CYBERSÉCURITÉ
VIGILE DE NOTRE AUTONOMIE STRATÉGIQUE

Arnaud MARTIN, Didier GRAS

THINK-TANK DIGITAL NEW DEAL

juin 2022

COLLECTION DIGITAL NEW DEAL "NUMÉRIQUE DE CONFIANCE"

“

LE RISQUE CYBER EST CONSIDÉRÉ COMME LE 3E RISQUE SYSTÉMIQUE (AVEC PANDÉMIQUE ET CLIMATIQUE) PAR LES SOCIÉTÉS D'ASSURANCE. ”

SOMMAIRE

PRÉFACE

Deux grands bouleversements récents ont mis au premier plan la question de la cybersécurité. Tout d'abord la crise du Covid, la digitalisation croissante des usages et l'interconnexion exponentielle des systèmes a mécaniquement soulevé la question de leur protection, chaque nouvel usage offrant une nouvelle opportunité d'attaque. L'Ukraine ensuite bien évidemment, la médiatisation des nouvelles « guerres hybrides » a permis au grand public de prendre conscience que les menaces du monde virtuel avaient des impacts bien réels dans nos vies.

Dans un tel contexte où les risques de cybersécurité deviennent de plus en plus rémanents et sophistiqués, l'Etat doit donc faire œuvre de pédagogie pour s'assurer que nos entreprises, collectivités territoriales, et concitoyens prennent bien la mesure des enjeux et soient armés pour faire face à des menaces toujours plus régulières et toujours plus graves.

L'Union Européenne doit quant à elle se munir d'une boussole *stratégique*[1] numérique, en faisant de la cybersécurité le quatrième pilier de son autonomie stratégique. Elle ne doit pas hésiter pour cela à remettre en question le cadre politique et juridique actuel. L'Europe doit en effet viser une totale autonomie dans sa capacité d'appréciation et de gestion du risque cyber.

C'est ce chemin, partant de la prise de conscience pour aller jusqu'à à la prise de confiance collective, que les auteurs Arnaud Martin et Didier Gras nous invitent à emprunter. Balisant tout au long de leur parcours des propositions concrètes permettant de nourrir cette ambition et d'enrichir ainsi notre collection « Numérique de confiance[2] » composée de quatre notes complémentaires. La cybersécurité étant selon notre think-tank le sous-jacent du triptyque « Cloud, Data, IA » qui constitue l'écosystème de confiance. Car point de confiance sans sécurité pour dissiper les peurs, et sans souveraineté pour s'assurer d'être maître de son destin.

" L'AUTONOMIE STRATÉGIQUE EST UNE CAPACITÉ À GÉNÉRER ET DÉFENDRE UN ÉCOSYSTÈME DE CONFIANCE QUI ORGANISE NOS INTERDÉPENDANCES TECHNOLOGIQUES "

Arno Pons,
Digital New Deal

[1] *Europe de la défense : la Boussole stratégique adoptée, Ministère des Armées, https://www.defense.gouv.fr/actualites/europe-defense-boussole-strategique-adoptee#:~:text=Cette%20Boussole%20strat%C3%A9gique%20repr%C3%A9sente%20pour,%C2%BB)%2C%20la%20r%C3%A9silience%20(%C2%AB*

[2] *Digital New Deal publie une collection de quatre notes sur la définition du "numérique de confiance" comme socle de notre autonomie stratégique : "Cloud de confiance" par Laurence Houdeville et Arno Pons en 2021, puis en 2022 "Cybersécurité, vigile de notre autonomie stratégique" par Arnaud Martin et Didier Gras, "Data de confiance" par Olivier Dion et Arno Pons, et "IA de confiance" par Julien Chiaroni et Arno Pons.*

INTRODUCTION

La menace cyber, est *« une potentielle utilisation malveillante de l'espace numérique. Elle prend forme lorsqu'une entité malveillante attaquante effectue un enchainement d'actions via des voies numériques ou physiques pour exploiter les propriétés du cyber espace (notamment ses vulnérabilités techniques ou structurelles) afin de réaliser des impacts, eux-mêmes d'ordres numériques ou physiques (en particulier financiers).»*[3]

Cette menace mondialisée fait désormais partie de l'actualité quotidienne. Récemment, l'invasion physique de l'Ukraine par la Russie, associée à un conflit cyber largement médiatisé (i.e. attaque du satellite ViaSat, création de l'IT Army of Ukrain, actions de sabotage d'infrastructures critiques ukrainiennes,…), ou bien au Costa Rica, où le président Rodrigo Chavez a déclaré le 10 mai 2022 l'état d'urgence pour lutter contre les cyberattaques attribuées au groupe Conti (de nombreuses agences gouvernementales ont été rançonnées par des pirates informatiques, espérant obtenir du gouvernement le paiement de plusieurs millions de dollars de rançons).

En France, sa prise en compte a été graduelle : initialement centrée sur le renseignement d'Etat elle fut, dès 2009, étendue à la défense des ministères et grandes administrations par la création de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) ; les lois de programmation militaire de 2013 et 2018 ont ensuite accrue les obligations des acteurs d'importance vitale (OIV) et des opérateurs de services essentiels (OSE) en matière de protection des actifs et de résilience d'activité, de détection et de réaction aux attaques ainsi que de gouvernance du risque cyber.

Parallèlement et au fil de la digitalisation du monde dans lequel nous évoluons la cybercriminalité et la manipulation de l'information ce sont fortement développées, en prenant de multiples formes. A commencer par les rançongiciels permettant de crypter les données ; sur le vol ou de recel d'images privées (sextorsion) ; ou celui des coordonnées bancaires au moyen de sites publiques falsifiés. Ainsi, de nombreuses collectivités territoriales et Centres Hospitaliers Universitaires (CHU) ont été privés de leurs données en pleine période de COVID-19 ; des milliers d'employés se sont fait dérober leurs crédits de formation (CPF) après avoir communiqué leurs mots de passe à des sites contrefaits. La seconde forme, véritable levier d'influence sur les populations, s'est développée grâce notamment aux technologies d'imagerie de synthèse par la diffusion sur les réseaux sociaux, de fausses informations et vidéos retouchées très réalistes (deepfake).

La prise de conscience est désormais réelle dans les grandes administrations ou les grandes entreprises, et les mesures techniques et organisationnelles se mettent petit à petit en place. Toutefois à l'autre bout de la chaîne, les citoyens comme les petites et moyennes entreprises sont trop souvent désarmés face à la menace cyber.

Si des mesures de prévention plus efficaces ne sont pas mises en oeuvre de manière pérenne, la menace cyber pourrait faire peser un risque sociétal sur la poursuite du développement du numérique dans nos sociétés.

Nous proposons pour cela un état des lieux de **la cybersécurité en France en huit constats et recommandations,** qui visent à en faire un **sujet de société** et un enjeu **de normalisatio**n. La première partie recense les actions préconisées pour assurer une prévention efficace pour la population (recommandations 1 à 4). La seconde détaille les évolutions souhaitables du cadre législatif afin de nous donner les moyens politiques de préserver notre autonome stratégique et d'ainsi garantir le développement des activités numériques (recommandations 5 à 8).

[3] *Cybersécurité, Cyberdéfense: enjeux stratégiques, Yann Salomon, Ellipses, 2021*

UNE PRISE DE CONSCIENCE COLLECTIVE DU RISQUE CYBER EST NÉCESSAIRE POUR CONSTRUIRE UN MONDE NUMÉRIQUE DE CONFIANCE. "

I. FAIRE DE LA CYBERSÉCURITÉ UN SUJET DE SOCIÉTÉ

Quatre recommandations pour s'assurer que la population soit bien prémunie

1. SENSIBILISER LE PLUS GRAND NOMBRE

CONSTAT 1: FAIBLE PRISE DE CONSCIENCE CITOYENNE DES RISQUES CYBER ET DÉSARROI DES VICTIMES

Nous avons tous été ciblés ou victimes d'une tentative de fraude au cours de ces deux ou trois dernières années (soit nous soit notre entourage proche). Les trois escroqueries les plus recensées sont[4] :

• la fraude à la panne informatique, qui consiste à bloquer l'appareil de la victime en lui faisant penser à un problème grave pour la pousser à appeler un faux support technique qui lui facture un pseudo dépannage de plusieurs centaines d'euros; la prise de conscience puis les investigations qui en ont résulté ont permis l'interpellation début 2019 de 3 individus et la saisie de 1,9 millions d'euros d'avoirs criminels;

• le chantage au crypto porno: c'est un message d'un prétendu « hacker » qui informe avoir piraté l'appareil des cibles et les fait chanter en les menaçant de publier des informations compromettantes si elles ne paient pas une rançon de plusieurs centaines à plusieurs milliers d'euros en cryptomonnaie (bitcoin); 30000 signalements et 2000 plaintes ont été déposées;

• les escroqueries à Mon Compte Formation, où des citoyens français se font siphonner leurs crédits de formation par des mécanismes d'usurpation d'identité et/ou des complicités dans les Organismes de Formations; le préjudice estimé est de plusieurs dizaines de millions d'euros.

Comment réagissons-nous la plupart du temps ? Fort heureusement, la majorité d'entre nous repère que c'est une tentative frauduleuse et le mail ou le SMS en question est tout simplement détruit. Parfois, nous recevons un coup de téléphone de ses parents ou grands-parents, anxieux à l'idée d'avoir reçu ce type de sollicitation. On les rassure en leur disant de l'ignorer.

