MANIFESTE

5 VŒUX
Pour une autonomie stratégique Européenne

CDSE

HEXATRUST

CLOUD CONFIDENCE & CYBERSECURITY

En association avec le club des juristes

INTENTION DES RÉDACTEURS

Ce document a été rédigé à l'intention des responsables politiques et donneurs d'ordres. Il a pour vocation d'offrir une impulsion au sujet de l'autonomie stratégique en rassemblant des voix issues, non seulement du cercle des professionnels de la cybersécurité, mais ultimement de tous milieux confondus. En effet, il incombe aux décideurs de réaliser le caractère éminemment urgent du sujet, en cela qu'il concerne d'ores et déjà une majeure partie de la société française (nous l'avons constaté lors de la crise sanitaire).

INTRODUCTION

Grâce au numérique et à son allié consubstantiel qu'est la cybersécurité, l'essentiel de nos entreprises a pu continuer à travailler lors de la crise sanitaire, le Covid19 imposant le télétravail comme norme de fait. Le numérique, pour survivre à cette crise, est apparu comme une denrée de première nécessité, que ce soit pour vaincre l'isolement ou pour éviter l'effondrement de notre économie.

La cybersécurité est au numérique ce que les masques, les tests, les appareils respiratoires ou les vaccins sont à nos équipements de santé. Elle est une partie intégrante de la résilience de notre société. Il est aussi de notre devoir d'anticiper une future « *pandémie numérique* ». En réponse à l'appel du gouvernement en début de crise, de nombreux acteurs de notre filière ont fourni des solutions et des conseils gracieux afin d'apporter la solidarité indispensable au maintien en conditions opérationnelles de l'informatique des organisations, et tout particulièrement aux organisations essentielles à la nation parmi les secteurs de l'alimentation, la santé, l'énergie, le transport, les télécoms et les services régaliens.

Nous constatons en France que tous les secteurs d'activités ne sont pas également équipés en matière de numérique et sont souvent insuffisamment préparés au risque inhérent. Le basculement vers un « tout numérique » met à l'épreuve notre société de manière disruptive.

Qu'adviendrait-il en cas de crise majeure et quelle garantie aurions-nous sur la disponibilité sans limite des outils que nous utilisons ?

Quelle serait notre marge de manœuvre en cas d'éventuels plans de restriction en matière de ressources numériques de nos exportateurs ?

Disposons-nous des produits et services de sécurité qui assurent notre indépendance numérique ?

Indéniablement non.

Nous sommes ultra-dépendants aux outils et plateformes étrangères, sans réelle prise en compte des implications que cela peut avoir en matière de restriction de disponibilité, sans parler du respect de la protection des données ou de maîtrise de notre autonomie stratégique.

Ce constat est un avertissement pour notre secteur et doit constituer une réflexion en profondeur de nos approvisionnements. Nous avons observé, par exemple, que les solutions de télétravail mises en œuvre sont essentiellement étrangères et ont entrainé une fuite massive d'informations confidentielles hors d'Europe. Les certifications de produits par l'ANSSI ont très peu d'impact sur les politiques d'achat en dehors des organisations très sensibles. L'industrie de cybersécurité, véhicule d'emplois, de croissance et d'inclusion sociale, doit être une industrie prioritaire au niveau national.

Nous, entreprises membres d'Hexatrust et du CDSE en association avec le Club des Juristes aspirons à renverser radicalement la tendance actuelle et émettons 5 souhaits vis-à-vis des responsables politiques et de l'Etat pour mener une politique prioritaire de l'industrie du numérique[1]. Ces vœux viennent en renfort des engagements pris lors de la signature, en Janvier 2020, du Contrat Stratégique de Filière (CSF) Industrie de Sécurité[2] avec les Secrétaires d'Etat Agnès Pannier-Runacher, Cédric O et le ministre Christophe Castaner, et ont pour objectif de :

- Rétablir un équilibre en matière d'autonomie numérique, en bâtissant une alternative européenne à la concurrence mondiale.

  Il ne s'agira pas ici de tomber dans un protectionnisme qui pourrait ralentir la créativité de l'offre, mais bien, de réduire notre dépendance aux outils et infrastructures étrangères sur lesquelles nous n'avons aucun contrôle afin de protéger les intérêts des organisations européennes quotidiennement et lors de la survenance d'une crise.

