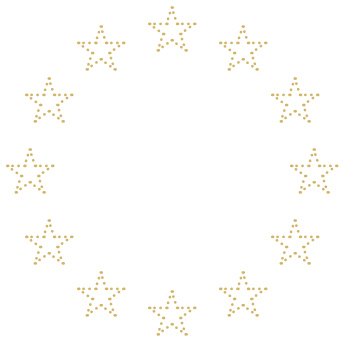
Agora FIC

FAIRE DE LA CYBERSÉCURITÉ LA CLÉ DE VOÛTE DE LA SOUVERAINETÉ NUMÉRIQUE EUROPÉENNE



28 recommandations pour la Présidence française du Conseil de l'Union européenne en matière de sécurité et de réglementation de l'espace numérique

SEPTEMBRE 2021

À PROPOS

L'Agora du FIC est le think-tank stratégique du Forum international de la cybersécurité (FIC). Il réunit les principaux décideurs économiques, académiques et politiques, et a pour vocation de contribuer au débat public sur les grands enjeux liés au numérique.

Ce rapport a été rédigé par un groupe de travail animé par le **général d'armée (2S) Marc Watin-Augouard**, fondateur du FIC, et **Guillaume Klossa**, fondateur d'EuropaNova et ancien conseiller spécial du vice-président de la Commission européenne. Les équipes d'Avisa Partners à Paris et Bruxelles y ont également contribué, notamment **Guillaume Tissier, Pauline Massart, Paul Azibert, Suzanne McNamara, Clément Rossi** et **Julien Tran Van Nhieu.**

Il s'appuie sur des auditions de personnalités venant des institutions nationales et européennes, ainsi que des sphères industrielles et académiques, et plus largement de la société civile.

Agora FIC

Le FIC est co-organisé par Avisa Partners
et la Gendarmerie nationale depuis 2013

www.forum-fic.com

SYNTHÈSE

DOMAINE	N°	TITRE	RECOMMANDATION
TALENTS & COMPÉTENCES 	1	FAVORISER L'ACCULTURATION AU NUMÉRIQUE	Développer un corpus central de formation des hauts fonctionnaires, décideurs politiques et économiques.
	2	GÉNÉRALISER LE NUMÉRIQUE DANS TOUTES LES FORMATIONS DIPLÔMANTES	Développer un e-Erasmus et une certification standardisée sur le modèle du TOEIC.
	3	ACCORDER L'OFFRE ET LA DEMANDE EN MATIÈRE D'EMPLOIS DU NUMÉRIQUE	Valoriser davantage les *« métiers du numérique »* et le *« numérique dans les métiers »* par une communication adaptée et développer une politique RH attractive.
DIPLOMATIE ET STABILITÉ DANS L'ESPACE NUMÉRIQUE 	4	PROMOUVOIR UNE VISION EUROPÉENNE DU DROIT INTERNATIONAL DU CYBERESPACE	Faire endosser par les institutions européennes les recommandations de l'Appel de Paris.
	5	APPROFONDIR LA BOÎTE À OUTILS CYBERDIPLOMATIQUE EUROPÉENNE	Enrichir les outils de la boîte à outils cyberdiplomatique : demande d'information ou d'actions correctives, partage de renseignement, capacités forensiques, liste noire…
	6	FAIRE ÉMERGER UNE RÉGULATION DU MARCHÉ DES VULNÉRABILITÉS *0-DAY*	Dresser une liste noire des entreprises ayant vendu des entités à certains régimes et encourager la coopération entre les propriétaires de vulnérabilités et les chercheurs.
	7	DÉVELOPPER UNE COMPRÉHENSION COMMUNE DES CYBERMENACES	Renforcer le dispositif collectif de connaissance de la situation cyber et opérationnaliser la clause de défense mutuelle des États membres.
CYBERDÉFENSE MILITAIRE 	8	RENFORCER LA CYBERDÉFENSE MILITAIRE DE L'UE	Mettre en place un forum des Cyber Commanders et soutenir la création d'un réseau européen de CERT militaires.
	9	RATIONALISER LA CYBERDÉFENSE EUROPÉENNE PAR UNE COMPLÉMENTARITÉ UE-OTAN	Développer le partage de bonnes pratiques entre l'UE et l'OTAN et assurer une complémentarité effective entre les deux institutions.
LUTTE ANTI CYBERCRIMINALITÉ 	10	RENFORCER LES CAPACITÉS DE LUTTE CONTRE LA CYBERCRIMINALITÉ	Créer un Parquet européen spécialisé dans la cybercriminalité et favoriser la création d'un réseau européen de compétences.
	11	PARVENIR À UNE SOLUTION ÉQUILIBRÉE SUR LA CONSERVATION DES PREUVES	Finaliser les travaux législatifs relatifs au règlement *« e-evidence »* dans le respect des prérogatives de l'autorité judiciaire et des principes fondamentaux liés aux données à caractère personnel.
	12	DONNER UNE NOUVELLE IMPULSION À LA CONVENTION DE BUDAPEST	Promouvoir la ratification de la Convention de Budapest par des États non membres du Conseil de l'Europe et poursuivre les travaux d'adaptation.
	13	RENFORCER LA LUTTE CONTRE LES CONTENUS ILLICITES	Mettre en place une base de données de signatures des contenus illicites et renforcer la place des acteurs de confiance.