Combien d'entre nous effectue un signalement (auprès des autorités ou bien auprès des mécanismes en place de signalement de spams dans les grandes entreprises françaises *(par exemple abuse@orange.fr pour l'opérateur historique ou le 33700 pour les SMS indésirables) ?* Parmi les citoyens français les plus fragiles, combien ont réellement donné suite et ont été escroqués ? Enfin, parmi cette dernière catégorie, quelle proportion trop honteuse à l'idée de s'être fait avoir, n'en parle ni à ses proches ni aux autorités: *« Après tout, je n'ai perdu qu'une centaine d'euros et c'est de ma faute, j'aurais dû être plus vigilant… »*

Les cyber criminels l'ont bien compris, lorsqu'ils restent en-dessous des seuils d'acceptabilité (individuel et/ou collectif), la probabilité qu'ils ne soient jamais inquiétés est proche de un. Les statistiques officielles de cyber délinquance en France sont par conséquent très probablement largement sous-estimées. Pire encore, les victimes se sentent

[4] *Source Cybermalveillance, rapport d'activité 2021*

très régulièrement responsables de leur e-crédulité.

Il est par conséquent crucial de faire évoluer la perception des citoyens, que les victimes réelles n'aient plus honte d'avoir subi une fraude et déposent systématiquement plainte. Il faut inverser la tendance: la majorité passive des Français doit signaler les tentatives dont elle est la cible.

RECOMMANDATION 1
RÉALISER UNE CAMPAGNE NATIONALE PLURIANNUELLE DE SENSIBILISATION SUR LA CYBERSÉCURITÉ.

Dans l'écosystème numérique, la simplicité d'utilisation de la technologie prévaut sur les potentiels risques. Force est de constater que l'on n'a jamais appris à nos concitoyens à utiliser de manière sécurisée les outils digitaux dont il est fait la promotion à grand renfort de publicité. Si nous faisons le parallèle avec le monde des transports, la complexité technique du fonctionnement d'une automobile est certes totalement masquée au conducteur. Par contre, tout conducteur a une conscience bien réelle des dangers de la route : il suit un apprentissage (permis de conduire), dispose de rappels réguliers (messages de prévention routière) et subit des contrôles (radars, caméra de trafic, gendarmerie, etc.)

Nous proposons donc de réaliser un programme de sensibilisation de type « sécurité routière » sur la prévention des risques cyber. La cible privilégiée de cette campagne serait les adultes entre 18 et 60 ans en prenant en compte l'effet levier qu'ils vont avoir sur les autres catégories de la population. Ils pourront diffuser les bons messages auprès de leurs enfants: les 11-18 ans sont connectés aux réseaux sociaux de plus en plus tôt (60% des 11-12 ans disposent d'un compte sur un réseau social) et le temps passé derrière les écrans a encore augmenté sur cette tranche d'âge lors des phases de confinement en 2020 et 2021. Les 18-60 ans seront également ambassadeurs des meilleures pratiques auprès des seniors (plus prudents que les jeunes, ces derniers font beaucoup appel à l'entourage familial, en particulier à leurs enfants et petits-enfants, pour toutes les questions techniques et informatiques, y compris les sujets de cybercriminalité).

Une synthèse des études réalisées sur ce sujet montre que cette démarche doit davantage s'apparenter à un programme plutôt qu'à une simple campagne. Il faut s'inscrire dans un processus long terme, accessible en permanence, en s'appuyant également sur la notoriété acquise par le mois européen de la cybersécurité en octobre. Les messages des experts en cyber sécurité souvent complexes devront être transformés en des messages simples, forts et ludiques afin de favoriser leur appropriation et leur propagation active. Un véritable plan média devra être établi; il sera par définition multicanal : TV (spots et émissions dédiés), réseaux sociaux (personnels et professionnels), avec des messages adaptés selon la segmentation de citoyens ciblés. Ce programme pourra également faire la promotion de l'app *TousActeursCyber* présentée dans la recommandation 4.

Le budget de ce type de programme a été estimé par une étude approfondie à environ 4 millions d'euros. Il conviendra probablement de dégager du budget pluriannuel pour reprendre les mêmes messages sur du long terme afin que cette recommandation porte ses fruits et aboutisse à une véritable prise de conscience citoyenne. Les campagnes des années suivantes pourront cependant être envisagées de manière plus ciblée.

2. FORMER À TOUT ÂGE – VOLET 1, LA FORMATION PAR L'EDUCATION NATIONALE

CONSTAT 2: EXISTENCE DE MULTIPLES INITIATIVES DE SENSIBILISATION DES 6 – 18 ANS À LA CYBERSÉCURITÉ

Le Permis Internet pour les enfants, lancé en 2013, est un programme national de responsabilisation des élèves de CM2 et de leurs parents, pour un usage vigilant, sûr et responsable d'Internet. La Gendarmerie nationale et l'association AXA Prévention unissent leurs forces et leur expertise en matière de protection et de prévention contre les risques numériques à destination des enfants de 9 à 11 ans. Fin 2019, deux nouveaux thèmes sont intégrés : le cyber harcèlement, en collaboration avec notamment la mission numérique de la Gendarmerie, et l'hyper connexion ainsi que les troubles de l'attention et de la concentration qui en découlent. En 2020, 72 529 élèves de primaire ont été sensibilisés par la Gendarmerie dans le cadre de ce programme. Les détails du Permis Internet sont à découvrir sur www.permisinternet.fr

Initiée par l'Etat en 2016, Pix est une structure à but non lucratif constituée en groupement d'intérêt public ayant pour mission d'accompagner l'élévation du niveau général de compétences numériques. Rapidement promue dans l'enseignement secondaire, la certification Pix remplace en 2021 le B2i en valorisant notamment tous les acquis numériques des collégiens de 3e via une évaluation obligatoire.

La cybersécurité est abordée dans la compétence « Protection et sécurité » autour de deux thématiques:

- **Sécuriser l'environnement numérique** : Sécuriser les équipements, les communications et les données pour se prémunir contre les attaques, pièges, désagréments et incidents susceptibles de nuire au bon fonctionnement des matériels, logiciels, sites internet, et de compromettre les transactions et les données (avec des logiciels de protection, des techniques de chiffrement, la maîtrise de bonnes pratiques, etc.).
- **Protéger les données personnelles et la vie privée** : Maîtriser ses traces et gérer les données personnelles pour protéger sa vie privée et celle des autres, et adopter une pratique éclairée (avec le paramétrage des paramètres de confidentialité, la surveillance régulière de ses traces par des alertes ou autres outils, etc.)

Depuis avril 2019, l'ANSSI, en partenariat avec le ministère de l'Éducation nationale, de la Jeunesse et des Sports (MENJS) lance l'expérimentation CyberEnJeux pour former à la cybersécurité par la création de jeux[5]. Cybermalveillance dispose également d'une page dédiée à la sensibilisation des jeunes publics[6]. Elle reprend pour les 7-11 ans « Les Incollables Deviens un super-héros du Net », « Les As du Web » et le Permis Internet, pour les 11-14 ans « 1,2,3 Cyber ! », pour les Adolescents « La Hack Academy ».

[5] *Tous les détails de l'expérimentation sont rappelés sur ce lien https://www.ssi.gouv.fr/uploads/2021/09/anssi-110_bis-cyberenjeux-kit_beta.pdfhttps://www.ssi.gouv.fr/uploads/2021/09/anssi-110_bis-cyberenjeux-kit_beta.pdf*
[6] *https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/dossier-accompagnement-sensibilisation-des-jeunes*

RECOMMANDATION 2
CONCENTRER TOUTES CES INITIATIVES AUTOUR DU PROJET PIX DE L'EDUCATION NATIONALE.

Même s'il faut se réjouir des différentes initiatives pour former les jeunes citoyens français, il serait plus efficace d'allier les efforts de tous les acteurs autour d'un unique projet commun (quitte à ce que plusieurs acteurs contribuent à l'élaboration des différents modules). La déclinaison des messages par l'Education Nationale via Pix semble être le bon levier pour plusieurs raisons.

Tout d'abord c'est un programme qui est désormais reconnu et qui permet le passage à l'échelle (1,2 millions d'agents et 12 millions d'élèves).

En outre, c'est un média global sur l'acculturation au numérique et pas une solution dédiée à la cyber sécurité. Pour être pertinentes et non anxiogènes, les problématiques cyber doivent être abordées dans le cadre de l'usage du numérique, de l'utilisation des tablettes, ordinateurs, smartphones, de l'utilisation des réseaux sociaux qui font partie du quotidien de nos enfants dès l'école élémentaire.

Enfin, au même titre que l'Education Morale et Civique (EMC) est dispensée dans le cadre des programmes scolaires par un professeur d'Histoire Géographie, il est clé de responsabiliser nos jeunes générations à une utilisation raisonnée d'internet au sein de l'école par des professeurs formés dans le cadre d'un programme pédagogique défini et validé par le Ministère de l'Education Nationale.

Une montée en puissance de Pix pourrait être envisagée en définissant une ambition graduelle des connaissances à acquérir sur le domaine de la cybersécurité :

- le cycle 1 (maternelle) semble prématuré pour aborder ces notions - mieux vaut sur ce cycle se cantonner aux usages digitaux avec une approche ludique ;
- le cycle 2 (CP-CE1-CE2) permettrait d'aborder les principaux risques associés à la découverte d'internet (mauvaises rencontres) ;
- le cycle 3 (CM1-CM2-6ème) permettrait de développer l'autonomie au travers de bonnes pratiques (choix d'un mot de passe, création d'une adresse email, utilisation d'avatars ou pseudo, achats en ligne) ;
- le cycle 4 (5ème à 3ème) permettrait de mettre l'accent sur les conséquences de son empreintes numériques (données personnelles, cyber harcèlement, fraudes, usurpation d'identité).

Chacune des étapes serait validée par l'obtention d'une ceinture de couleur (comme au judo) que l'élève pourrait télécharger sur son application TousActeursCyber présentée en recommandation 4.

Le lycée et l'enseignement supérieur pourraient développer des modules spécifiques adaptés au niveau et aux spécialités des différents étudiants : la vulgarisation des notions de chiffrement, d'hash de mots de passes et d'attaques de type brut-force pourraient être une bonne illustration du programme de mathématiques dans un cursus scientifique quel qu'il soit.