- Favoriser les investissements dans une transformation numérique résiliente et de confiance, conforme aux règles de protection des données personnelles, et dont la pérennité et la disponibilité ne dépendent que de nous.

  Le défi pour la France sera de financer l'adoption massive et l'industrialisation de nos innovations, au lieu de concentrer les politiques d'investissements uniquement sur la recherche et le développement, les brevets et les startups. Nous devons faire émerger de grands compétiteurs comparables aux GAFAM et aux champions de la cyber à l'échelle de l'Europe. Pour reprendre les mots de Claude Revel, ancienne déléguée à l'Intelligence Economique, il s'agira de *« Faire grandir ce qui est né en France »*.

1_ L'industrie de cybersécurité figure parmi les dix domaines stratégiques du pacte productif du Président Emmanuel Macron.

2_Signature du Contrat de Filière le 29 Janvier 2020 au FIC : https://www.conseil-national-industrie.gouv.fr/files_cni/files/csf/Securite/contrat_csf_industries_de_securite_janvier_2020.pdf

VOEU 1 :
Plan d'équipement cyber

Aujourd'hui, nous devons consacrer l'effort d'investissement dans la relance de l'économie aux enjeux de transformation numérique immédiats, avec la résilience et la continuité d'activité en toutes circonstances, à travers les mesures suivantes :

• Financer un *« plan d'équipement cyber et continuité d'activité numérique »* à l'image du plan d'équipement pour les Centres Hospitaliers Universitaires du CSF, cette fois à l'échelle de la nation.

  o Déterminer des plateformes et équipements capacitaires pour l'ensemble des organisations de certains secteurs essentiels à la nation (parmi lesquels l'alimentation, la santé, l'énergie, le transport, les télécoms et les administrations nationales, administrations territoriales, établissements publics…). Ces plateformes et équipements doivent être impérativement sélectionnés parmi les solutions de confiance certifiées et européennes - excepté lorsqu'elles n'existent pas au catalogue d'offres certifiées.

• Intégrer aux critères de notation extra-financière des entreprises l'investissement en solutions numériques sécurisées et souveraines au titre des investissements socialement responsables dans le cadre de la RSE.

VOEU 2 :

Instaurer une proportion d'achats fléchés vers les PME françaises de confiance

Cette transformation numérique pérenne ne peut être garantie que si les investissements des organisations publiques et privées - en particulier l'Etat, les collectivités locales, les établissements de santé ou nos PME – sont dirigés vers des solutions de transformation numérique certifiées et en accord avec les règlementations Européennes. Elle permettrait de relocaliser la production de solutions de cyber en Europe pour assurer notre souveraineté. Pourquoi soutenir des entreprises par des aides directes ou indirectes alors que les achats publics continuent à être effectués auprès de leurs concurrents ?
Nous préconisons donc de :

• Mettre en place un *« Small Business Act For Cyber »* pour renforcer la part des PME-ETI françaises à la commande publique et privée.

  o Pour la commande publique : Ajouter une clause réservant 30% de la part cyber et numérique des marchés publics européens aux PME-ETI européennes.

  o Pour la commande privée : Inciter les entreprises à intégrer des critères de relocalisation des activités stratégiques en support local ainsi qu'un score d'indépendance aux lois extraterritoriales à l'intérieur de leur cahier des charges.

  o Encourager les intégrateurs et les prescripteurs à mettre en avant les innovations européennes dans leurs offres.

• Adapter le code des marchés publics au secteur stratégique de la cybersécurité en ajoutant un critère d'un poids de 25% dans la note finale atteinte portant sur :

  o La localisation des lieux de centres de compétences, de production des produits et services proposés (Recherche & Développement).

  o Les dispositifs d'hébergement des données garantissant que l'hébergeur est une structure de droit européen.

  o Le territoire sur lequel est réalisé l'hébergement.

• À partir des expressions des besoins des administrations, OIV et OSE, mettre en place un dispositif d'achat groupé - synonyme d'économies au niveau national - permettant de répondre aux besoins existants et à venir de ces organisations avec l'aide des centrales d'achats existantes et sous conseil de l'ANSSI.

• Renforcer la Loi de Programmation Militaire en exigeant l'équipement des OIV/OSE en solutions qualifiées et certifiées par l'ANSSI ; sous réserve d'une réduction des délais de certifications et qualifications ainsi qu'une priorisation des offreurs de solutions européennes. En l'absence de solutions certifiées par l'ANSSI, prioriser l'adoption de solutions labellisées France Cybersécurité.