DOMAINE	N°	TITRE	RECOMMANDATION
CYBERSÉCURITÉ & RÉSILIENCE 	14	IMPOSER LA SÉCURITÉ « *BY DESIGN* »	Accélérer la mise en place de schémas européens de certification et faire adopter au niveau international le principe de responsabilité des éditeurs et fabricants systémiques.
	15	DÉVELOPPER UNE CAPACITÉ EUROPÉENNE DE RÉACTION FACE À DES INCIDENTS MAJEURS	Finaliser la mise en place de la nouvelle unité conjointe de cybersécurité en s'inspirant du dispositif existant en matière de sécurité civile.
	16	RENFORCER LA PROTECTION DES SYSTÈMES D'INFORMATION DE L'UE	Renforcer les capacités du CERT-UE et créer une qualification *« cybersécurité »* obligatoire pour tous les fonctionnaires de l'UE.
	17	RENFORCER LA PROTECTION DES INFRASTRUCTURES CRITIQUES	Finaliser le projet de directive NIS 2, en y intégrant toute la chaîne d'approvisionnement des produits numériques, et en intégrant un levier réglementaire sur les fournisseurs de services numériques.
	18	ENCOURAGER LES POLITIQUES DE DIVULGATION COORDONNÉE	Imposer aux entités *« essentielles »* et *« importantes »* au sens du projet de directive NIS 2 des politiques de divulgation coordonnée de vulnérabilités.
	19	AMÉLIORER LA CYBERSÉCURITÉ TRANSFRONTALIÈRE	Créer à titre expérimental des CERT transfrontaliers, soit généralistes, soit sectoriels (énergie par exemple).
POLITIQUE INDUSTRIELLE 	20	CRÉER UN INDICATEUR DE TRAÇABILITÉ NUMÉRIQUE	Mettre en place un indicateur de traçabilité des produits et services numériques reposant sur la transparence de la chaîne de valeur utilisée, la conformité au RGPD, ainsi que la localisation du stockage et des principaux traitements de données.
	21	REDYNAMISER LE SYSTÈME EUROPÉEN DE NORMALISATION	Décliner le cadre européen de certification institué par le *Cybersecurity Act* et créer une certification des équipements de sécurité valable à l'échelle de l'UE.
	22	MOBILISER L'ACHAT PUBLIC ET PRIVÉ	Instituer un *« Buy Digital European Act »* pour tout achat public et mettre en place des crédits d'impôts et mécanismes de sur-amortissement pour l'achat privé.
	23	RENFORCER L'INVESTISSEMENT PUBLIC ET PRIVÉ	Adapter les conditions proposées par la Banque européenne d'investissement (BEI) ou le Fonds européen d'investissement (FEI) aux PME et ETI et mobiliser le fonds du Conseil européen de l'innovation.
	24	FACILITER LES TRANSFERTS DE TECHNOLOGIES	Assouplir les conditions de propriété intellectuelle et les modalités financières encadrant les transferts de technologie du monde académique vers les entreprises.
	25	AMÉLIORER LE SOUTIEN DE L'INNOVATION	Assurer une meilleure coordination et évaluation des programmes existants et donner une place à part aux *« deep tech »*.
	26	FAIRE ÉMERGER DES LEADERS EUROPÉENS EN MATIÈRE DE *CLOUD COMPUTING*	Créer des alliances industrielles dans le cadre de la nouvelle politique industrielle de la Commission européenne en utilisant le statut *« Projets importants d'intérêt européen commun »* (PIIEC).
	27	FAVORISER LE DÉVELOPPEMENT D'UNE IDENTITÉ NUMÉRIQUE EUROPÉENNE	Favoriser l'adoption de la nouvelle mouture du règlement eIDAS et initier une meilleure adoption des identités numériques au sein du secteur privé régulé.
	28	ACCÉLÉRER LA MISE EN PLACE D'UNE RÉGULATION DES ACTEURS SYSTÉMIQUES	Appliquer strictement le droit de la concurrence aux marchés numériques grâce à un *Digital Markets Act* (DMA) robuste et doter la Commission européenne d'un service d'intelligence économique.