Enfin, dans le cadre de la Stratégie Nationale de Cybersécurité du Programme d'Investisse-

ments d'Avenir, la démarche de soutien et d'adoption de solutions cyber par les individus, les entreprises, les collectivités et l'Etat pourrait très bien être hébergée par Pix pour toutes les initiatives en ligne. Il est prévu que cette démarche soit financée à hauteur de 176 millions d'euros, dont 156 millions de financements publics.

Pix permettrait ainsi de fédérer deux enjeux importants et indissociables tout au long de la scolarité :

- d'une part, la formation obligatoire aux nouvelles technologies de l'information et de la communication (NTIC) des élèves de la maternelle (aspect ludique) à la terminale (aspect plus scientifique) ;
- d'autre part, les risques associés à ces usages, en mettant l'accent sur la prise de conscience des manipulations possibles sur les réseaux sociaux et des dangers d'Internet.

L'utilisateur ne perçoit qu'une infime partie du chemin que parcourent ses données personnelles. Elles permettent notamment de proposer des **recommandations de produits individualisées**, ou d'estimer le prix qu'un client est prêt à payer pour un produit, et donc s'il est pertinent de lui proposer ou non une réduction sur le prix : c'est une forme de **discrimination par les prix**. Pour l'utilisateur, les données de sortie de ces algorithmes, c'est-à-dire les publicités qu'il voit, les produits qui lui sont recommandés et les prix qui lui sont proposés sont la seule manifestation de l'usage généralisé de ses données par les différents acteurs numériques.

" LE NIVEAU DE VULNÉRABILITÉ DE L'ENSEMBLE DES LOGICIELS DANS LE MONDE A ATTEINT UN STADE EXTRÊMEMENT PRÉOCCUPANT "

3. FORMER À TOUT ÂGE – VOLET 2, LA FORMATION PROFESSIONNELLE

CONSTAT 3: LES GÉNÉRATIONS DÉJÀ FORMÉES N'ONT PAS D'ACQUIS SUR LA CYBERSÉCURITÉ

La formation académique ne suffit pas pour que des générations formées il y a une vingtaine d'années, quel que soit leur niveau universitaire, disposent de compétences en adéquation avec les évolutions du monde actuel. Typiquement, la génération X n'a que très peu entendu parler de cyber sécurité pendant ses études, même pour les ingénieurs qui s'étaient spécialisés en programmation informatique. La formation professionnelle tout au long de sa carrière ou dans le cadre de reconversion est donc un levier clé de la méthode de gestion prévisionnelle emplois compétences (GPEC).

Depuis 2015, le compte personnel de formation (CPF) permet d'acquérir des droits à la formation mobilisables tout au long de sa vie professionnelle. C'est un outil au service des compétences dans les entreprises et pour les citoyens, dans les changements et transformations qu'ils rencontrent, notamment celles liées aux transitions écologiques et numériques. Parmi les principaux enjeux à venir pour Mon Compte Formation, on peut en citer trois :

- amplifier l'engagement des entreprises aux côtés de leurs salariés, en élargissant l'offre de service à destination des entreprises au travers d'abondement ;
- renforcer les contrôles qualité sur les certifications professionnelles ;
- lutter contre la fraude endémique et le démarchage abusif sur le dispositif.

Le succès du dispositif est un atout sur lequel nous pouvons capitaliser[7] : 4 millions de téléchargements de l'application mobile, 16,7 millions de visiteurs uniques sur le site, 3,87 millions de dossiers de formation acceptés pour un coût pédagogique de 5,06 milliards d'euros. Toutefois l'offre proposée actuellement en cybersécurité sur MCF est faible. Parmi les formations à distance, on ne recense que quatre formations dont une liée au droit de la cybersécurité. Pour les formations en physique, les statistiques sont un peu meilleures mais il n'y a par exemple que cinq formations à Rennes ainsi qu'à Paris qui sont pourtant les deux régions phares en terme de cybersécurité en France.

Pour élargir le constat, l'État français a instauré une obligation générale de formation dans certains domaines : ainsi, l'article L. 4141-2 du code du travail stipule que l'employeur doit organiser une formation pratique et appropriée à la santé et à la sécurité au travail. Elle porte sur plusieurs modules les conditions de circulations (R. 4141-13), les conditions d'exécution du travail (R.4141-13), la conduite à tenir en cas d'accident ou de sinistre (R. 4141-17) et l'utilité des mesures de prévention prescrites (R. 4141-4). La Caisse des Dépôts, en lien avec le Ministère du Travail, de l'Emploi et de l'Insertion travaille actuellement pour positionner Mon Compte Formation au cœur de ce dispositif de formation obligatoire en entreprise.

[7] *Données au 22/02/2022*

RECOMMANDATION 3
UTILISER MONCOMPTEFORMATION COMME LEVIER DE LA FORMATION PROFESSIONNELLE EN CYBER.

Nous proposons dans une première étape de promouvoir l'utilisation de Mon Compte Formation pour toutes les formations et certifications cyber en France.

Dans un premier temps, il conviendra d'étoffer fortement les offres proposées en incitant les organismes de formations des ESN françaises (Formind, Advens, Atos, H2S, OCD, etc.) à inscrire leurs formations et obtentions des différentes certifications (ISO27001 Lead auditor, ISO27001 Lead Implementor, ISO27005 Risk Manager, CISSP, etc.) sur Mon Compte Formation.

Dans un second temps, une grande campagne de promotion de la démarche auprès des services RH des entreprises pourrait être organisée afin de mettre en avant la dotation entreprises sur un domaine phare de gestion des compétences : la formation en cybersécurité. Une étude récente du cabinet PWC faisait état d'une pénurie de talents dans les métiers de la cyber de l'ordre de 5 000 postes à pourvoir. Une dotation entreprise de 25 millions d'euros sur le seul créneau de la cyber serait très vraisemblable au regard de l'abondement déjà alloué par l'ANCT (Agence Nationale de la Cohésion des Territoires) sur les métiers du numérique il y a deux ans.

Enfin, dans le cadre du programme France 2030, 140 millions sont prévus pour mettre en place des formations en cybersécurité via un appel à manifestation d'intérêt (AMI CMA). Le dispositif MCF pourrait naturellement devenir le portail de mise en relation entre l'offre et la demande de formations au même titre que les abondements déjà mis en oeuvre dans le cadre de France Relance 2025.

Une seconde étape, plus disruptive, serait d'intégrer la cybersécurité dans les dispositifs légaux de sécurité au travail au même titre que les risques psychosociaux. Le code du travail (et en particulier les conventions collectives des domaines les plus exposés en termes de risques cyber) pourrai(en)t être amendé(es) pour inclure le risque cyber dans les articles traitant des conditions d'exécution du travail (R.4141-13), et de la conduite à tenir en cas d'accident ou de sinistre (R. 4141-17). Fort de son initiative dans le contexte non réglementaire décrit ci-dessus, le dispositif MCF serait positionné comme un levier naturel pour la mise en oeuvre d'une formation à l'échelle afin que le tissu industriel et économique français puisse ainsi devenir davantage résilient à une attaque cyber ciblée ou bien plus globale.

4. OFFRIR UN SERVICE UNIQUE ACCESSIBLE À TOUS

CONSTAT 4: MULTIPLICITÉ ET COMPLEXITÉ DE LA DÉMATÉRIALISATION DES SERVICES DE L'ÉTAT POUR LUTTER CONTRE LA CYBERCRIMINALITÉ

L'État investit massivement depuis deux décennies dans la dématérialisation des démarches des citoyens. Le Ministère des Finances était précurseur avec la mise en place du site impots.gouv.fr désormais utilisé par tous les Français a minima une fois par an. Le développement du guichet unique France Services donne également accès dans un seul et même lieu aux

[15] *Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, en ligne.*
[16] *Sondage IFOP réalisé en avril 2019 sur un échantillon représentatif de 1 000 personnes, en ligne.*

“

IL EST CRUCIAL DE FAIRE ÉVOLUER NOTRE PERCEPTION : LA MAJORITÉ PASSIVE DOIT SIGNALER LES TENTATIVES DONT ELLE EST LA CIBLE. ”

principaux organismes de services publics : le ministère de l'Intérieur, le ministère de la Justice, les Finances publiques, Pôle emploi, l'Assurance retraite, l'Assurance maladie, la CAF, la MSA et la Poste.

La cyber criminalité étant par essence d'origine numérique, elle n'échappe pas à la volonté de digitalisation des services publics pour lutter contre son explosion ces dernières années. Le gouvernement français a ainsi mis en service différents services qui connaissent tous un succès important : Pharos, Percev@l et cybermalveillance.gouv.fr.

La plate forme Percev@l (ouverte en 2018) permet à tout citoyen de signaler aux forces de l'ordre l'utilisation frauduleuse de sa carte bancaire. Si un citoyen détecte une transaction par carte bancaire dont il n'est pas à l'origine et qu'il est toujours en possession de sa carte, il va saisir un signalement à partir des opérations identifiées sur son relevé de compte en banque. Concrètement, la personne doit renseigner le numéro de sa carte bancaire, le nom de la banque, la date, le libellé et le montant des dépenses frauduleuses constatées, ainsi que des commentaires complémentaires susceptibles d'aider les services enquêteurs dans leurs recherches. Le signalement permet de faciliter et d'accélérer le remboursement des transactions frauduleuses sur présentation d'un récépissé à sa banque.

Percev@l a une vocation uniquement judiciaire et permet de rapprocher des faits dont le préjudice est individuellement faible mais qui, une fois corrélés entre différentes victimes, peuvent représenter des montants conséquents et donc donner lieu à des saisines de services d'enquête de la gendarmerie ou de la police nationale. En 2020, Percev@l a reçu près de 320 000 signalements soit une augmentation de 86% par rapport à 2019. En moyenne, ceci représente 873 signalements par jour pour un montant cumulé du préjudice de 136 604 730 euros (soit 428 euros en moyenne par signalement).

