POSITION PAPER

INITIATIVE SOUVERAINETÉ

INSTITUT CHOISEUL

La cybersécurité, préalable à toute souveraineté économique

Plaidoyer pour un nouveau leadership privé et public en matière de cybersécurité

Juin 2022

L'*Initiative Souveraineté*, lancée en janvier 2022, est la plateforme de l'Institut Choiseul dédiée aux enjeux de souveraineté et de résilience. Cette Initiative a pour but d'identifier et de promouvoir des mesures pragmatiques et concrètes destinées à renforcer l'autonomie stratégique de la France et de l'Europe. Au travers de rencontres régulières réunissant acteurs économiques de premier plan et experts reconnus, et par la production de documents de synthèse et d'orientation émanant des écosystèmes réunis, l'Institut Choiseul entend ainsi prendre part au débat sur la nécessaire souveraineté nationale et européenne dans des domaines aussi variés que la défense, l'industrie, l'agroalimentaire ou encore les transports.

La première *Rencontre Souveraineté & Résilience* s'est tenue en mai 2022 autour d'acteurs de premier plan qui ont partagé leur témoignage, vision prospective et bonnes pratiques : Daniel Le Coguic, (Alliance pour la Confiance Numérique & Atos) Elena Poincet (Tehtris), Cédric Sylvestre (Olvid) et Michel Van Den Berghe (Campus Cyber).

Introduction

La cybersécurité est la clé de voûte de l'autonomie stratégique d'aujourd'hui et de la souveraineté de demain

La cybersécurité permet d'assurer l'intégrité et la sécurité de toutes les entités physiques utilisant des systèmes d'information, des données ou des logiciels, garantissant le fonctionnement des administrations, des entreprises, des infrastructures essentielles ou critiques. Une cybersécurité efficace s'impose comme la condition préalable d'une souveraineté numérique pleine et entière.

L'objectif premier est de permettre le développement d'entreprises françaises et européennes spécialisées dans la cybersécurité pour garantir l'excellence de leurs solutions et de ce fait faciliter leur promotion et leur utilisation massive et systématique par le plus grand nombre d'acteurs publics et privés. Une prise de conscience sur le besoin et l'opportunité d'acquérir et de faire confiance aux produits français ou européens, à caractéristiques et performances égales, est indispensable.

Un nouveau leadership privé et public dans la cybersécurité pour transformer la culture des entreprises et des administrations

La multiplication des cybermenaces doit conduire l'ensemble des acteurs à prendre conscience du phénomène et les inciter à s'inscrire dans une feuille de route globale.

L'industrie de la cybersécurité a besoin d'un sursaut de leadership et d'une prise de conscience des décideurs, au sein des grands acteurs de l'économie autant que dans les petites entreprises ainsi qu'au plus haut niveau de l'échelon politique français et européen.

La responsabilité du choix des outils ne peut être portée par les seules directions des systèmes d'information (DSI) ou responsable de la sécurité des systèmes d'information (RSSI). Les décisions doivent être portées et assumées au plus haut niveau, par les directions générales des entreprises et des administrations. La cybersécurité et les choix de souveraineté technologique doivent irriguer les organisations en partant du plus haut niveau de gouvernance. La transformation des cultures d'entreprises et d'administrations ne peut se faire que par un fort volontarisme des niveaux décisionnaires en premier lieu. Une « culture du cyber », comprise comme existentielle et transversale par nature, doit être insufflée dans les entreprises et administrations françaises, à l'instar de la dynamique salutaire qui a mobilisé ces quinze dernières années autour des enjeux de RSE.

L'Institut Choiseul appelle à placer la cybersécurité au cœur d'une stratégie de souveraineté renouvelée

La surface d'attaque s'élargit, la cybersécurité est devenue l'affaire de tous

La dimension globale du cyberespace engendre une multiplication des menaces et une diversification des acteurs touchés, citoyens, États, entreprises, quelles que soient leurs tailles.

L'ultra connectivité des sociétés et des économies et la numérisation exponentielle des chaînes de production entrainent une augmentation continue de la surface d'attaque. La cybersécurité devient un enjeu transversal, hautement régalien.