SOMMAIRE

[...] Parce que l'Europe manifeste son dynamisme, parce que ce marché de 320 millions d'habitants au niveau de vie élevé suscite bien des convoitises, on n'hésite pas à nous dépeindre en train d'ériger murailles et tours d'angles. Ne soyons pas dupes. Ceux qui nous décrivent ainsi sont ceux qui veulent voir l'Europe ouverte sans politique commune, sans réaction, sans volonté politique. Ce sont ceux qui, chez eux, votent des lois commerciales protectionnistes ou ralentissent par toutes sortes de faux-semblants une timide ouverture de leur propre marché. À ceux-là nous disons clairement : l'Europe sera ouverte, mais pas offerte.

JACQUES DELORS
AU PARLEMENT EUROPÉEN

17 JANVIER 1989

INTRODUCTION

L'**Europe du numérique se construit.** Il y a encore quelques décennies, une telle hypothèse n'était pas envisageable, car la transformation numérique n'avait pas l'ampleur d'aujourd'hui. Cette dynamique s'est néanmoins récemment accélérée, sous l'effet d'une Union européenne (UE) plus volontariste, qui multiplie les annonces en faveur d'une stratégie industrielle numérique pour ses vingt-sept États membres.

Le rêve d'une Europe en mesure de proposer sa propre gamme de produits numériques n'est pourtant pas nouveau. Dès 1970, la création du consortium Unidata, qui réunissait la Compagnie internationale pour l'informatique (France), Philips (Pays-Bas) et Siemens (Allemagne), visait à concurrencer dans la dimension industrielle les États-Unis, en lui opposant un poids lourd européen. Le retrait unilatéral de la France, quelques années plus tard, a néanmoins brisé cet élan. Si ce projet a engendré nombre d'irritants, il éclaire aujourd'hui l'avenir et donne des indications sur ce qu'il convient d'accomplir : **la Présidence française du Conseil de l'Union européenne (PFUE) à venir doit être marquée par un volontarisme teinté d'humilité.**

Un demi-siècle plus tard, les ambitions européennes s'inscrivent dans un nouveau contexte stratégique influencé par deux super-puissances numériques, les États-Unis et la Chine. Cette dynamique risque à terme de marginaliser notre continent, qui s'immisce pourtant entre ce duopole en qualité de deuxième économie mondiale. Si l'UE s'est distinguée sur la scène internationale par son encadrement du numérique (directive vie privée et communications électroniques, eIDAS, RGPD…), elle reste une *« colonie du monde numérique »* sur le plan industriel, au regard de son dénuement dans certaines technologies structurantes de l'ère numérique (grandes plateformes, *cloud*, semi-conducteurs, etc.), et de son incapacité à développer une commande publique européenne en mesure de rivaliser avec celles nationales des États-Unis et de la Chine.

La crise sanitaire a dès lors accéléré la prise de conscience de la nécessité de faire évoluer l'Europe de puissance *« régulatrice »* à *« créatrice »*. Une quête qui ne doit pas pour autant nous conduire à dégarnir le front réglementaire, comme en témoignent les futurs *Digital Markets Act* (DMA), *Digital Services Act* (DSA) et *Data Governance Act* (DGA). **La pandémie a mis en exergue, outre le besoin de maîtriser les dépendances géopolitiques et économiques, l'exigence d'une *« souveraineté numérique »* sous l'angle de l'autonomie stratégique.** La Commission a ainsi érigé le numérique comme l'un de ses quatorze *« écosystèmes industriels »* prioritaires, pour recréer des chaînes de valeur et d'approvisionnement dans le marché unique.

