Quels enjeux et défis régaliens dans le numérique, notamment en matière de cybersécurité ?

Par Patrice CAINE
Président-directeur général de Thales

La cybersécurité ne doit pas être seulement vue comme une formalité contraignante pour protéger nos systèmes d'information. Elle est, pour ma part, la condition du succès de notre économie numérique. Nous nous arrêterons d'abord sur la variété des menaces et la multiplicité des contextes que recouvre le terme de « cybersécurité ». Puis nous nous interrogerons sur la capacité de la France et de l'Europe à assurer leur souveraineté numérique alors que les équipements et logiciels venant des États-Unis et de Chine irriguent tous les systèmes d'information.
Elles le pourront, selon moi, à condition de structurer une filière française et européenne et d'y injecter les moyens financiers et humains nécessaires. Car les compétences existent, en particulier dans des groupes industriels comme Thales. Reste donc aux autorités, tant au niveau français qu'européen, à sonner la mobilisation générale pour que nous puissions nous affirmer en tant que leaders dans des domaines aussi structurants que l'intelligence artificielle, l'Internet des objets ou la cryptographie post-quantique.

Introduction

À regarder de près l'échiquier international, force est de constater que la puissance des États ne se mesure plus seulement à l'aune de leur force militaire et diplomatique, mais repose également et de plus en plus sur leurs capacités industrielles et technologiques. Être souverain, c'est maîtriser les données et les technologies de pointe, notamment celles du numérique, lesquelles sont garantes de l'autonomie stratégique. Vaste défi, quand on sait que des milliards de données sont échangées chaque jour et que leur volume va croissant.

Plus de numérisation et de connectivité implique également plus de vulnérabilités et des besoins accrus en matière de cybersécurité. Rappelons d'ailleurs que derrière ce mot se cache une grande variété de menaces : celles qui touchent à la confidentialité des données, mais aussi celles qui visent leur disponibilité et/ou leur intégrité, ou bien encore mettent en péril la sécurité des identités numériques. Diversité des menaces donc, mais aussi multiplicité des contextes : selon les situations, on parlera de cyberattaques, de cybercriminalité, de cyberguerre ou de cyberterrorisme. Il est donc essentiel de protéger notre « territoire national numérique » face à des comportements hostiles ou à des infrastructures numériques extraterritoriales.

Dans ce domaine, Thales fait partie des quelques entreprises françaises d'envergure mondiale capables de proposer les solutions de souveraineté numérique que sont la protection des réseaux et des données, la gestion des identités et des accès, la biométrie, le suivi des menaces, la détection et la réponse aux attaques, le conseil et les opérations de cybersécurité. En tant que groupe dual, riche de son expertise sur le marché de la Défense, la cybersécurité et la préservation de notre souveraineté font partie depuis longtemps de la culture et de la stratégie de Thales. Grâce à ses dernières acquisitions (Vormetric en 2016, sur le marché de la protection des données, et Gemalto en 2019), le Groupe a pu asseoir sa position de leader français, européen et mondial.

Il est essentiel, pour mieux répondre aux divers enjeux liés à la cybersécurité et pour faire face à la concurrence internationale, de structurer une filière française et européenne. Si elles se mobilisent, la France et l'Europe ont les moyens de s'affirmer en tant que leaders dans des domaines aussi structurants que l'intelligence artificielle, l'Internet des objets ou la cryptographie post-quantique.

