LUC RENOUIL (89) *directeur du développement et de la stratégie défense-sécurité de Bertin Technologies-groupe CNIM*

DÉVELOPPER UNE INDUSTRIE FRANÇAISE ET EUROPÉENNE DE CONFIANCE

La création aux niveaux français et européen d'une industrie de la confiance forte et autonome nécessite « l'union sacrée » des acteurs publics et privés et le développement d'un écosystème industriel dans lequel coopèrent des entreprises de toute taille.

La transformation numérique promet des lendemains qui chantent et des gisements de croissance et de productivité. En France, la part de PIB issue du numérique est de plus de 100 milliards d'euros, la valeur du commerce en ligne depuis 2007 a été multipliée par trois, le taux d'équipement en tablettes entre 2011 et 2013 a été multiplié par quatre. Dans notre pays, les ventes de smartphones ont été multipliées par six depuis 2008, la capacité de stockage de données a été multipliée par douze depuis 2005 [1], enrichissant de manière radicale l'expérience client et révolutionnant les organisations.

« Les attaques informatiques croissent de près de 50 % par an depuis trois ans »

LENDEMAINS QUI CHANTENT

Avec l'accès à Internet et la mobilité, on a démultiplié la productivité des cadres, l'accès aux données de l'entreprise depuis le monde extérieur, en calquant les usages de l'entreprise sur les usages personnels pour s'assurer l'adhésion des salariés. Avec le *cloud*, c'est-à-dire l'informatique externalisée, l'usine à gaz informatique interne est rationalisée par des professionnels sur leur propre infrastructure optimisée. Qui aurait, de nos jours, l'idée de produire soi-même son électricité ? À chacun son métier. Les dépenses en *cloud* progressent toujours sur un rythme supérieur à 15 % en *cloud* privé et près de 30 % en *cloud* public [2]. Avec l'Internet des objets, c'est la promesse de contrôler à distance les états des matériels connectés qui se profile, sans que soient encore assurées la fiabilité et la non-compromission de ces objets.

UN RISQUE QUI PEUT DEVENIR UNE CHANCE

L'existence de menaces persistantes sur la sécurité informatique est devenue le cauchemar des responsables de sécurité informatique et désormais des dirigeants. L'augmentation du nombre des attaques informatiques est de près de 50 % par an depuis trois ans.

La sécurité n'est pas un business de la peur, mais suppose une coopération efficace entre acteurs publics – en particulier les régulateurs, en tant que primo-intervenants et tours de contrôle de la menace, garants du bien public de sécurité – et acteurs privés, qui doivent intégrer la sécurité dans leur modèle économique comme un risque propre, avec ses conséquences au plan concurrentiel, au plan humain et sur la continuité d'activité.

Cette coopération entre public et privé est le point fort culturel du modèle écono-

REPÈRES

Récemment, la société Sony a subi un vol massif de données *via* Internet. Puis TV5 Monde a été victime d'un *malware* provoquant la discontinuité d'activité pour un groupe média moyen, vraisemblablement utilisé comme vengeance de nos engagements diplomatiques. Les services de renseignement américains auraient eu accès aux outils de génération de secrets de la société Gemalto, pourtant un des acteurs essentiels de la sécurité informatique. Des événements qui montrent que le risque numérique peut devenir un sérieux obstacle au progrès de la transformation numérique.

© VIPERAGP / FOTOLIA

Les dépenses en *cloud* augmentent de 15 à 30 % par an.

mique français, quand elle est bien opérée. La loi de programmation militaire et le plan cybersécurité ont donné à la France une impulsion décisive depuis 2014. Mais tout est à mettre en place, et s'il y a une contrainte à concilier les différentes réglementations nationales pour une société privée aux multiples implantations nationales, autant démontrer que l'approche française est efficace.

CROISSANCE FORTE ET DOMINANCE ANGLO-SAXONNE

Selon les chiffres de différents cabinets d'études, le marché de la cybersécurité sera de près de 100 milliards de dollars en 2015, près de 170 milliards de dollars en 2020. Il atteint près de 3 milliards d'euros en France et plus de 30 milliards d'euros en Europe.

Ce marché ne se limite pas à la stricte sécurité informatique mais la dépasse, puisque de nombreux systèmes informatiques industriels du « cyberespace » peuvent être défaillants ou attaqués (automobile, aéronautique, exploitation des infrastructures, etc.). Sa croissance selon les régions du marché est supérieure à 10 % annuellement. Le marché est dominé par l'Amérique du Nord et l'Europe, mais l'Asie prend de l'importance.

La cybersécurité est un marché globalement calqué sur le marché du logiciel et des services associés, plus que sur le marché de la sécurité. Dans les services, les missions confiées à des tiers de confiance sont en très forte croissance. Elles correspondent à l'externalisation du service de supervision de la sécurité informatique.