Pharos est l'acronyme pour Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements. C'est un site web créé en 2009 pour signaler des contenus et comportements en ligne illicites. Le rôle central de cette plate-forme a été réaffirmé suite à l'attentat contre Samuel Paty avec l'ajout de personnel afin que ce service soit désormais disponible 7 jours sur 7, 24 heures sur 24. En 2020, 289 590 signalements ont été effectués en ligne. La plus grande partie des signalements concernent des escroqueries et extorsions. Viennent ensuite les atteintes aux mineurs (pédopornographie, prédation sexuelle, etc.), les signalements dans le domaine des discriminations et enfin ceux concernant l'apologie d'actes terroristes.

Le Groupement d'Intérêt Public CyberMalveillance.gouv.fr a vu le jour en 2017 (suite à une incubation au sein des services de l'ANSSI en 2016-2017). Il constitue un observatoire de la menace numérique mais assiste également les victimes d'actes de cybermalveillance. 173 000 demandes d'assistance ont été déclenchées en 2021, pour un nombre total de visiteurs uniques de 2 482 700. Les principaux types d'arnaques (faux support technique, crypto porno, MonCompteFormation, etc.) sont expliqués aux citoyens français.

Le citoyen agile en termes de dextérité digitale trouvera sans nul doute le bon site en ligne afin d'alerter efficacement et rapidement les services publics sur la fraude ou le délit d'origine cyber dont il est victime. Mais le citoyen moins alerte en outils numériques et déjà fortement perturbé par le préjudice qu'il vient de subir, risque de vite se décourager face à la complexité de l'arbre de décision auquel il est confronté pour effectuer son signalement.

RECOMMANDATION 4
CRÉER UNE APP TOUSACTEURSCYBER CENTRALISANT TOUTES LES FONCTIONNALITÉS ET INFORMATIONS CYBER ATTENDUES DES CITOYENS.

A l'instar de l'application *TousAntiCovid* qui centralise l'ensemble des informations sur la crise pandémique en France, nous proposons de développer une unique solution d'information et de signalement en ligne sous la forme d'une app Android et IOS : *TousActeursCyber*.

Le risque cyber faisant partie des trois risques systémiques communément admis par toutes les sociétés d'assurance dans leur rapport annuel depuis deux ans, avec le risque pandémique et le risque de réchauffement climatique, un parcours citoyen fluide devrait être pensé et mis en oeuvre afin d'adresser par anticipation ou par réaction toute aggravation potentielle de la cyber criminalité dans les semestres ou années à venir.

Tout d'abord, en terme de pourcentage de la population française potentiellement ciblée, cette application s'adresserait potentiellement à tous les citoyens français. Rappelons que *TousAntiCovid* compte 52 millions de premiers téléchargements et 42 millions d'activations depuis sa création en juin 2020. Bien évidemment, il est peu probable que l'application *TousActeursCyber* connaisse un tel niveau de téléchargement (sauf à ce que la France subisse une attaque cyber massive dans un futur proche ce que personne bien évidemment n'espère). Néanmoins, l'accompagnement de la mise en oeuvre de *TousActeursCyber* par les mesures proposées autour de la formation (auprès des plus jeunes, via la promotion dans Pix, auprès de toute la population française dans le cadre d'une campagne type sécurité routière et globalement via un pop-up dans MonCompteFormation lors de recherches de formations sur le domaine cyber) permettrait d'augmenter sa notoriété notamment auprès des générations Y et Millenium.

En termes de fonctionnalités, l'app devra avant tout promouvoir les services rendus auprès des citoyens français:

- L'intégration obligatoire des fonctionnalités de signalement (Percev@l, Pharos, Signal-Spam, etc.). Outre la centralisation de tous les services, des éléments d'amélioration pourraient être apportés sur certains d'entre eux : par exemple pour Percev@l, les banques pourraient se voir imposer de mettre à disposition une fonctionnalité de sélection des transactions par carte bancaire frauduleuses et de les exporter sous la forme d'un format pivot directement téléchargeable par l'app *TousActeursCyber* (automatisant ainsi un certain nombre de ressaisies manuelles sans aucune valeur ajoutée voire même plutôt source d'erreurs).
- La mise à disposition d'éléments d'actualité cyber : à l'instar du bulletin du CERT FR de l'ANSSI, des synthèses vulgarisant des informations sur la cybersécurité pourraient être consultées au moyen de cette app. Cette partie très neutre dans un 1er temps serait également susceptible d'être un relais de Viginum à terme, afin d'assurer des fonctionnalités de Lutte Informatique d'Influence (L2I) en cas de fakenews ou de tentatives d'influence de la population lors de grands évènements en France (élections nationales, organisation de JO à Paris en 2024, etc.)
- La mise en relation directe avec les services de la gendarmerie ou de la police en cas

d'attaque avérée, ainsi que la possibilité d'être informé des acteurs locaux privés (ceux ayant obtenu le label expert cyber de CyberMalveillance.gouv.fr) pouvant porter assistance notamment aux petites structures ou aux citoyens.

- Plus complexe à circonscrire en terme de liberté individuelle et de conformité CNIL, la possibilité d'envoyer des alertes au travers de l'application en cas de croisement d'informations obtenues par les opérateurs supercritiques (Cf. recommandation 7): par exemple, un smartphone connecté depuis un réseau wifi privé avec un adresse IP publique ayant été la cible d'un scan ou d'une attaque d'un serveur Command and Control (C&C) connu d'un groupe de cyber criminel pourrait être averti d'un potentiel risque imminent ou passé.
- Plus anecdotique, le stockage de passeports cyber, notamment ceux obtenus au travers de Pix (Cf. recommandation 2)

Un point structurant de la réussite de cette recommandation sera de vérifier la faisabilité au regard du droit français de concentrer tous ces services en une seule et même application. On peut se rappeler que *TousAntiCovid* a notamment subi plusieurs retouches de la part du Conseil d'État. Il est important que cette application puisse respecter la vie privée et les libertés individuelles des citoyens mais qu'elle puisse être nominative et ce indépendamment du lieu de connexion, grâce à FranceConnect par exemple pour l'identification.

L'UNION EUROPÉENNE DOIT DÉVELOPPER UNE CAPACITÉ D'APPRÉCIATION AUTONOME ET AUTOMATISÉE DU RISQUE CYBER DE SES ENTREPRISES. "

II. ADOPTER UNE STRATÉGIE NORMATIVE AMBITIEUSE ET DÉTERMINÉE

Quatre recommandations pour faire évoluer le cadre européen actuel

5. DÉROGER AU PRINCIPE D'UNIVERSALITÉ DU BUDGET POUR LA CYBERDÉFENSE

CONSTAT 5 : CROISSANCE DES RECETTES FISCALES (TAXES ET AMENDES) LIÉES AUX ACTIVITÉS DU NUMÉRIQUE

La règlementation de la sphère numérique et la lutte contre la cyber criminalité sont avant tout des moyens de sécurisation et d'encadrement du monde digital. Les taxes, amendes ou mises sous séquestre atteignent cependant ces dernières années des montants financiers importants susceptibles d'être réinvestis dans l'assainissement du monde dual numérique dans lequel tout citoyen français évolue et évoluera de plus en plus à l'avenir.

Prenons l'exemple de la CNIL : crée par la loi informatique et liberté du 6 janvier 1978, la Commission Nationale de l'Informatique et des Libertés est l'autorité administrative indépendante chargée de veiller à la protection des données personnelles contenues dans les fichiers et traitements informatiques ou papier, aussi bien privés que publics. Depuis l'application du règlement européen général sur la protection des données (RGPD) le 25 mai 2018, la CNIL a connu une croissance d'activité exponentielle. En 2020, elle employait 225 agents pour un budget de 20,1 millions d'euros. Elle a procédé à 49 mises en demeures, 38 rappels à l'ordre et 14 sanctions pour un montant d'amendes infligées de 138 millions d'euros (en 2021, le montant cumulé devrait encore être supérieur).

L'AGRASC (Agence de Gestion et de Recouvrement des Avoirs Saisis et Confisqués) est un établissement public à caractère administratif placé sous la tutelle conjointe du garde des Sceaux et du ministre des Comptes Publics. L'agence, qui est chargée de l'exécution de la peine de confiscation au nom du procureur de la République, vise par ailleurs à répondre au besoin indispensable de gestion des biens saisis, lorsque ceux-ci exigent des actes d'administration (véhicules, immeubles, fonds de commerce, bateaux, etc.) Comme une forte croissance des saisies est observée sur tous les crypto actifs, levier clé du développement de la cybercriminalité internationale, la consignation de ces actifs devrait être confiée à terme à la Caisse des Dépôts, qui serait alors susceptible de les réinvestir à 100 % dans l'économie numérique souveraine via sa banque d'investissement.

Dernier exemple, la taxe sur les services numériques. Faute d'accord européen, la France a adopté, le 11 juillet 2019, sa propre taxe GAFAM sur les services numériques. Les entreprises concernées sont celles dont le chiffre d'affaires annuel obtenu pour ses services est supérieur à 750 millions d'euros à l'échelle mondiale et 25 millions d'euros à l'échelle de la France. Le montant de la taxe est calculé en appliquant un taux de 3 % sur ce chiffre d'affaires réalisé en France. Le 1er juillet 2021, un accord plus global a été signé à l'Organisation de Coopération et de Développement Economiques (OCDE) pour la mise en place d'une fiscalité mondiale des entreprises harmonisée, avec un taux minimum d'au moins 15 %.

RECOMMANDATION 5
FLÉCHER L'ÉQUIVALENT BUDGÉTAIRE DE CES RECETTES FISCALES VERS LA SÉCURISATION DU MONDE NUMÉRIQUE.

La cybersécurité étant identifiée comme un des trois risques systémiques depuis 2019-2020, nous recommandons de s'assurer que l'équivalent en terme de budget de toutes les taxes, amendes, mises sous séquestre liées au domaine du numérique soit directement réinvesti dans la sécurisation de ce secteur en France dans un premier temps, et si possible à l'échelon de l'Union Européenne pour afficher haut et fort une ambition commune de lutte contre la cybercriminalité sur notre continent.