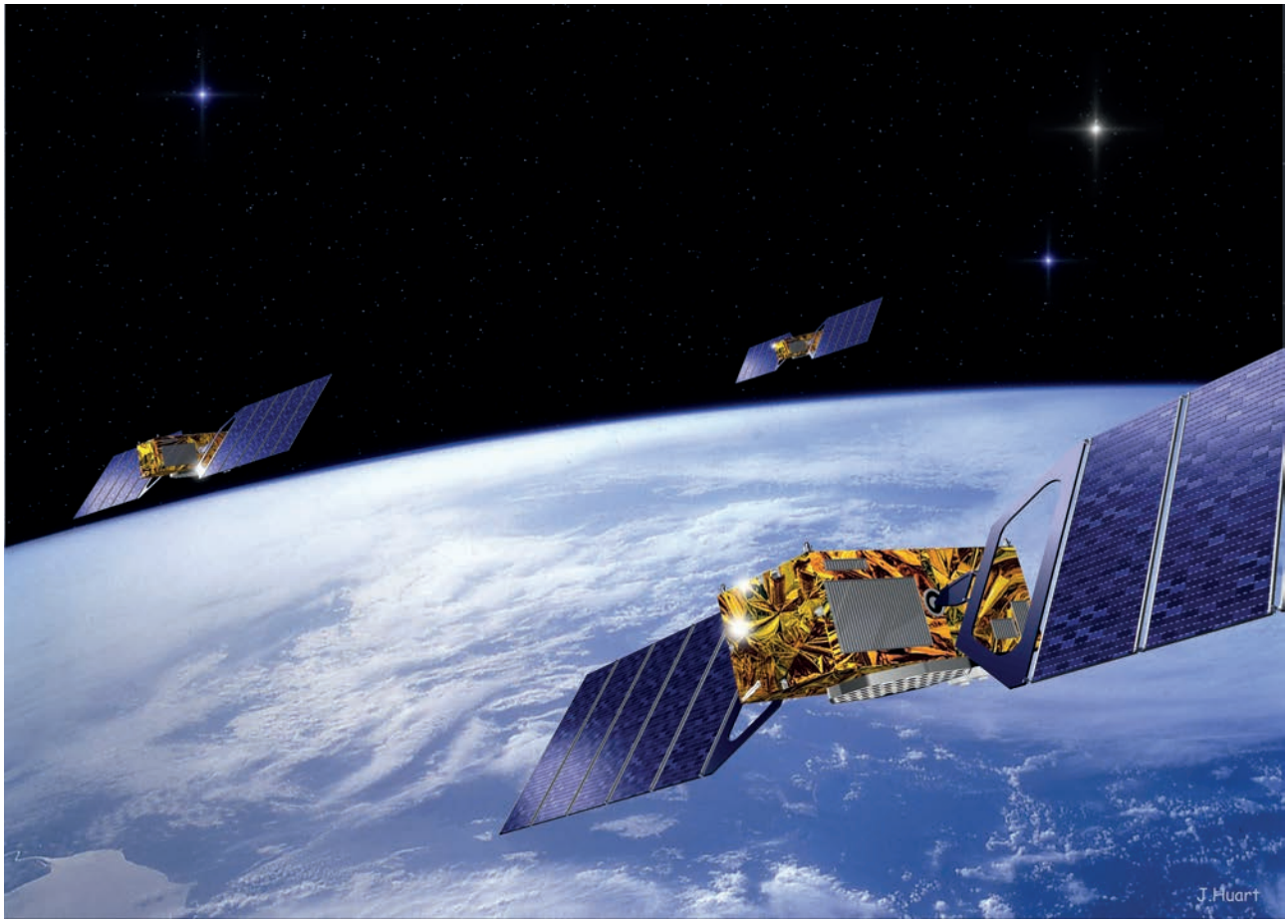

Photo © ESA

Le système Galileo est le système européen de positionnement et de navigation par satellite. Il est opérationnel depuis 2016.

Répondre aux divers enjeux de la cybersécurité

La sonnette d'alarme est fréquemment tirée face à l'étendue des risques cyber. Pour y répondre**, être une entreprise positionnée de longue date sur des projets à forts enjeux souverains**, et donc satisfaire des clients institutionnels exigeants, est un facteur différenciant :

- dans le domaine de l'espace et de l'aéronautique, les exigences sont toujours plus fortes : par exemple, pour assurer la protection du système de radionavigation européen Galileo ou la sécurité de systèmes de gestion du trafic aérien ;
- en matière de Défense, le combat collaboratif connecté en cours de développement dans le cadre du programme Scorpion [(1)] entraînera des besoins de sécurisation des données et des communications de plus en plus importants. Dès aujourd'hui, le risque de voir son infrastructure IT et ses communications militaires paralysées par un adversaire doit être pris très au sérieux.

La cybersécurité est essentielle pour garantir le bon fonctionnement des réseaux constituant le cœur de l'autonomie des États et de la sécurité des personnes. D'où la **nécessité, pour les entreprises, de développer des stratégies dépassant la sécurité de leurs seuls systèmes d'information,** et ce en misant sur la sécurisation de leurs produits et systèmes à tous les stades de leur cycle de vie :