Pour se donner les moyens de son ambition, l'UE a doté en avril 2021 son programme pour une Europe numérique (2021-2027) d'un budget de 7,6 milliards d'euros[1]. Celui-ci vise, outre la compétitivité et la souveraineté technologique, **le déploiement généralisé des technologies numériques au service des citoyens, des entreprises et des administrations publiques de l'UE.** Ce projet s'appuie à cet égard sur des investissements en faveur de quatre priorités, qui constituent autant de domaines stratégiques : le calcul à haute performance, l'intelligence artificielle, les *« compétences numériques avancées »* et la cybersécurité.

En matière de cybersécurité, clé de sa souveraineté numérique, l'Europe a vite pris la mesure du risque et de ses évolutions. En 2007, la cyberattaque visant l'Estonie a été un électrochoc qui a conduit plusieurs États membres à concevoir une stratégie dédiée. Si l'UE s'est d'abord penchée sur les infrastructures critiques, puis sur les réseaux et les systèmes d'information, l'augmentation et la sophistication des attaques l'a décidée à aller plus loin pour

1. Règlement (UE) 2021/694 du Parlement européen et du Conseil du 29 avril 2021.

ne pas devenir le *« maillon faible de la lutte contre cette menace mondiale*[2] *»*. Elle a ainsi voté le *Cybersecurity Act* (2019) qui jette les bases d'une approche commune de la cybercriminalité, la *« criminalité du XXIème siècle »*. D'autant qu'une cyber-conflictualité s'y superpose, souvent d'origine ou d'inspiration étatique, en profitant de l'absence d'une gouvernance reconnue de tous.

Dans ce contexte incertain, **la Commission européenne a présenté sa nouvelle stratégie de cybersécurité en décembre 2020.** Cette feuille de route vise, outre le développement de la résilience collective vis-à-vis du risque cyber, à rendre sûrs et fiables les outils et les services numériques à la disposition des citoyens et des entreprises en Europe. Elle permettra dès lors à l'UE de s'affirmer en acteur incontournable des normes et des standards de cybersécurité, en plus d'un meilleur encadrement de sa coopération internationale en faveur d'un cyberespace *« ouvert, stable, sûr »*. Celui-ci doit se fonder sur les valeurs européennes : la démocratie, l'État de droit, les droits de l'homme et les libertés fondamentales. Plusieurs mesures concrètes sont prévues à cet égard en termes de réglementation, d'investissements et d'actions.

La conception européenne de la transformation numérique doit replacer l'humain au cœur du débat et de l'action, en s'appuyant sur les valeurs que partagent les citoyens européens. Ces derniers doivent être les acteurs d'une mutation profonde et *« historique »* de la société sous l'effet d'un espace numérique qui est désormais un substrat intriqué dans tous les milieux, terrestre, maritime, aérien ou extra-atmosphérique.

L'hyperconnexion, couplée à l'intelligence artificielle et au big data, se développe de manière exponentielle et confère au traitement des données et à leur exploitation une puissance inégalée dans l'histoire. La croissance annoncée du *cloud* est telle que celui-ci sera demain *« l'espace numérique »* à lui seul.

Les citoyens portent des espérances sur les progrès escomptés, en même temps qu'ils craignent de devenir esclaves d'un système à l'encontre de leur autodétermination numérique, au travers de leur conditionnement par les algorithmes, d'atteintes à la vie privée, ou à leurs libertés d'opinion et de décision, fortement entamées par les manipulations de l'information. La couche sémantique de l'espace numérique sera sans doute demain le centre de gravité, dans toutes les acceptions du terme, de la cybersécurité.

Il importe certes que le discours européen porte sur les usages, les technologies et notamment de rupture, la réglementation et les organisations. **Mais il faut surtout des actes qui, au-delà de l'indispensable confiance qu'ils sont susceptibles de créer, mobilisent des Européens mieux informés et formés.** La ressource humaine sera le meilleur atout de l'Europe si elle ambitionne de tenir son rang dans le monde. La crise sanitaire a perturbé le quotidien des citoyens, remis en cause des certitudes, créé le doute, notamment dans la capacité des élites nationales ou européennes à maîtriser un séisme économique et social inédit. Le numérique appliqué à la santé devient dès lors le vecteur le plus approprié sans doute pour relancer une conscience collective.