• Créer une médiation Public/Privé en cas de constat du non-respect de cette nouvelle Loi de Programmation Militaire.

VOEU 3 :

Constituer une Europe de la Cybersécurité

La Revue stratégique de cyberdéfense[3] mentionnait déjà en 2018 la nécessité de l'émergence d'un marché européen soutenant le développement de solutions européennes performantes dans le domaine du numérique, non pas en opposition à une logique de marché ouvert, mais bien pour garantir l'autonomie stratégique de l'Europe et ses Etats membres. Une Europe de la cybersécurité qui s'affranchit de la dépendance à un certain nombre de pays étrangers, nécessite la mise en place de dispositifs européens pour créer son marché, et des normes et standards communs, pouvant s'appuyer sur les mesures suivantes :

- Développer une reconnaissance mutuelle des certifications entre pays européens pour créer un marché européen dans le cadre du Cyber Act et d'un travail mutuel entre ANSSI et ENISA.
- Mettre en place un label chapeau Européen, permettant de flécher les 30% de la part cyber et numérique des marchés publics européens, sur le modèle du Label France Cybersecurity.
- Participer aux groupes de travail dans le cadre de l'ENISA pour faire émerger des standards de la cyber Européenne (ainsi que des évaluations des besoins et offres du marché européen).
- Constituer des acteurs cyber multinationaux européens en encourageant des initiatives européennes telles que le projet Gaia-X (projet franco-allemand d'infrastructures de données européennes) ou des rapprochements entre sociétés européennes.

VOEU 4 :

Un financement conséquent des ETI de croissance

Le développement d'une industrie de cybersécurité et de cloud puissante nécessite l'accès des PME et ETI de croissance au financement. Cet accès est souvent l'occasion pour des intérêts non souhaités de s'inviter dans les fleurons de notre industrie. Pour éviter que des entreprises stratégiques ou à fort potentiel de croissance se retrouvent ainsi sous l'influence de capitaux étrangers, voire rachetées, il est nécessaire que l'Etat joue un rôle actif en tant qu'investisseur, en particulier lors de la phase de « Capital Développement » où les tickets sont souvent importants. Il s'agirait alors de :

- Favoriser la création de fonds d'investissement « late-stage » dédiés aux PME/ETI de croissance franco-européennes de la cyber et du cloud pour leur permettre d'effectuer des levées de fond importantes (supérieures à 50 millions d'euros).
- Faire émerger 3 à 5 sociétés à fort potentiel comme champions industriels de la cybersécurité et du cloud Franco-Européen.
- Créer un Label Entreprises Innovantes de Croissance afin de favoriser les entreprises d'hypercroissance basées sur l'innovation dans le cadre du Crédit d'Impôt Recherche (CIR).

3_« Revue stratégique de cyberdéfense », 12 février 2018, URL : http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf

VOEU 5 :
Une Assurance-Cyber

Depuis 10 ans, l'Union Européenne, sous l'impulsion de la France, a créé les conditions de l'émergence d'une approche du numérique fondée sur la résilience des infrastructures numériques critiques[4] et sur la protection des données personnelles[5].
Toutefois, la mise en application de ces obligations et de normes d'hygiène informatique est génératrice d'une forme de distorsion en pratique entre deux familles d'acteurs. D'une part, les grands acteurs publics et privés disposant des ressources humaines et financières propres à assurer une transformation digitale pérenne et légalement conforme et d'autre part la majorité des entités professionnelles ne disposant pas de tels moyens[6].
Il s'agirait donc de :

- Créer une « Couverture Assurantielle du Cyber-Risque », mise en œuvre par des opérateurs de services dédiés, des compagnies d'assurance, ou par l'Etat, ciblant particulièrement des auto-entrepreneurs /artisans /professions libérales/ TPE/ startups/ PME, voire ETIs, et enfin des collectivités territoriales ou structures administratives de taille modeste. Il s'agit d'instaurer une obligation d'assurance professionnelle pour protéger non seulement les professionnels des cyber risques, mais aussi les utilisateurs victimes de vol ou de perte de leurs données personnelles. Elle impliquerait une mesure du risque, l'implémentation de moyens de prévention, de remédiation en cas d'incident, voire de réparation en cas d'incident grave causant des dommages et permettrait :
    - o De susciter une prise de conscience collective du risque cyber, essentielle à l'implémentation d'un plan de continuité global d'activité pour les entreprises.
    - o D'étendre la garantie responsabilité civile professionnelle et la garantie perte d'exploitation aux aspects cyber face à la multiplication des risquesde droit européen.