Le marché des produits comprend notamment le marché de l'édition de logiciels et, dans une moindre mesure, des produits de sécurité (aussi appelés *appliances*). C'est un marché industriel, pour lequel les positions et les cycles d'investissements sont dominés par les grands éditeurs anglo-saxons.

« Le marché de la cybersécurité est calqué sur celui du logiciel et des services associés »

UN RECOURS CROISSANT À L'EXTERNALISATION

Avec l'évolution vers l'externalisation des infrastructures et des services, les modèles économiques se rapprochent. Les prestataires doivent proposer une expertise outillée différenciante au moindre coût.

Les marchés verticaux introduisent eux-mêmes une segmentation, car l'usage de l'informatique et ses enjeux ne sont pas les mêmes dans le domaine de l'énergie ou dans le domaine bancaire.

Finalement, la grande particularité du domaine de la cybersécurité est sa forte adhérence au besoin gouvernemental. Ce besoin doit être pensé comme l'occasion de promouvoir des offres et des fonctionnalités qui favorisent le tissu industriel domestique.

Le domaine industriel des services informatiques et du logiciel reste dominé par les acteurs américains, qui regroupent plus

LOI DE PROGRAMMATION MILITAIRE

L'article 22 de la loi de programmation militaire concerne les systèmes d'information. L'objectif de cet article et des décrets afférents est de définir les systèmes d'information concernés et des règles efficaces, soutenables et adaptées aux métiers et spécificités des opérateurs industriels dont la défaillance ou l'attaque pourrait porter atteinte à la sécurité de l'État, et de garantir la bonne articulation de ce nouveau dispositif avec les réglementations préexistantes. D'où la mise en place au début de l'année 2015, pour chaque domaine d'activité (eau, énergie, finances, transports, etc.), de groupes de travail rassemblant, autour de l'ANSSI, les opérateurs d'importance vitale, les ministères coordonnateurs et les autorités sectorielles.

UN ÉCOSYSTÈME EN ÉBULLITION

Dans le domaine des fusions acquisitions et des opérations en Bourse, nous avons assisté en France à une opération emblématique en octobre 2015 : le rachat de l'éditeur américain Vormetric par Thales pour près de 400 millions de dollars. Mais cela n'atteint pas les sommets de l'écosystème anglo-saxon. L'éditeur Sophos a été coté à Londres et valorisé pour 1,6 milliard de dollars, Microsoft a racheté la société israélienne Adallom, spécialisée dans la sécurité du *cloud* pour 320 millions de dollars, tandis que Cisco a acquis Open DNS pour 635 millions de dollars. Ce sont des dizaines d'opérations de plusieurs dizaines de millions de dollars qui ont eu lieu à un rythme s'accélérant au cours des douze derniers mois. Pour ce qui est du capital investissement, près de 2 milliards de dollars ont été investis dans des *start-ups* cyber aux USA l'an dernier et plus de 1 milliard de dollars au premier semestre 2015. Signalons que plusieurs levées de fonds aux USA ont concerné des montants de plusieurs dizaines de millions de dollars, Google Capital ayant investi 100 millions de dollars sur Crowdstrike.

de 70 % des principaux acteurs (IBM, Microsoft Oracle, tous intéressés de près ou de loin à la sécurité informatique).

La même domination s'observe dans le domaine de la cybersécurité, puisque les cinq plus gros acteurs du secteur sont Symantec, IBM, Intel Security, Trend Micro (Japon) et EMC. Leur activité approche ou dépasse largement le milliard de dollars annuel. L'émergence de Trend Micro, voire de Kaspersky, est peut-être le signal d'une remise en cause de cette hégémonie.

UN PLAN DE TRAVAIL COMPLET À METTRE EN ŒUVRE

En France, la cybersécurité, en première approche, c'est 700 entreprises dont 100 se spécialisent réellement sur des produits et services de haute technologie. Une vingtaine tout au plus exportent. Il faut être champion sur son territoire pour pouvoir aller à l'international.

Au sein de Hexatrust, cluster de vingt-cinq éditeurs de cybersécurité français créé en 2014[3], rassemblant plus de 1 500 employés, nous générons une croissance annuelle de 25 % à 30 %.

Dans le contexte de dialogue public-privé évoqué préalablement, nous préconisons qu'une image globale de la situation du tissu industriel soit élaborée et partagée par l'ensemble des acteurs du secteur.

L'écosystème européen de la cybersécurité se limite encore à quelques actions communes de recherche et développement. Il faut une volonté industrielle et normative forte, comme ce fut le cas avec Airbus, pour dégager des capacités d'investissement européen à la hauteur de l'enjeu industriel. Les initiatives d'investissement qui pourraient être prises en France et en Europe, visant à donner aux meilleures innovations les moyens de passer à l'échelle industrielle globale, seront bienvenues.