Avant de vouloir penser pour le monde, l'Europe doit agir pour elle-même, tout en évitant l'entre-soi de ses vingt-sept États membres. L'heure est venue pour elle d'offrir une voie, de porter une voix qui s'adresse au reste du monde, à l'attention d'autres États qui ne souhaitent pas s'inscrire dans une nouvelle bipolarité. Cette action doit se tourner vers des pays situés dans d'autres continents, en Afrique, Amérique latine et Asie avec lesquels elle partage des valeurs et des intérêts communs. Le Brésil, l'Inde, l'Afrique du Sud, le Japon, la Corée du Sud et Taïwan, sans oublier la francophonie, sont des partenaires avec lesquels cette stratégie peut être développée. Celle-ci ne doit pas contrarier le dialogue transatlantique mais l'équilibrer.

Du 1er janvier au 1er juillet 2022, la France assurera la présidence tournante du Conseil de l'UE, succédant au Portugal et à la Slovénie, et précédant la République tchèque. Cette présidence s'inscrit dans un mouvement collectif,

2. Discours de Jean-Claude Juncker au sommet numérique de Tallin en septembre 2017.

porté depuis plusieurs années par les vingt-sept États membres. Il serait donc prétentieux d'afficher une posture de rupture. Pour autant, la France, fondatrice de l'UE, conserve une influence forte, au sein de l'Union mais aussi dans le reste du monde. Son discours est souvent attendu, même si certains le critiquent.

La France devra sans doute faire avancer la réponse collective à la question *« comment ? »*, par la mise en œuvre des voies et moyens permettant de mettre en application les décisions déjà prises, d'en accélérer le calendrier par un dialogue stimulant. Mais elle devra surtout contribuer à un nouveau souffle, dont les premiers signes se font sentir, par la réponse à la question *« pourquoi ? »*. Le sens doit être le moteur de la vision stratégique. Avec humilité, mais aussi avec sa capacité d'influence, elle doit faire de la PFUE un moment fort qui devra être prolongé par la présidence tchèque. La construction du discours relève de la responsabilité politique, mais son contenu sera d'autant plus riche qu'il prendra en compte les propositions de la société civile.

Le Forum international de la cybersécurité (FIC) est une enceinte qui a, depuis ses origines, l'ambition de rassembler l'écosystème numérique en transcendant les clivages liés aux frontières, en développant les partenariats public-privé, avec un regard résolument tourné vers le service de l'humain. Il s'agit de son ADN !

C'est donc avec un état d'esprit, reflet de son ambition, qu'il présente ci-après des propositions. Ces travaux ne couvrent pas le seul champ de la cybersécurité qui ne saurait être dissocié d'une conception plus englobante de la transformation numérique. La cybersécurité conditionne l'essor du numérique, le numérique apporte une contribution à la cybersécurité.

Bien que ce ne soit pas l'objet direct de cette réflexion, l'Europe du numérique ne peut être conçue sans l'exigence de durabilité, cybersécurité et durabilité étant deux composantes de la résilience.

Le discours politique sur le numérique ne peut définitivement plus se résumer à l'objectif de développement de *« nouveaux usages »* et du marché intérieur.

TEXTES FONDATEURS

L'EUROPE DU NUMÉRIQUE

- Directive vie privée et communications électroniques *12 juillet 2002*
- Règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur – eIDAS *23 juillet 2014*
- Règlement 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 – RGPD *27 avril 2016*
- Façonner l'avenir numérique de l'Europe *19 février 2020*
- Une stratégie européenne pour les données *19 février 2020*
- Rapport sur les conséquences de l'intelligence artificielle, de l'internet des objets et de la robotique sur la sécurité et la responsabilité *19 février 2020*
- Livre blanc sur l'intelligence artificielle : une approche européenne axée sur l'excellence et la confiance *19 février 2020*
- Nouvelle stratégie industrielle : construire un marché unique plus fort pour la relance de l'Europe *5 mai 2021*