La pandémie COVID-19 a donné lieu à la mise en œuvre de mesures exceptionnelles en France dans le cadre de la politique initiale du « quoi qu'il en coûte » décidé par le Président de la République.

Quelques jours avant la COP26, le ministre de l'Economie a proposé de flécher les recettes fiscales liées aux énergies fossiles vers la lutte contre le réchauffement climatique. Une proposition qui déroge au principe d'universalité du budget. Près de 35 milliards seraient ainsi affectés au climat par an.

Ce principe pourrait être appliqué aux investissements en cyberdéfense : chaque euro collecté par la CNIL, l'AGRASC, les taxes GAFAM, etc. serait réinvesti pour rendre l'accès au monde digital plus sûr. La Cour des comptes pourrait diligenter une mission pour définir les priorités d'allocation de ces budgets et pérenniser un suivi de cette mesure sur du long terme. Dans un premier temps, les budgets de certaines entités particulièrement sous-dimensionnées et/ou entités permettant d'avoir un effet levier sur les entrées d'argent (amendes, mises sous séquestre) pourraient être augmentés de façon substantielle. Des actions concrètes d'urgence seraient ainsi financées, notamment sur les moyens alloués à la justice pour la lutte contre la cybercriminalité. Par exemple, la section J3 du parquet de Paris est spécialisée en matière de lutte contre cybercriminalité. C'est un élément clé du dispositif judiciaire français pour adresser le sentiment d'impunité dont les cyberattaquants ont longtemps bénéficié. Le J3 est actuellement composé de trois (3) magistrats, deux (2) greffiers, un (1) assistant spécialisé (un second en cours de recrutement fin 2021), un (1) juriste assistant et un (1) officier de liaison gendarmerie. Au cours de l'année 2021, la capacité de saisine du J3 a augmenté de 540 %. Par exemple, au titre de la compétence concurrente, il y a plus de 638 dossiers transférés au J3 qui viennent des autres juridictions. L'affectation de magistrats, greffiers supplémentaires, ainsi que l'outillage (dans un but d'automatisation) du J3 permettraient de traiter beaucoup plus efficacement les dossiers actuellement en retard ou dépriorisés.

En parallèle de ces efforts explicites sur du court terme, les investissements actuels dans le cadre des différents plans d'investissements PIA4, France Relance 2025 et France 2030 doivent bien évidemment être maintenus. L'ambition de la stratégie nationale d'accélération pour la cybersécurité, présentée le 18 février 2021 et réaffirmée en février 2022, est dotée d'un budget de 1 039 millions d'euros (dont 720 millions d'euros d'argent public). Même si les montants investis sont importants (250 millions d'euros par an en moyenne sur 5 ans dont 180 millions d'euros d'argent public), le principe de fléchage systématique induirait une marge de manœuvre globale estimable à environ 700 millions d'euros d'argent public par an.

Si la stratégie nationale cloud devait être financée sur le même fléchage, les montants annoncés au second semestre 2021 (1 791 millions d'euros dont 667 millions d'euros d'argent public, 680 millions d'euros de fonds privés et 440 millions d'euros de subvention européenne) représenteraient un delta de capacité d'investissement pour la cyber en moins d'environ 150 millions d'euros par an.

Ainsi, ce serait quelques 700 M€ (budget estimatif) - 250 M€ (plan cyber) - 150 M€ (plan cloud) = 300 M€ annuels restants pour financer en plus directement d'autres projets de souveraineté numérique et de cybersécurité en France.

Évidemment, l'augmentation de la recette fiscale devra s'accompagner dans le même temps d'une rationalisation des dépenses par une mutualisation des moyens. Il existe en effet actuellement trop d'initiatives isolées en cybersécurité, la plupart étant très souvent pertinentes et légitimes mais parfois difficilement en capacité de passage à l'échelle et adressant des problématiques trop ciblées. Cette dispersion des moyens, mentionnée dans un rapport de la Cour des Comptes rédigé en mars 2022 mais non publié, adressait en premier lieu *« l'éparpillement des compétences de la puissance publique en matière de lutte contre la cybercriminalité[8] ».*

[8] *Lettre A, article du 17 mai 2022*

LES INVESTISSEMENTS PUBLICS DEVRAIENT ÊTRE ASSUJETTIS À UNE CLAUSE DE SOUVERAINETÉ EUROPÉENNE GARANTISSANT UN NIVEAU DE "CYBERSÉCURITÉ NATIVE ET EXPLICITE". "

6. RENFORCER LES NORMES EUROPÉENNES SUR LES PRINCIPES DE « SECURITY BY DESIGN »

CONSTAT 6: UNE CROISSANCE EXPONENTIELLE DU NOMBRE DE VULNÉRABILITÉS

La généralisation du numérique a mécaniquement augmenté le nombre de solutions connectées que nous utilisons au quotidien, la plupart étant faillibles sur le plan de la sécurité autrement dit vulnérables.

Une vulnérabilité ou faille est une faiblesse dans un système informatique permettant à un attaquant de porter atteinte à l'intégrité de ce système, c'est-à-dire à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient. **Ces vulnérabilités sont la conséquence de faiblesses dans la conception**, la mise en œuvre ou l'utilisation d'un composant matériel ou logiciel du système, mais il s'agit souvent d'anomalies logicielles liées à des erreurs de programmation ou à de mauvaises pratiques. Ces dysfonctionnements logiciels sont en général corrigés à mesure de leurs découvertes, mais l'utilisateur reste exposé à une éventuelle exploitation tant que le correctif (temporaire ou définitif) n'est pas publié et installé. La procédure d'exploitation d'une vulnérabilité logicielle est appelée "exploit".

Le niveau de vulnérabilité de l'ensemble des logiciels au niveau mondial, a atteint une situation extrêmement préoccupante. L'appréciation de cette situation repose sur plusieurs critères de référence.

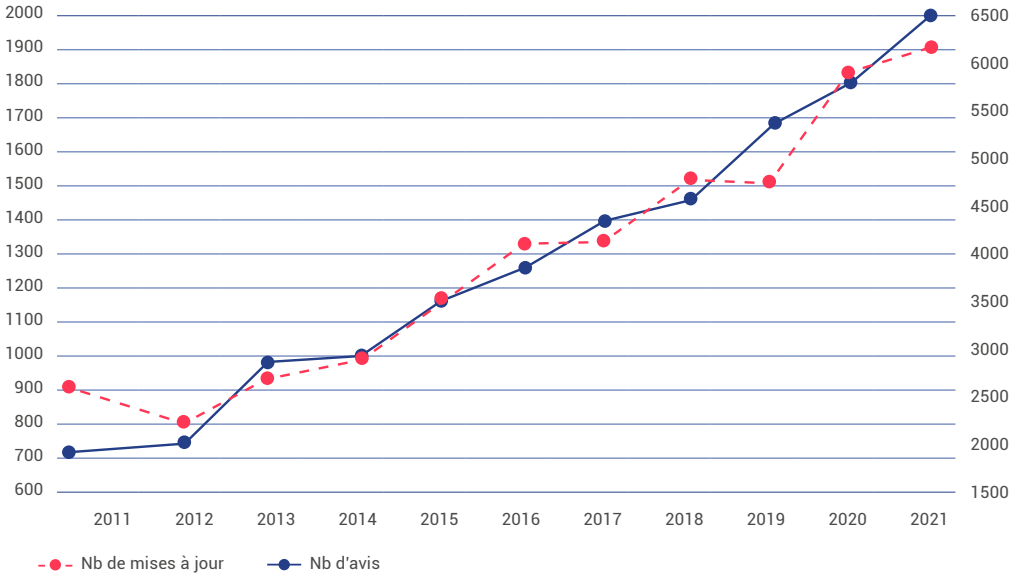

Figure 1 – Bilan 2021 de l'association Cert-IST

***(1) Le nombre d'Avis de sécurité publiés.** Ils décrivent les nouvelles vulnérabilités découvertes dans les produits suivis par le Cert-IST. 1 987 avis de sécurité ont été publiés en 2021 par le Cert-IST. Le nombre d'avis est en augmentation constante depuis plusieurs années (cf. la courbe ci-dessus), avec en 2021 une augmentation de 9% par rapport à 2020. Cette augmentation continue montre que la découverte de vulnérabilités est un phénomène en constante croissance.*

*(2) **Le nombre d'Avis modifiés.** Ces avis sont enrichis de façon continue avec des mises à jour mineures ou majeures. Ces dernières correspondent par exemple au cas où des programmes d'attaques – des "exploits" – sont publiés. 5 982 mises à jour mineures et 173 mises à jour majeures ont été publiées en 2021 par le Cert-IST.*

*(3) **Le nombre de vulnérabilités dites 0Day.** Une vulnérabilité 0Day, ou vulnérabilité du jour zéro, est une vulnérabilité informatique n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif connu. L'existence d'une telle faille sur un produit informatique implique qu'aucune protection n'existe, qu'elle soit palliative ou définitive. La terminologie « zero day » ne qualifie pas la gravité de la faille : comme toute vulnérabilité, sa gravité dépend de l'importance des dégâts pouvant être occasionnés, et de l'existence d'un exploit, c'est-à-dire d'une technique « exploitant » cette faille afin de conduire des actions indésirables sur le produit concerné.*