- au préalable, ces stratégies doivent s'assurer que les couches de protection cyber n'impactent pas la performance des outils sur lesquels elles sont apposées, en termes d'expérience utilisateur ou de vitesse. C'est, par exemple, l'intérêt des solutions de chiffrement ultra rapide, à même de servir la protection des données et des transactions bancaires qui ne peuvent souffrir aucun temps de latence ;
- ensuite, la sécurité périmétrique est nécessaire mais insuffisante dans un environnement où de plus en plus de services numériques sont fournis depuis des *clouds* publics. Il faut donc protéger la donnée elle-même en gardant à l'esprit deux principes fondamentaux :
  - la confiance, car l'acceptation des technologies numériques par les utilisateurs passera à la fois par une exigence de transparence et par le fait de conserver l'humain au centre du processus de décision,
  - la facilité d'utilisation car, sans elle, pas de protection efficace. Renforcer la sécurité numérique en ajoutant des couches de sécurité les unes aux autres va à l'encontre du but recherché. Trop contraignantes, elles incitent les utilisateurs à les contourner.

(1) https://www.defense.gouv.fr/dga/equipement/terrestre/le-programme-scorpion

Photo © Nexter

La variante EPC (Engin Poste de commandement) du véhicule GRIFFON développée dans le cadre du programme Scorpion (https://www.thalesgroup.com/fr/group/journaliste/press_release/scorpion-le-griffon-poste-commandement-qualifie).

Quelles politiques conduire pour structurer la filière française et européenne de la cybersécurité et faire face à la concurrence internationale ?

Le renforcement de champions français et européens existants est une condition nécessaire pour que l'Europe puisse tenir son rang, alors que les équipements et logiciels venant des États-Unis et de Chine irriguent tous les systèmes d'information. L'enjeu est de disposer d'entreprises leaders de la cybersécurité, qui aient atteint une taille critique de classe mondiale et soient capables de développer des gammes de produits compétitives et par là même exportables.

L'État s'est d'ores et déjà organisé, après avoir ouvert la voie avec la LPM [2] 2014-2019 qui a fixé de nouvelles obligations aux opérateurs d'importance vitale (OIV) en matière de cybersécurité :

- il a favorisé la structuration d'une concertation État-industrie, qu'incarne le Comité stratégique de filière des industries de sécurité, présidé par Marc Darmon, notre directeur général adjoint ;
- saluons également sa stratégie d'accélération cyber lancée en février 2021 qui mobilise 1 milliard d'euros, dont 720 millions d'euros de financements publics. Ces fonds bénéficieront notamment à l'ANSSI [3], dans ses efforts pour aider les entreprises et administrations à faire face à la menace, et à la DGNum [4] ;
- cette stratégie accompagne également la création du Campus Cyber qui rassemblera les acteurs du secteur afin de développer des synergies entre les grands groupes (Thales, Atos, Capgemini, Orange), des PME, des *start-ups*, les services de l'État, les organismes de formation, les acteurs de la recherche et du monde associatif. Il aura pour mission de fixer le cap et les grandes échéances de la R&D dans le domaine cyber et commencera à définir les contours d'une politique européenne (détermination des grandes catégories d'utilisateurs et des contraintes spécifiques suivant les domaines d'application, investissements et complémentarité des fonds publics/privés …) ;
- à travers le lancement de ce Campus, mais aussi, par exemple, de celui de la Cyber Défense Factory au sein du ministère des Armées, l'État poursuit sa politique d'innovation ouverte qui constitue un puissant catalyseur de progrès et de synergies.

(2) LPM : loi de programmation militaire.

(3) ANSSI : Agence nationale de la sécurité des systèmes d'information.
(4) DGNum : direction générale du Numérique et des Systèmes d'information et de communication du ministère des Armées.

Au niveau européen, citons les initiatives bienvenues du Fonds européen de Défense en matière de sécurité dans le domaine militaire, lesquelles traduisent une vraie prise de conscience du caractère transnational de ces enjeux.

L'écosystème de Thales

Les industriels ne sont pas en reste et endossent le rôle de partenaires de confiance sur les différents enjeux régaliens. Thales s'implique ainsi fortement dans l'écosystème de cybersécurité :