« En France, la cybersécurité, c'est 700 entreprises »

CONSTRUIRE UN MARCHÉ EUROPÉEN DE LA CYBERSÉCURITÉ

Le problème n'est pas tant la nationalité des entreprises que la richesse de l'écosystème qui doit être construit. Il faut rendre la cybersécurité attractive pour y attirer des investisseurs. Cela exige croissance et rentabilité. La première exige d'ouvrir les horizons de marché : le marché européen de la cybersécurité doit devenir une réalité. Si la seconde tarde à se concrétiser, cela fragilisera l'ensemble du dispositif, sauf présence d'acteurs capables de consolider l'ensemble. Les initiatives doivent venir du monde industriel. Le rachat par Thales de Vormetric (déjà précédé de celui de Sysgo par le même Thales) doit être suivi d'autres opérations avec d'autres acteurs au plan européen pour donner crédit à la démarche. Les annonces d'investissements importants de Cisco et Microsoft en France doivent être suivies. La rentabilité des acteurs de la filière doit pouvoir être améliorée, pour faciliter leur solidité et leur capacité d'investissement autonome.

© GEORGEJMCLITTLE / FOTOLIA

En France, le nombre de tablettes a été multiplié par 4 entre 2011 et 2013.

AGIR SANS DÉLAI

L'achat public doit, comme aux États-Unis, être utilisé en France comme un accélérateur de croissance pour les acteurs industriels nationaux. Les intérêts essentiels de sécurité permettent de justifier cette approche.

À court terme, des solutions hybridant intégrateur français et éditeurs étrangers permettent de préserver nos intérêts et de développer la filière sans hypothéquer l'avenir. Ainsi, la mise en place de la notion de service souverain pour garantir une solution sur la base de composants étrangers est l'approche choisie par Orange en France (comme par IBM en Chine). L'analyse de code doit être autant que possible privilégiée. Les données doivent être stockées en France. Il faut assurer un juste report des contraintes opérationnelles dans les contrats des donneurs d'ordre vers les fournisseurs. Enfin, comme tout domaine industriel, la cybersécurité devra intégrer des modèles d'externalisation du risque vers les assureurs, ce qui permettra peu à peu au risque cyber de se financiariser et, par là, de pénétrer transversalement l'entreprise.

IL N'Y A DE RICHESSE QUE D'HOMMES

Les prévisions font état d'un besoin de plusieurs centaines de milliers de spécialistes par an dans les prochaines années en Europe[4]. Les filières de formation en France dans le développement informatique sont encore trop peu développées et n'incluent pas suffisamment la sécurité informatique. La cybersécurité appelle des transferts de compétences, notamment des spécialistes d'autres domaines en retournement comme les systèmes embarqués et les réseaux.

Techniquement, la sécurité n'est pas que périphérique, mais doit être pensée en profondeur. Le contrôle d'exécution et la sécurité des plateformes sont des domaines techniques à réinvestir. La cryptologie a de beaux jours devant elle, car elle reste un ultime rempart important, et porte ses propres innovations comme la cryptologie dite homomorphe, qui permet de confier les calculs à un tiers sans que celui-ci ne connaisse ni les données ni les résultats. En termes d'innovation, l'analyse comportementale dans le flot de données va faire la différence à l'avenir. Développer de telles solutions requiert des profils de très haut niveau, capables de faire le pont entre statistiques et comportement des acteurs.

En termes d'ingénierie, le principal défi sera de passer à une conception produit intégrant plus fortement la sécurité et les usages. Une mauvaise qualité de développement logiciel est la pire menace informatique qui existe. Nous devons développer les métiers industriels du logiciel : programmation et développement produit, test et validation, incluant les méthodes et outils formels générateurs de productivité dans une logique de certification et de qualité produit.

Enfin, il faut adapter les dépenses en marketing, gestion du produit, commercial et juridique à une vision ambitieuse de conquête. Un cycle de vie du produit dynamique et une adaptation native à l'environnement du client doivent être le standard et non l'exception pour nos produits. ■

« L'achat public doit être utilisé comme un accélérateur de croissance »

© BERNARD ROUSSEAU / THALES

Thales a acheté Vormetric pour près de 400 millions de dollars.

1. Mc Kinsey, *Accélérer la mutation numérique des entreprises : un gisement de croissance et de compétitivité pour la France.*
2. Source IDC 2015.
3. Dont Bertin Technologies est une des fondatrices.
4. Le besoin aux États-Unis est évalué à 1 million de personnes à former annuellement.