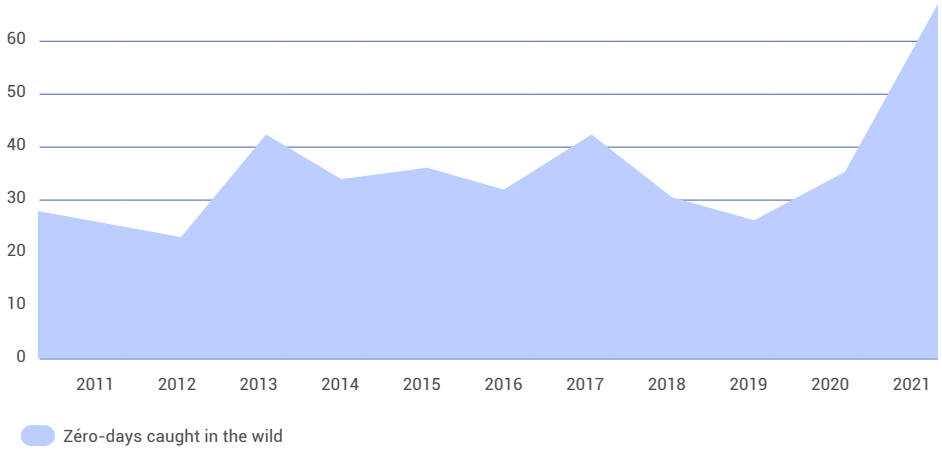

Figure 4 - Étude du MIT - Vulnérabilités 0Day sur l'année 2021

*(4) **L'ensemble des éditeurs concernés.** En résumé, l'ensemble des éditeurs est concerné. Il est intéressant de noter que les éditeurs qui font partie des plus grandes capitalisations boursières, présentent un nombre de vulnérabilités découvertes parmi les plus importantes au monde. Ce qui nous amène à considérer l'industrie des logiciels dans l'incapacité à assurer des services de confiance.*

Jusqu'à aujourd'hui, les administrations et les entreprises font face à un nombre exponentiel de vulnérabilités à traiter (correctifs ou mesures palliatives) et doivent mobiliser à leurs frais des ressources et appliquer de manière régulière (et parfois en urgence) les correctifs développés par les éditeurs.

RECOMMANDATION 6.A.
IMPOSER UNE NORME CYBER EU LISTANT LES PRINCIPES FONDAMENTAUX À FAIRE RESPECTER PAR LES INDUSTRIELS.

Avant de pouvoir accéder au marché EU, nous recommandons que toute solution connectée doive respecter un certain nombre d'engagements en termes de « vulnerability discloser policy ». Des sanctions, en cas de dysfonctionnement avéré grave, pourraient

être appliquées (ou des rappels aux frais des éditeurs et constructeurs pour remédiation à l'instar de ce qui est imposé aux constructeurs automobiles).

En complément, nous recommandons d'imposer aux professionnels du numérique une obligation de transparence ou d'information permettant à chaque usager de disposer des points de repère nécessaires pour appréhender les enjeux de sécurité associés aux produits ou solutions proposés et favoriser une utilisation responsable.

RECOMMANDATION 6.B.
RENDRE UN DIAGNOSTIC FLASH CYBERSÉCURITÉ OBLIGATOIRE.

Les entreprises devraient être tenues de faire réaliser annuellement un diagnostic flash (par exemple d'une durée d'une journée) sur quelques points de contrôle des mesures de sécurité essentielles en analogie avec le contrôle technique d'un véhicule ou la vérification d'une installation contre l'incendie. Personne ne doute qu'un ensemble de dispositifs de détection contre l'incendie soit nécessaire pour protéger les personnes et les biens matériels. Mais il n'y a pas encore la même perception sur l'immatériel. Une cyberattaque peut avoir de gros impacts opérationnels, financiers et/ou réputationnels, et aller jusqu'à paralyser une entreprise gravement et même définitivement. Combien d'entreprises connaissent les mécanismes coupe-feu, de détection ou d'isolement dans le domaine du numérique ?

7. ÉLARGIR LE PÉRIMÈTRE LÉGAL DE DÉTECTION D'ATTAQUES À CERTAINS OPÉRATEURS SUPERCRITIQUES

CONSTAT 7: EXISTENCE DE CERTAINS ACTEURS PRIVÉS AYANT UN RÔLE PRIVILÉGIÉ DANS LA LUTTE CONTRE LA CYBERCRIMINALITÉ.

Dans la revue stratégique de cyberdéfense du 12 février 2018, un zoom est effectué sur la protection des opérateurs d'importance vitale (OIV) et la protection des activités essentielles (OSE). Parmi les OIV, en raison de leur rôle de fournisseur de services auprès d'autres OIV, les secteurs des communications électroniques et de l'approvisionnement en énergie électrique peuvent être qualifiés de supercritiques (une attaque cyber sur l'un de ces acteurs ayant un effet domino sur l'ensemble des OIV). De facto, ces acteurs (notamment les acteurs historiques Orange et EDF) ont développé très tôt des capacités de cyber détection avancées et le niveau de maturité de leur CERT est reconnu par l'ensemble des acteurs privés comme publics.

Dans l'article 34 (L.33-14) de la Loi de programmation militaire 2018-607 du 13 juillet 2018, les opérateurs de télécommunications ont également vu leur rôle accru : l'ANSSI est désormais en capacité de partager avec eux des marqueurs techniques (indicateurs de compromission) afin qu'ils puissent monitorer sur leurs réseaux la présence éventuelle de ces marqueurs. Uniquement dans le cas où la présence de ces marqueurs est détectée sur des OIV ou des OSE, l'ANSSI est en capacité de disposer des informations détaillées sur ces flux. Ce processus est très strictement encadré par l'ARCEP.

De manière plus ponctuelle et sur des investigations classifiées *(que nous ne pourrons*

donc pas détailler dans ce rapport), des opérations de recherche approfondie ont été effectuées par certains opérateurs télécom. Des équipements réseaux de victimes avaient été infectés par une attaque étatique et l'analyse des flux réseau sur la totalité des équipements réseaux de France a permis de circonscrire précisément le périmètre des victimes. Concrètement et de manière très ponctuelle, certains opérateurs ont été en capacité d' « éclairer » l'ensemble des flux internet de manière séquentialisée, ce qui correspond à une recherche très précise de quelques trames sur des débits de l'ordre d'une dizaine de terabits par seconde.

Contrairement à l'interconnexion centralisée du réseau chinois à l'Internet mondial, les architectures des réseaux européens et notamment des réseaux français sont décentralisées. Il existe quelques dizaines de points d'échange internet (Global Internet eXchange) en France et une centaine de GIX en Europe de l'Ouest. Même si ces interconnexions ne sont pas uniques et rendent donc le principe de la Grande Muraille numérique de Chine impossible à décliner en Europe, leur nombre reste néanmoins fini.

RECOMMANDATION 7
ENVISAGER DE DONNER UN RÔLE PLUS IMPORTANT AUX OPÉRATEURS TELCO DANS LA DÉTECTION DES ATTAQUES CYBER.

La neutralité d'Internet est un principe fondamental de nos démocraties occidentales. Sans remettre en question cette neutralité, nous proposons d'augmenter de manière substantielle la capacité de détection des activités cyber sur les réseaux des opérateurs télécoms en inspectant des flux dupliqués (mirrorés) au niveau des points de concentration afin de ne jamais offrir à un acteur privé ou un État la capacité de filtrer certains flux d'information d'Internet (et éviter ainsi toute tentation de censure privée ou étatique).

Nous suggérons dans un premier temps d'élargir le périmètre légal de détection au niveau français ou européen. Si les marqueurs fournis actuellement sont détectés sur des entreprises (sauf OIV ni OSE), l'ANSSI n'a pas le droit d'obtenir le détail de ces informations. Une mission parlementaire (assistée d'ingénieurs de corps techniques, de juristes et d'expert de la CNIL) pourrait être diligentée pour revoir le périmètre légal d'applicabilité de la recherche de marqueurs techniques à la totalité des entreprises et citoyens sur les réseaux du territoire français. Un acteur étatique spécifique membre du comité C4 (l'ANSSI par exemple) pourrait être en charge de sélectionner les marqueurs partagés et être le garant de l'utilisation et la notification directe, des entreprises ou des citoyens, d'alertes les concernant.

Si ces contraintes légales peuvent être assouplies, des infrastructures techniques dédiées et standardisées devront être construites et financées. Les sondes actuelles (ni celles homologuées par l'ANSSI dans le cadre la LPM, ni aucune autre sonde commerciale) ne sont en capacité d'absorber des flux de plusieurs centaines de gigabits par seconde (voire quelques térabits par seconde). La plupart proposent également un mode de fonctionnement en coupure (ce qui par principe architectural devra être interdit). Ce projet dédié de recherche appliquée pourrait devenir un des projets phare du Campus Cyber nouvellement inauguré. Ces sondes auraient plusieurs modes de fonctionnement :

• mode *sampling*, avec des alertes sur des marqueurs par échantillonnage (une trame toutes les 10 000 trames par exemple) ; ce mode généraliste pourrait permettre de fournir

une météo globale de la cyber en France;

• mode *deep inspection*, avec des recherches détaillées plus ciblées (sur des temps plus courts, sur des typologies de trafic internet beaucoup plus précises) par rapport à des informations consolidées par l'ANSSI (après accord des services de renseignements dans le cadre du comité C4) ;

• des modes graduels d'inspection, entre la vision à spectre large et la vision à champ très précis, exposés ci-dessus, permettant ainsi de zoomer sur certaines typologies d'attaque (selon l'actualité ou la cible des recherches (groupe APT X ou Y)

D'un point de vue plus technique, les marqueurs partagés seraient très majoritairement des adresses IP de serveurs Command and Control (C&C) connus d'attaquants. Tout trafic IP source ou destination avec ces C&C permettrait d'identifier une adresse IP publique d'une potentielle victime (passée, en cours ou future). La résolution de cette adresse IP publique en un nom de personne (physique ou morale) et/ou une adresse email permettrait d'alerter de manière adaptée la cible potentielle. Pour l'alerte des citoyens, on peut même imaginer un dispositif permettant d'utiliser l'application *TousActeursCyber* pour véhiculer des alertes sur potentiellement n'importe quel équipement du LAN de la maison. En effet, l'application connectée sur un Wifi domestique aurait la même application IP publique que celle détectée dans le cadre du trafic malicieux et une alerte type « Contact à risque dans *TousAntiCovid* » pourrait être générée avec un lien vers des explications vulgarisées du risque encouru et les différentes actions à mener.