- en tant que parrain du programme de cybersécurité de Station F (campus de *start-ups* situé dans la Halle Freyssinet, à Paris), Thales accélère le développement de *start-ups* en leur apportant conseils, expertise et accès à nos plateformes technologiques pour co-construire des solutions innovantes, tout en soutenant l'émergence de nouveaux champions du secteur ;
- à Palaiseau, nous disposons de compétences de R&D de pointe au sein de notre laboratoire ThereSIS (Thales European Research Centre for Security & Information Systems), qui fédère les efforts de recherche que nous menons en lien avec l'École polytechnique et divers pôles de compétitivité regroupant laboratoires universitaires et partenaires industriels, dont des PME ;
- à Rennes, nous avons inauguré la « Ruche ». C'est dans cette structure créée au sein du pôle d'excellence cyber, que nos ingénieurs travaillent en partenariat étroit avec des *start-ups* locales, la direction générale de l'Armement et les opérationnels pour répondre aux besoins critiques du ministère des Armées en matière de cyberdéfense ;
- à l'international, nous conduisons une centaine de partenariats technologiques avec de grands groupes tels qu'IBM, Palo Alto Networks, Cisco, etc. Nous nous rapprochons également de nouveaux acteurs pour accroître notre capacité d'innovation et notre flexibilité (PrimeKey, Senetas, Ground Labs…).

En pleine révolution des *deep tech*, faire émerger des champions français et européens nécessite également un accompagnement financier conséquent tant les besoins d'investissements sont considérables :

- nous devons pouvoir compter sur le soutien financier sectoriel ou transverse de l'État et de l'Union européenne. Entre autres dispositifs, nous citerons évidemment le CIR [5], un outil puissant qui nous donne les moyens d'exister au niveau mondial, mais aussi les études amont ou le Programme d'investissements d'avenir (PIA 4) qui finance des innovations structurelles, notamment sur les sujets IA, cyber ou quantique ;
- en parallèle, l'État doit engager une politique d'achats à la hauteur des enjeux, pour répondre aux carences encore récemment constatées au sein des collectivités territoriales et institutions de santé, trop souvent victimes d'attaques.

Pour faire face à la concurrence internationale, la France et l'Europe ont besoin de disposer d'un **capital humain** de plus haut niveau. Mais dans un contexte de pénurie de compétences, les défis en la matière sont nombreux : sensibilisation dès le plus jeune âge aux métiers de la sécurité numérique, diagnostic de l'offre de formation, plus grande féminisation des métiers considérés (les femmes représentent à peine 11 % des effectifs [6] !), stratégies d'attractivité et de rétention vis-à-vis des talents, etc.

Enfin, n'oublions pas l'importance de nous entendre sur le sujet de la **certification** porté notamment par l'ANSSI en France et l'ENISA [7] au niveau européen. La certification, qui permet d'assurer que les produits, solutions et services respectent un niveau standard de sécurité, constitue un outil indispensable pour garantir la souveraineté nationale et européenne. Mais encore faut-il s'entendre sur la définition de normes exigeantes et unanimement partagées.

Quelles perspectives en matière de cybersécurité à moyen et long terme ?

En la matière, nous pouvons citer trois perspectives structurantes, à moyen et long terme.

La protection du *cloud*

D'abord, il faut veiller à assurer **la protection du *cloud***, qui est devenu le socle incontournable de quasiment tous les champs de l'innovation numérique (IA, IoT, 5G, *quantum computing*…) et sur lequel sont hébergées de nombreuses données sensibles d'entreprises et d'administrations publiques.

Elle est nécessaire à une transformation numérique réussie. Qui peut imaginer une voiture connectée et pilotée depuis un *cloud* d'entreprise qui serait vulnérable à n'importe quelle attaque ? Pour en assurer la sécurité, il faut recourir à des processus et à des outils spécifiques qui ne soient pas sous le contrôle de l'opérateur d'un *cloud* et qui permettent de gérer la sécurité des données et des accès (chiffrements, gestion des identités, gestion des clés…). Il est essentiel pour les entreprises de désigner un tiers de confiance capable de les accompagner dans le choix et la gestion de ces outils.

Le marché s'oriente vers des solutions hybrides, alliant *clouds* privés et *clouds* publics, afin de prendre en compte le niveau de sensibilité des données. Quatre critères doivent entrer en ligne de compte : l'attrait du modèle d'affaires, celui de l'offre technique, une situation de dépendance vis-à-vis d'un fournisseur et la souveraineté des

(5) CIR : Crédit d'impôt recherche.

(6) Commission supérieure du numérique et des postes, Avis n°2021-03 du 29 avril 2021 portant recommandations dans le domaine de la sécurité numérique.

(7) ENISA : European Union Agency for Cybersecurity.