L'industrie de la cybersécurité devient un levier de compétitivité mondiale pour la France et une opportunité de développement des tissus territoriaux

En France, la cybersécurité constitue une industrie fortement exportatrice, avec 14,1 milliards d'euros de chiffre d'affaires réalisés à l'international et 5 milliards d'euros de chiffre d'affaires à l'exportation. Elle crée 7,1 milliards d'euros de valeur ajoutée et emploie 70 500 personnes. « *Non seulement l'industrie de sécurité est la filière industrielle qui a la croissance la plus forte avec le plus fort taux de valeur ajoutée (près de 43 %), mais la cybersécurité constitue le segment de cette filière qui tire la dynamique du secteur* », précise un Rapport du Sénat du 10 juin 2021.

La cybersécurité offre l'opportunité de placer les acteurs français et européens de la confiance numérique parmi les leaders mondiaux du domaine

Les acteurs français de la cybersécurité et de la confiance numérique au sens large sont mondialement reconnus pour la fiabilité de leurs solutions et leur force d'innovation. Une base solide existe donc pour installer comme leaders des acteurs qui disposent d'une taille critique pour rivaliser sur la scène internationale, à l'instar d'Orange Cyberdéfense, Thales, SopraSteria, Airbus CyberSecurity, Tehtris ou YesWeHack. Cette base solide constitue la partie immergée d'un écosystème privé vivace et innovant constitué de nombreuses PME, starts-ups et scale-ups.

Par ailleurs, de grands acteurs industriels attachés à la souveraineté de leur production et la sécurisation de leur chaine de valeur, développent des réponses cyber propres à leurs activités dès le design et en amont du développement.

La France peut compter sur des acteurs publics forts et voit ses écosystèmes se fédérer avec des initiatives reconnues :

- l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) est devenue une référence qui a pris toute sa place pour sensibiliser, alerter, former et lutter contre les cyberattaques ;
- le comité stratégique de filière « industries de sécurité » qui met en avant le projet fédérateur « cybersécurité » rassemblant l'Etat (DGE) et les acteurs industriels de la sécurité sous l'égide du conseil national de l'industrie ;
- le Campus Cyber constitue un modèle pour faire collaborer tous les acteurs de la filière, au bénéfice de l'attractivité pour toute une profession.

Les acheteurs, comptes publics ou privés, sont eux-mêmes en demande de solutions technologiques dites « souveraines », développées en France et certifiées par l'ANSSI, à l'image de la solution de détection MACTAN développée par Sopra Steria ou la solution Olvid, messagerie instantanée utilisée par des entreprises et de nombreux ministères dont celui de l'Intérieur. ■

La cybersécurité en chiffres

4e *La France est le 4ème pays le plus touché au monde par attaques au nombre d'habitants*

Les attaques ciblant les entreprises de toutes tailles ont été multipliées par 4 entre 2020 et 2021 en France **x4**

15 000 *postes dans la cybersécurité sont en attente d'être pourvus en France*

5 700 Mds €
Les besoins en cybersécurité sont estimés à 5700 milliards d'euros dans le monde

70 500 salariés
travaillent dans le secteur de la cybersécurité en France

Failles - Limites - Menaces

Les enjeux d'autonomie propre à la cyber ne sont pas encore unanimement partagés et le recours aux solutions étrangères reste trop important

Au quotidien, les acteurs publics et privés en Europe ont souvent recours à des outils numériques d'origine étrangère. Ces technologies sont régies par le droit du pays de développement de ces solutions, ce qui met à mal le principe de souveraineté.

Les grands acheteurs publics et privés ne font pas suffisamment le choix de solutions cyber françaises ou européennes dans leur politique d'achat, alors même que 30 % des RSSI des entreprises du CAC 40 sont d'ores et déjà convaincus des risques posés par les fournisseurs étrangers de solutions.

Des contradictions fortes demeurent entre les objectifs politiques affichés et les actions déployées

De nombreux projets illustrent le fossé qui existe entre les objectifs affichés par les autorités publiques et leur concrétisation.

Les choix réalisés en matière de commande publique témoignent également de fortes contradictions. C'est par exemple le cas du récent choix fait par la Commission européenne de sélectionner une entreprise britannique, British Telecom, pour gérer les communications confidentielles entre États membres et ce, pour un montant de 1,2 milliard d'euros.