Si l'on reprend un peu de distance par rapport à cette recommandation, la notification des potentielles alertes sera un point clé du dispositif : elle devra être industrialisée mais personnalisée par typologie de victime potentielle, automatisée et non anxiogène, tout ceci dans un cadre préservant les libertés individuelles protégées par la CNIL.

IL N'EXISTE AUCUNE GARANTIE D'INDÉPENDANCE, AUCUN CONSENSUS SUR LA VÉRITABLE VALEUR DES NOTATIONS DE RISQUE CYBER PUBLIÉES PAR L'OLIGOPOLE DES AGENCES AMÉRICAINES. "

8.DÉVELOPPER UNE AGENCE DE NOTATION DU RISQUE CYBER SUR UN MODÈLE NORMATIF EUROPÉEN POUR TOUS LES ACHATS PUBLICS.

Après la notation financière, la notation extra-financière s'est largement développée dans la deuxième moitié du XXe siècle. Aujourd'hui incontournable, elle répond à l'obligation croissante pour les entreprises de communiquer sur la prise en compte d'objectifs ESG dans leur stratégie d'investissement. Le risque cyber y fait son apparition sous la forme d'une notation particulière. La notation répond au besoin d'indicateurs de pilotage comparatifs, car si le risque numérique est aujourd'hui considéré par tous comme majeur, il est appréhendé de façon hétérogène dans les entreprises, investisseurs, assureurs et décideurs en sont les premiers consommateurs. Depuis 2011, il se crée en moyenne une agence de notation dédiée par an dans le monde. À l'heure de la recherche de nouveaux équilibres « géo/éco-politiques » qui conduisent les blocs constitués à revendiquer une certaine autonomie stratégique, la plupart des agences de notation cyber sont nord-américaines et il n'existe aucun acteur de poids en Europe. La présidence française de l'UE porte son action sur la « souveraineté » européenne et sur la mise en œuvre d'un modèle de développement qui soutient la croissance des acteurs européens du numérique définissant ses propres règles (data, intelligence-artificielle, cyber, processeurs). Dans ce contexte, nous pensons qu'elle doit considérer le développement d'une capacité d'appréciation autonome, externe et automatisée du risque cyber des entreprises européennes.

CONSTAT 8.A. : ABSENCE DE CAPACITÉ AUTONOME D'APPRÉCIATION DU RISQUE CYBER

Il existe un oligopole des agences de rating US (95 % du marché de la notation) qui publient de plus en plus d'indices ESG et crée des standards de fait. Ces agences imposent une dépendance ou une soumission à un rating cyber unilatéral. Ces évaluations exposent les entreprises européennes aux risques de délocalisation du droit, de distorsion de concurrence ou de conflit d'intérêt.

Pour illustration BitSight, société américaine leader du marché, prend pied en Europe. La société qui compte déjà 2400 clients dans 30 pays vient de faire entrer Moody's à son capital. Elle dispose d'ores-et-déjà d'un portefeuille conséquent de mesures sur les entreprises européennes, d'un centre de développement au Portugal et des bureaux commerciaux en France. Ses équipes commerciales déploient des stratégies de conquête agressives basées sur une évaluation et un comparatif sectoriel non sollicité.

Il n'existe à date, aucune alternative européenne d'envergure, aucune garantie d'indépendance et de sérieux des mesures effectuées, aucun consensus sur la valeur des notations largement publiées.

RECOMMANDATION 8.A.
CRÉATION D'UNE ACCRÉDITATION EUROPÉENNE POUR LA NOTATION CYBER.

Compte tenu du caractère stratégique de la cybersécurité, nous recommandons la mise en place d'une accréditation européenne de notation cyber à destination des acteurs de la notation extra-financière.

Cette accréditation aurait pour objectif de garantir la fiabilité des mesures, l'indépendance des notes publiées ainsi que l'équité de traitement des entreprises européennes face aux choix d'investissement ou d'assurance liés à l'évaluation externe du risque cyber. Les exigences relatives à l'obtention de cette accréditation devraient notamment porter sur les modes de gouvernance et de financement de l'opérateur de mesure, sur la conformité de ses pratiques à des normes européennes partagées.

CONSTAT 8.B. : DES MÉTHODES D'ÉVALUATION DU RISQUE CYBER HÉTÉROGÈNES ET OPAQUES

Chaque agence de notation dispose de sa propre méthode de mesure et d'évaluation ; celle-ci sont rarement publiées. Aussi, les agences de notation extra financières font l'objet des mêmes remarques que leurs ainées : absence de transparence et insuffisance professionnelle.

Dans le cas de la notation cyber, les témoignages recueillis portent principalement sur l'incertitude relative à la pertinence du périmètre évalué, sur l'opacité des méthodes de mesures et des règles de notation, l'interprétation de la note et du niveau de risque associé au niveau des directions générales.

Il n'existe, en France, aucun consensus sur les méthodes de rating cyber déployées par les agences de notation au sein des instances professionnelles des métiers de la cybersécurité. L'absence de référence limite l'exploitation des notes aujourd'hui attribuées par les agences au seul acte de communication.

RECOMMANDATION 8.B.
DÉFINITION D'UN MODÈLE NORMATIF EUROPÉEN DE NOTATION CYBER.

Nous recommandons la concertation, le développement, la validation et la publication, au sein des instances européennes, d'une méthode normative de mesure à même d'offrir une visibilité instantanée sur l'exposition relative à un portefeuille de risques cyber explicite.

La norme éditée doit fournir une information objective et agrégée en termes de gestion de la performance, de mesure de maturité (selon les lois, règlements, normes et standards européens : NISv2, GDPR, DORA) et de risques cyber à destination des parties prenantes (actionnaires, fonds d'investissements, cabinets de M&A, banques, assureurs, donneurs d'ordres).

Elle s'appuierait sur l'aptitude technologique des acteurs européens à adresser, analyser et visualiser et partager des prises d'empreintes numériques multiples pour les confronter à des menaces protéiformes toujours plus « intelligentes » en reprenant les techniques actuelles de data management et d'IA.

CONSTAT 8.C. : DES ÉCARTS D'INTERPRÉTATION DE LA NOTATION CYBER

Au-delà de la notation, il existe d'importants écarts d'interprétation de la note accordée entre les différentes parties prenantes (décideurs, spécialistes cyber, assureurs ou investisseurs). Ces écarts proviennent d'une part de l'absence de référentiel de mesure et d'autre part des divergences liées aux perceptions individuelles d'acteurs aux parcours et aux expertises variés.

RECOMMANDATION 8.C.
MISE EN PLACE D'UNE CERTIFICATION EUROPÉENNE D'ANALYSTE CYBER.

Nous recommandons la mise en place et la formation d'analystes cyber, en vue de produire des notes d'accompagnement de la notation cyber au regard de la réalité des mesures et des impacts sur le contexte européen (politique, économique, sociétal, écologique et réglementaire).

La filière cyber est par essence technique et en regard des enjeux, il semble indispensable de former une nouvelle filière d'analystes qui sachent évaluer ces impacts, devenus majeurs pour l'Europe.

Au-delà de l'aspect normatif de cette approche de notation cyber européenne, cette recommandation servirait directement à valider que l'ensemble des investissements publics dans le numérique soient assujettis à une clause de souveraineté européenne garantissant un « niveau de cybersécurité native et explicite » des investissements proposés dans le cadre de la recommandation 5.

CONCLUSION

Vous aurez peut-être remarqué que nous avons opté pour deux partis pris dans ce rapport. Le premier, est que par souci d'efficacité économique et de responsabilité écologique, chacune de nos recommandations a visé à ne pas ajouter un nouveau dispositif, mais au contraire à dupliquer au domaine de la cybersécurité des mesures déjà connues et éprouvées dans un autre domaine, ou bien à greffer un volet cyber à des dispositifs déjà matures afin de bénéficier au maximum d'un effet levier.

Le second, a été le choix de ne pas formuler de recommandation s'appuyant sur des solutions techniques complexes ou des domaines de recherche. Nous sommes pourtant totalement convaincus qu'une partie de la réponse à la menace cyber sera adressée par les innovations techniques actuelles et à venir. Nous nous situons en effet sur le domaine cyber à une période charnière, à l'instar de celle qu'ont vécu nos ancêtres lors de la révolution industrielle : Comment passer d'un mode de production artisanal à un fonctionnement industriel ? Les ruptures dans l'innovation nous permettront ce passage d'un processus majoritairement manuel, nécessitant des efforts importants pour leur mise en œuvre et couplés à une pénurie de compétences, à une automatisation des tâches et une éradication de certains dysfonctionnements.

A ce titre, le développement des méthodes de preuves formelles en mathématiques laisse espérer une éradication à la source des vulnérabilités dans les codes informatiques les plus critiques. Les méthodes de déviances comportementales basées sur des algorithmes d'IA entrainés sur des dictionnaires de confiance pourraient aussi révolutionner l'approche actuelle des Security Opérations Center. L'implémentation systématique d'algorithmes de chiffrement post-quantiques rendrait caduques toute tentatives d'attaques par force brute. La maîtrise des fournisseurs pour se protéger des attaques par supply chain, pourrait être adressée par les travaux de recherche sur le deep-code binary analysis… La liste n'est pas exhaustive.