Photo © 123rf

données. Outre les attaques informatiques, la mesure du risque doit aussi prendre en compte les lois extraterritoriales, comme le Cloud Act américain, ou encore le danger de voir des données d'entreprises françaises ou européennes fuiter aux États-Unis pour être exploitées dans le cadre d'enquêtes pénales :

- les premières couches de protection des environnements *cloud* concernent les données (plateforme CipherTrust de Thales), ainsi que la gestion des identités et le contrôle des accès (comme nous le proposons avec Safenet Trusted Access) ;
- quand le niveau de sécurité et de souveraineté recherché l'exige, il est possible de passer par des tiers de confiance européens qui garantissent la sécurité de solutions *cloud* du marché (ou qui proposent directement des offres sécurisées). C'est une solution mise en avant par le gouvernement français au travers du label « *cloud* de confiance » ;
- enfin, des prérequis supplémentaires et spécifiques s'appliquent à la Défense, où le *cloud* privé est de rigueur pour les données classifiées et la projection sur les théâtres d'opérations.

Les initiatives européennes, Gaïa-X pour les *clouds* publics et Military multi-domain operations cloud (M-DOC) pour les *clouds* de Défense, visent à renforcer la cybersécurité de ce levier indispensable à la transformation numérique.

Le besoin de protection lié à l'arrivée de la 5G

Par ailleurs, l'arrivée de la 5G va élever **la protection de nos systèmes et objets connectés** au rang d'enjeu majeur de sûreté, sachant que le nombre d'objets connectés pourrait être multiplié par 48 d'ici à 2025, selon l'Institut Green IT [8].

Dans l'avionique, par exemple, les systèmes récents offrent aux compagnies aériennes et aux passagers un degré de connectivité inégalé permettant des liaisons fluides et continues entre l'avion et le sol. Cette nouvelle donne va façonner l'avenir du transport aérien en matière d'expérience des passagers, de sécurité et d'efficacité énergétique des vols.

Les nouvelles opportunités offertes par l'IoT créent aussi de nouvelles vulnérabilités pour des systèmes qui sont de plus en plus interconnectés. Pour y faire face, il est crucial que les notions de sûreté et de résilience soient intégrées au cœur même du développement de ces nouveaux services, en particulier dans des secteurs tels que la Défense, la santé ou les transports, autant de domaines où la préservation des vies humaines est un véritable enjeu.

La protection liée à l'avènement des ordinateurs quantiques

Enfin, dernier défi de taille, celui du passage à l'échelle en matière de **cryptographie post-quantique**. L'enjeu, ici, est de garantir la résistance du chiffrement de nos données dans le contexte de l'avènement des ordinateurs quantiques. Il est probable que certains États commencent déjà à stocker des données chiffrées avec l'espoir de pouvoir en casser les clés cryptographiques lorsque les technologies quantiques le permettront, probablement d'ici une dizaine d'années. États, OIV, transports ferroviaire et aérien, entreprises de toutes tailles…, aucun réseau ne serait à l'abri.

Au sein de Thales, plus d'une centaine de nos chercheurs travaillent à renforcer le chiffrement des données, notamment nos équipes de cryptologues qui œuvrent à des projets de Défense pour le gouvernement français. Nous participons également activement à des travaux de recherche qui rassemblent des industriels et des acteurs du monde académique : au niveau national, dans le cadre du PIA RISQ, qui ambitionne de regrouper les compétences françaises en cryptographie post-quantique, et, au niveau

(8) GreenIT, *Empreinte environnementale du numérique mondial*, 2019.

européen, avec le projet de recherche H2020 Prometheus. Nous rencontrons d'ailleurs un succès certain dans ce domaine : l'algorithme de signature post-quantique Falcon, dont nous sommes co-inventeurs, est ainsi l'un des deux finalistes retenus pour devenir le standard mondial en matière de signature électronique.

Conclusion

La cybersécurité est la condition du succès de notre économie numérique dans un monde de réseaux, où les données circulent en permanence et sont stockées dans le *cloud*.

Conserver notre indépendance stratégique en la matière passera par le renforcement d'une filière industrielle devant nous permettre de concevoir des solutions maîtrisées, du composant *hardware* jusqu'aux systèmes d'information stratégiques, et s'appuyant sur des équipements de protection et de décision souverains. C'est par leur capacité à former les bonnes personnes, à développer les meilleures technologies compétitives au niveau mondial et à organiser une mobilisation volontariste des sphères publique et privée, que la France et l'Europe pourront mieux se positionner sur les marchés mondiaux et souverains.

Les atouts sont là. La France et l'Europe ont pris conscience des enjeux cyber à leur échelle. À nous, responsables politiques, industriels et académiques, de trouver les voies et les moyens pour lutter à armes égales avec nos concurrents dans un contexte de compétition internationale exacerbée.