L'attractivité des métiers et les cursus de formation ne sont pas encore à la hauteur des enjeux

La filière cyber repose sur un *pool* de talents, véritable atout pour la France (analystes, consultants, et surtout développeurs, ingénieurs et techniciens).

Toutefois :

- les travaux prospectifs s'accordent sur une pénurie de talents à venir. En France, près de 15 000 postes ouverts dans ce domaine ne sont pas aujourd'hui pourvus ;
- la jeune génération n'est pas suffisamment sensibilisée aux métiers de la cybersécurité et les carences au niveau de l'enseignement des mathématiques et plus généralement des sciences informatiques se ressentent fortement. ■

Propositions - Orientations - Actions

Faire de la commande publique et privée un levier de renforcement de l'offre cyber européenne et d'indépendance technologique 1

Diriger la commande publique vers les acteurs européens : une préférence aux solutions « *Made in Europe* » en s'appuyant sur un *Buy European Act*.

Inciter les grands acheteurs privés à orienter une partie de leurs commandes IT à destination d'entreprises françaises et européennes proposant des solutions de cybersécurité de confiance.

Renforcer le capacitaire en s'appuyant sur la révision du cadre réglementaire européen 2

Associer aux infrastructures critiques et économiquement essentielles une technologie européenne de confiance : introduire l'origine des produits et des services comme critère de confiance des solutions proposées, de manière systématique dans tous les textes en discussion (par ex., révision de la Directive NIS (*Network and Information Security*), *Cyber Resilience Act*).

Faire converger les initiatives par un réseau unifié et cohérent de normes : s'assurer que la révision du Règlement eIDAS qui vise à accroitre la confiance dans les transactions électroniques au sein du marché intérieur, soit réalisée en cohérence avec la révision de la directive NIS.

Démocratiser les compétences utiles et repenser le parcours des talents de la cybersécurité de demain 3

Initier dès le plus jeune âge les enfants aux bases du développement. La découverte du code à l'école, et par la même occasion des enjeux de cybersécurité, est devenue une nécessité.

Mieux organiser les formations publiques dans le développement en les rendant plus accessibles. Des certifications ou diplômes en mathématiques appliquées ne doivent plus être un critère pour bénéficier de ces formations et l'offre des formations continues doit être augmentée ouvrant ainsi notamment la voie à plus de reconversions professionnelles en cybersécurité.

Clarifier les offres privées d'enseignement supérieur et mettre en place un label national et européen.

Développer une vision industrielle et compétitive de la cybersécurité soutenue par des dispositifs de financement des acteurs à la hauteur des enjeux 4

Adopter et faire partager une vision de la souveraineté numérique conquérante pour saisir les opportunités du marché de la cybersécurité, et ne pas céder à une vision de la souveraineté trop protectrice qui conduirait au repli et à la perte de compétitivité.

Favoriser la croissance des entreprises industrielles engagées sur les sujets cyber, non seulement sur le périmètre de l'IT pour les pourvoyeurs de solutions mais aussi sur le périmètre de l'OT pour les entreprises métiers qui s'engagent sur du *cyber by design* de leurs process industriels avec des solutions en propre, européennes ou nationales.

Monter en gamme dans le recours aux fonds privés pour adresser tout l'écosystème numérique européen, avec :

- favoriser l'émergence de nouveaux fonds d'investissements avec un périmètre européen et capables de déployer leur capital en levée de fonds du niveau Growth (à partir de Series B, +10 M€) ;
- la mise en place de davantage de fonds de Corporate Venture Capital dédiés ou mutualisés sur l'ensemble du périmètre de la souveraineté (défense, spatial, renseignement…).

Permettre à des acteurs privés de bénéficier de financements non européens pour scaler et dépasser une taille critique sur les marchés. Sous réserve du maintien de contrôle, et d'une série de critères sur les technologies utilisées, leurs pays d'origine, les pays d'implantation des employés et des centres de décision, il est important de faire preuve de pragmatisme pour contrebalancer le manque de financements européens et d'accueillir des investissements étrangers qui ne remettent pas en cause l'indépendance décisionnelle et opérationnelle des acteurs souverains pour leur permettre de conquérir de nouveaux marchés à l'international.

