network*[13], renforçant ses liens avec le monde de l'innovation civile dans le domaine de la cybersécurité.

Le concept de base industrielle et technologique de cybersécurité (BITC) est récent et fait référence à une pluralité d'acteurs. Au niveau européen, il suscite des problématiques spécifiques comme celle liée à la création d'un marché unique, condition pour une meilleure consolidation du secteur. La convergence des politiques dédiées entre Etats détenteurs d'une BITC apparaît également déterminante dans le contexte de la présence sur le marché européen d'acteurs étrangers aux positions dominantes.

Kévin MARTIN
Chargé de recherche, FRS
k.martin@frstrategie.org

Notes

1.Familles de solutions proposées (matériel, softwares, services), fonctions de sécurité assurées (pare-feu, antivirus, chiffrement surveillance réseau, etc.), niveau de sécurité offert (IoT, secret Défense, etc.), systèmes sécurisés (infrastructures fixes, équipements de mobilités, bases de données, systèmes industriels, etc.).

2.Approche sectorielle (banque, finance, santé, e-administration, etc.), Défense, Civils (administrations publiques, gestionnaires d'infrastructures vitales, grands groupes, ETI, PME consommateurs), géographique (maturité des marchés, règles juridiques, labels, etc. selon pays/régions).

3.Start-Up Nation Central, *Israel cybersecurity industry in 2017*, 2018.

4.« A look back at the Israeli cyber security industry in 2018», *Techcrunch*, 30 janvier 2019.

5.Ministry of Economy and Industry, State of Israel, *R&D Centers – Investments models in Israel,* 2017.

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

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

8.Par exemple règlement EIDAS, RGPD ou de la directive NIS. La mise en place de certificats européens de cybersécurité pourrait être une étape supplémentaire en vue de réduire les barrières à l'entrée engendrées notamment par les coûts de certification et de labellisation nationaux.

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

10.Department for Digital, Culture, Media & Sport, Margot James MP, *UK Cyber Security Sectoral Analysis*, 30 octobre 2018.

11.Depuis septembre 2015, la filiale a fusionné avec le groupe.

12.Élément rappelé par la ministre des Armées, Florence Parly, dans le cadre de la création de l'Agence de l'innovation de défense : *« La nouvelle agence de l'innovation aura donc pour mission d'organiser les échanges avec cet écosystème de l'innovation, qui est plutôt civil* ». *Cf.* « Entretien de la ministre des Armées », *Usine nouvelle*, 31 mai 2018.

13.« BAE Systems Proposes a New Collaborative Approach to Cybersecurity », *CBR*, 9 juillet 2018.