4_Adoption de la Directive NIS le 6 Juillet 2016

5_Activation du Règlement Général sur la Protection des Données (RGPD) le 25 mai 2018 qui confère aux citoyens européens le choix de partager ou non leurs données.

6_En 2019, 60% des entreprises n'allouent pas de budget spécifique pour lutter contre le risque de cybercriminalité selon le baromètre 2019 Euler Hermes - DFCG

Qui sommes-nous ?

HEXATRUST

HEXATRUST, est le groupement d'entreprises innovantes, des leaders du cloud computing et de la cybersécurité. Les solutions labellisées Hexatrust répondent toutes à des exigences techniques de maturité, sont reconnues en Europe et à l'international par les plus grandes organisations et s'inscrivent dans des logiques de certification et de souveraineté. La soixantaine de sociétés membres d'Hexatrust œuvrent ensemble pour promouvoir et construire la confiance dans le Cloud et l'excellence Cyber.

https://www.hexatrust.com

Le Club des directeurs de sécurité des entreprises (CDSE) :

Le CDSE fédère depuis 25 ans les expériences des professionnels de la sécurité et de la sûreté au sein des entreprises. Il rassemble les principales entreprises françaises privées et publiques (CAC 40 et SBF 120) qui opèrent dans 48 secteurs d'activités et à l'international dans plus de 180 pays. Ces dernières sont représentées au sein du Club par leur directeur de la sécurité ou de la sûreté. Ils sont ainsi les premiers donneurs d'ordre en matière de sécurité privée, les premiers clients des industries de sécurité et les interlocuteurs naturels des pouvoirs publics pout toutes les questions relatives à la sécurité des entreprises.

www.cdse.fr

Le Club des Juristes :

Le Club des juristes est le premier think tank juridique français. Lieu indépendant de débats et de propositions, créé en 2007, il réunit des professionnels d'horizons divers : magistrats, avocats, représentants d'entreprises, universitaires. Ils formulent, sur des sujets d'actualité ou de prospective, des recommandations innovantes, utiles aux décideurs publics. Par ses publications et les événements qu'il organise, le Club des juristes renforce la place du droit dans le débat public et améliore la compréhension des questions juridiques par tous.

www.leclubdesjuristes.com

INFOS & CONTACT

SOUS LA DIRECTION DE :

DE GALZAIN Jean-Noël,
Président, HEXATRUST

VOLANT Stéphane,
Président, CDSE

RÉDACTEURS :

ALAY-EDDINE Maxime,
Président, CYBERWATCH

BINDLER Marc-Antoine,
Secrétaire Général, CDSE

BLANC Stéphane
Président, ANTEMETA

CUER Valentin,
Assistant chef de projet, HEXATRUST

DEREPAS Fabrice,
CEO, TrustInSoft

DE REMUR Edouard,
Directeur, OODRIVE

DESCORMIERS-THOLLOT Loreline,
Chef de projet, HEXATRUST

GARNIER Alain,
CEO, JAMESPOT

GENDRE Adrien,
Chief Solution Architect, VADE SECURE

GENDREAU Philippe,
Délégué, HEXATRUST

GIROND Anne,
Directrice Générale, CDSE

LOTIGIER Georges,
CEO, VADE SECURE

MOREL Olivier,
Directeur Général Adjoint,
ILEX INTERNATIONAL

PAGEZY Christophe,
Co-Président, PROVE & RUN

PIOTROWSKI Jean-Nicolas,
Président, ITRUST

RENOUIL Luc,
Directeur stratégie et développement Défense et Sécurité, BERTIN

SOUILLÉ Alexandre,
Président, OLFEO

WALLER Romain,
Directeur Général Cybersécurité, ERCOM

CONCEPTION/ RÉALISATION :

CDSE & HEXATRUST

Club des Directeurs CDSE de Sécurité des Entreprises

H E X A T R U S T
CLOUD CONFIDENCE & CYBERSECURITY

En association avec le club des juristes

HEXATRUST

WWW.HEXATRUST.COM