Doubler le total des financements prévus (de 1 à 2 milliards d'euros) dans le cadre de France 2030 au profit de la stratégie d'accélération cybersécurité en innovant grâce à du financement public privé.

Consolider une offre cyber *made in Europe* de haut niveau, véritable alternative à des solutions étrangères et avantage compétitif de long terme 5

Établir un socle commun des principes et critères des solutions de cybersécurité « souveraines » qui se distingue au niveau mondial : respect du cadre des libertés publiques, traçabilité des flux financiers et respect de la réglementation en matière de lutte contre le terrorisme et de blanchiment d'argent, respect des données et du RGPD, recours à des solutions européennes, part majoritaire des développeurs et équipes techniques européens…

Bâtir un catalogue des solutions souveraines de cybersécurité reconnu et largement partagé, accessible à l'ensemble des potentiels utilisateurs. Nombreuses sont les initiatives visant le référencement des solutions françaises de cybersécurité ou les catalogues capacitaires qui constituent une première base. À l'instar des travaux de référencement des « produits et services qualifiés » réalisés par l'ANSSI et le lancement du label « *Cybersecurity Made in Europe* », il serait bon de mutualiser les sources de référencement dans un catalogue de référence, le promouvoir et permettre son accessibilité au plus grand nombre notamment pour les structures de petites et moyennes tailles. Le référencement pourrait utilement se compléter d'éléments sur les cas d'usage résolus par les solutions référencées, établissant un lien concret entre l'avis technique et usages opérationnels dans les entreprises et administrations. Ce nouveau catalogue pourrait être réalisé en mettant à contribution des acteurs légitimes qui regroupent des solutions engagées pour la souveraineté, tels que le Comité Richelieu, l'Alliance pour la confiance numérique ou l'Institut Choiseul, sous le pilotage de l'ANSSI. L'intérêt d'un tel catalogue a d'ailleurs clairement été identifié par la commission Numérique cyberespace du GICAT prochainement créée, qui a identifié ce référencement comme un de ses axes de travail.

Adopter de nouveaux standards et pratiques pour plus d'efficacité et de confiance 6

Mettre en place de la *Security by design* dans le développement des produits et solutions informatiques.

Développer la sécurité crowdsourcée qui assure un niveau de sécurité élevé en encourageant les collaborateurs d'une entreprise à rapporter les incidents et les vulnérabilités qu'ils peuvent découvrir. Les politiques de *vulnerability disclosure* qui permettent la divulgation des vulnérabilités en partageant la gravité et l'ampleur des failles, tout en protégeant juridiquement les chercheurs, sont ainsi centrales pour favoriser la confiance dans les systèmes d'information et dans les technologies futures.

Mettre en place des programmes obligatoires de recherche de vulnérabilités à l'instar de ceux développés aux États-Unis (*Hack DHS* ou *Operational Directive 20-01*). ■

À propos

L'Institut Choiseul

L'Institut Choiseul est un *think and do tank* indépendant, non partisan et à but non lucratif. Il se dédie au décryptage des grands enjeux économiques et à la fédération de la jeune génération économique.

Pour alimenter le débat public et incarner les dynamiques économiques en cours, l'Institut Choiseul produit des Notes Stratégiques, des études ponctuelles et des classements de jeunes leaders. Pour fédérer et animer ses communautés, il déploie des évènements de haut-niveau mêlant networking convivial, témoignage d'experts et de praticiens et échanges sur des sujets de prospective, sur différents territoires et verticales économiques, en France, en Europe et en Afrique.

Au croisement de la communauté d'affaires et du cercle de réflexion, l'Institut Choiseul offre une plateforme aux décideurs économiques privés comme publics pour s'identifier mutuellement, se mettre en réseau, promouvoir leurs initiatives et réfléchir aux grandes tendances économiques de demain.

Les partenaires de l'Initiative Souveraineté

L'Institut est accompagné par un noyau dur de partenaires fondateurs, tous acteurs français ou européens, qui prennent une part active à la discussion et à la formalisation de recommandations :

INSTITUT CHOISEUL

Institut Choiseul

12, rue Auber 75009 Paris
+33 (0)1 53 34 09 93

www.choiseul.info