Mais en attendant toutes ces ruptures technologiques prometteuses, l'Etat comme les citoyens ont un rôle important à jouer, ici et maintenant, pour améliorer encore notre prise de conscience collective du risque cyber et œuvrer pour construire un monde numérique de confiance, basé sur nos valeurs françaises et européennes, et garant de nos intérêts. C'est pourquoi dans cette note, nous avons préféré nous concentrer sur la formulation des pistes d'actions concrètes afin d'améliorer d'une part la **prise de conscience de la cybermenace au sein de la société française à travers la sensibilisation et la formation** (quelle que soit la période de la vie des citoyens, et quelles que soient leurs connaissances initiales sur ce domaine) ; et d'autre part en **donnant les moyens politiques à l'Union Européenne de son autonomie stratégique via l'infléchissement de certains principes, normes ou règlements.**

RECAPITULATIF DE NOS RECOMMANDATIONS

1ER ENJEU : FAIRE DE LA CYBERSÉCURITÉ UN SUJET DE SOCIÉTÉ

S'ASSURER QUE LA POPULATION SOIT BIEN PRÉMUNIE, VIA 4 PROPOSITIONS :

SUJET	CONSTAT	RECOMMANDATION
1. Sensibiliser le plus grand nombre	Faible prise de conscience citoyenne des risques cyber et désarroi des victimes	Réaliser une campagne nationale pluriannuelle de sensibilisation sur la cybersécurité
2. Former à tout âge - volet 1, la formation par l'Education Nationale	Existence de multiples initiatives de sensibilisation des 6-18 ans à la cybersécurité	Concentrer toutes ces initiatives autour du projet Pix de l'Education Nationale
3. Former à tout âge - volet 2, la formation professionnelle	Les générations déjà formées n'ont pas d'acquis sur la cybersécurité	Utiliser Mon Compte Formation comme levier de la formation professionnelle en cyber
4. Offrir un service unique accessible à tous	Multiplicité et complexité de la dématérialisation des services de l'État pour lutter contre la cybercriminalité	Créer une app TousActeursCyber centralisant toutes les fonctionnalités et informations cyber attendues des citoyens

2ÈME ENJEU : ADOPTER UNE STRATÉGIE NORMATIVE OFFENSIVE

FAIRE ÉVOLUER LE CADRE EUROPÉEN ACTUEL, VIA 4 PROPOSITIONS :

5. Déroger au principe d'universalité du budget pour la cyberdéfense	Croissance des recettes fiscales (taxes et amendes) liées aux activités du numérique	Flécher l'équivalent budgétaire de ces recettes fiscales vers la sécurisation du monde numérique
6. Renforcer les normes européennes sur les principes de « security by design »	Une croissance exponentielle du nombre de vulnérabilités	6.a. Imposer une norme cyber eu listant les principes fondamentaux à faire respecter par les industriels 6.b. Rendre un diagnostic flash cybersécurité obligatoire
7. Élargir le périmètre légal de détections d'attaques à certains opérateurs supercritiques	Existence de certains acteurs privés ayant un rôle privilégié dans la lutte contre la cybercriminalité	Envisager de donner un rôle plus important aux opérateurs telco dans la détection des attaques cyber
8. Développer une agence de notation du risque cyber sur un modèle normatif européen pour tous les achats publics.	8.a. Absence de capacité autonome d'appréciation du risque cyber 8.b. Des méthodes d'évaluation du risque cyber hétérogènes et opaques 8.c. Des écarts d'interprétation de la notation cyber	8.a. Création d'une accréditation européenne pour la notation cyber 8.b. Définition d'un modèle normatif européen de notation cyber 8.c. Mise en place d'une certification européenne d'analyste cyber

DIDIER GRAS

Ingénieur de formation (EPITA, Télécom Paris) présente plus de 25 ans d'expérience professionnelle dédiés au domaine de la Cybersécurité qui ont permis d'éprouver dans plusieurs secteurs d'activités, l'ensemble des composantes de ce domaine sensible. Un parcours professionnel singulier qui permet d'assurer actuellement la fonction de CISO (Chief Information Security Officer) et d'IT Risk Officer de BNP Paribas – BanqueCommerciale en France.

Élu à plusieurs reprises par ses pairs, en tant qu'administrateur et secrétaire général du CESIN – Club des Experts de la Sécurité de l'Information et du Numérique (réunissant plus de 800 CISO français d'entreprises de toute tailles, d'administrations et de collectivités).

Il participe à la professionnalisation de la Filière Cyber et a créé une plateforme d'échanges sécurisés dans le cadre de la gestion intersectorielle d'alertes sur des vulnérabilités et incidents Cyber critiques.

ARNAUD MARTIN

Arnaud Martin, directeur de la cybersécurité du groupe Caisse des Dépôts, est diplômé de l'Ecole Polytechnique (X98) et de la Technische Universitaet Muenchen (2003).

Il travaille depuis 19 ans dans les technologies de l'information et leur sécurisation: chez Siemens (en Allemagne), puis en France au sein du groupe Orange et désormais à la Caisse des Dépôts.

Il a été membre du GITSIS (Groupement Interprofessionnel pour les Techniques de Sécurité des Informations Sensibles) entre 2015 et 2019, puis du CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) depuis 2019, où il anime les travaux du collège A.

Il est également auditeur de la session nationale de l'IHEDN 2021 - 2022 (majeure Souveraineté Numérique et Cybersécurité).

Digital New Deal

NOS REMERCIEMENTS

Cette publication a été écrite en parallèle de travaux menés à l'IHEDN session nationale 2021 - 2022 - majeure souveraineté numérique et cybersécurité. Elle s'appuie sur des entretiens réalisés auprès des auditeurs de la session, des intervenants extérieurs mais également de réflexions sur des thématiques ponctuelles avec des pairs du CESIN ou des collègues du groupe Caisse des Dépôts. Ce travail n'aurait pas pu voir le jour sans nos échanges notamment avec Cyril, Céline, Philippe, Gautier, Johanna, Jérôme, Laurent, Hélène, William, Antoine.

Nous remercions spécifiquement l'IHEDN et le CESIN pour nous permettre de réfléchir dans des écosystèmes privilégiés à des problématiques globales sur la cybersécurité et d'oeuvrer ainsi à la sécurisation d'une France et d'une Europe numérique.

Enfin, un grand merci à Arno Pons et Olivier Sichel pour leurs conseils avisés et relecture avant la publication de cet note !

DIGITAL NEW DEAL
LE THINK-TANK DE LA NOUVELLE DONNE

Digital New Deal accompagne les décideurs privés et publics dans la création d'un Internet des Lumières, Européen et Humaniste. Notre conviction est que nous pouvons offrir une 3ème voie numérique en visant un double objectif : défendre nos valeurs en proposant une nouvelle régulation contre la centralisation des pouvoirs ; et défendre nos intérêts en créant les conditions de la coopération face à la captation de la valeur par les « Big Tech ».

Notre activité de publication a pour vocation d'éclairer de manière la plus complète possible les évolutions à l'œuvre au sein de enjeux de « souveraineté numérique », dans l'acception la plus large du terme, et d'élaborer des pistes d'actions concrètes, voire opérantes via le Do tank, à destination des organisations économiques et politiques.

LE CONSEIL D'ADMINISTRATION

Olivier Sichel (président fondateur) et Arno Pons (délégué général), pilotent les orientations stratégiques du think-tank sous le contrôle régulier du conseil d'administration.

Forts de leur intérêt commun pour les questions numériques, les membres du Conseil d'administration ont décidé d'approfondir leurs débats en formalisant un cadre de production et de publication au sein duquel la complémentarité de leurs expériences pourra être mise au service du débat public et politique. Ils s'impliquent personnellement dans la vie de Digital New Deal, notamment dans le choix des rapports et de leurs rédacteurs. Il sont les garants de notre indépendance, académique et économique.

SÉBASTIEN BAZIN
PDG AccorHotels

NATHALIE COLLIN
DG branche Grand Public et Numérique Groupe La Poste

NICOLAS DUFOURCQ
DG de Bpifrance

AXELLE LEMAIRE
Ex-Secrétaire d'Etat du Numérique et de l'Innovation

ALAIN MINC
Président AM Conseil

DENIS OLIVENNES
DG Libération

YVES POILANE
DG Ionis Education Group

ARNO PONS
Délégué général du think tank Digital New Deal

JUDITH ROCHFELD
Professeur agrégée de Droit, Panthéon Sorbonne

OLIVIER SICHEL
President Digital New Deal
DGA Caisse des Dépôts

BRUNO SPORTISSE
PDG Inria

ROBERT ZARADER
PDG Bona fidé

NOS PUBLICATIONS

RGPD, acte II : la maîtrise collective de nos données comme impératif | Julia Roussoulières, Jean Rérolle – *mai 2022*

Fiscalité numérique, le match retour | Vincent Renoux - *septembre 2021*

Défendre l'état de droit à l'ère des plateformes | Denis Olivennes et Gilles Le Chatelier - *juin 2021*

Cloud de confiance : un enjeu d'autonomie stratégique pour l'Europe | Laurence Houdeville et Arno Pons - *mai 2021*

Livres blancs : Partage des données & tourisme | Fabernovel et Digital New Deal - *avril 2021*

Partage de données personnelles : changer la donne par la gouvernance | Matthias de Bièvre et Olivier Dion - *septembre 2020*

Réflexions dans la perspective du Digital Services Act européen | Liza Bellulo - *mars 2020*

Préserver notre souveraineté éducative : soutenir l'EdTech française | Marie-Christine Levet - *novembre 2019*

Briser le monopole des Big Tech : réguler pour libérer la multitude | Sébastien Soriano - *septembre 2019*

Sortir du syndrome de Stockholm numérique | Jean-Romain Lhomme - *octobre 2018*

Le Service Public Citoyen | Paul Duan - *juin 2018*

L'âge du web décentralisé | Clément Jeanneau - *avril 2018*

Fiscalité réelle pour un monde virtuel | Vincent Renoux - *septembre 2017*

Réguler le « numérique » | Joëlle Toledano - *mai 2017*

Appel aux candidats à l'élection présidentielle pour un #PacteNumérique | *janvier 2017*

La santé face au tsunami des NBIC et aux plateformistes | Laurent Alexandre - *juin 2016*

Quelle politique en matière de données personnelles ? | Judith Rochfeld - *septembre 2015*

Etat des lieux du numérique en Europe | Olivier Sichel - *juillet 2015*

contact@thedigitalnewdeal.org

THINK-TANK
DIGITAL
NEW DEAL

juin 2022

www.thedigitalnewdeal.org