L'EUROPE DE LA CYBERSÉCURITÉ

- Directive concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection *8 décembre 2008*
- Directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union – NIS *6 juillet 2016*
- Règlement relatif à l'Agence de l'Union européenne pour la cybersécurité et à la certification de cybersécurité des technologies de l'information et des communications, également appelé *Cybersecurity Act* *17 avril 2019*
- Règlement concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres *17 mai 2019*
- Stratégie de cybersécurité européenne pour la décennie numérique *16 décembre 2020*

RECOMMANDATIONS

TALENTS
& COMPÉTENCES

Pour l'Europe, le développement des talents et des compétences numériques conditionne la transformation numérique de son économie et le développement de la citoyenneté – et donc de l'identité – européenne. Sur le plan professionnel, près de neuf emplois sur dix exigeront à l'avenir de maîtriser certaines compétences numériques, tandis qu'une large partie de l'exercice de la vie démocratique s'appuiera sur le numérique.

Ces talents et compétences sont de deux ordres :

- Cognitives, émotionnelles ou sociales, qui sont une base nécessaire à l'utilisation des technologies numériques. L'acculturation est ainsi essentielle dans la lutte contre le phénomène des *« fake news » ;*

- Techniques, qui permettent d'utiliser le numérique de façon sûre, qu'il s'agisse de compétences liées à l'utilisation des technologies ou à la production d'équipements ou services intégrant du numérique. Le cadre des compétences numériques (DigComp) de l'UE en distingue 21 réparties en cinq domaines (traitement de l'information, communication, création de contenu, sécurité et résolution de problèmes).

1 FAVORISER **L'ACCULTURATION AU NUMÉRIQUE**

CONSTAT La transformation numérique bouleverse notre société. Parce qu'elle est caractérisée par l'infiniment grand, l'infiniment petit et l'infiniment rapide, elle s'opère hors du cadre espace-temps traditionnel et se développe à une vitesse qui est décorrélée du rythme classique de la décision politique, administrative, financière. L'accélération du monde n'attend pas. Les organisations traditionnelles sont mises à l'épreuve avec l'émergence d'organisations systémiques, globales et réticulaires. C'est à une rupture des pratiques professionnelles que sont confrontées les élites qui subissent souvent plus qu'elles ne portent la transformation numérique. À court terme, la *« déconnexion des élites »*[3] pourrait contrarier le développement de la société numérique et entraîner une rupture générationnelle vecteur de tensions. Parce qu'il faut *« épouser son siècle »*, les décideurs européens publics ou privés, civils ou militaires, doivent partager une vision collective s'appuyant sur un référentiel commun.

OBJECTIF Créer dans chaque État membre qui le souhaite une formation à destination des décideurs sur le modèle de l'Institut des hautes études de Défense nationale (IHEDN) en France. Une formation similaire pourrait être organisée pour tous les responsables de haut niveau, civils et militaires, qui travaillent au sein des institutions de l'Union européenne.

RECOMMANDATIONS

› Développer un corpus central de formation des hauts fonctionnaires, décideurs politiques et économiques. Celui-ci guidera les formations nationales, qui prendront en compte les spécificités des États membres. Le cursus central pourra être développé conjointement par le Collège d'Europe avec le soutien des chercheurs de l'Institut d'études de sécurité de l'Union européenne (IESUE) et du Collège européen de sécurité et de défense (CESD), s'appuyant sur l'expérience de ce dernier dans la création d'un cursus européen de formation en cyberdéfense pour les militaires des vingt-sept États membres.

› Favoriser les échanges croisés d'auditeurs entre les États membres afin de disposer à terme d'une *« communauté du cyber »* européenne partageant une même vision. Un MOOC commun pourrait être la première étape d'un dispositif plus élaboré.

3. Laure Belot, *La déconnexion des élites*, Les Arènes, 2015.

INTÉGRER LE **NUMÉRIQUE** ET LA **CYBERSÉCURITÉ** DANS LES **CURSUS UNIVERSITAIRES**

2

CONSTAT Le manque de compétences sur le numérique va augmenter dans les années qui viennent en Europe. La Commission européenne évoque 500 000 emplois non pourvus dans ce domaine en général, et en particulier la cybersécurité, la science des données et l'intelligence artificielle d'ici 2025. Cette pénurie risque de constituer pour l'Europe un goulet d'étranglement majeur pour la croissance et l'emploi, un frein à l'innovation et un risque sérieux de la voir perdre la maîtrise des technologies.

La transformation numérique a un impact sur tous les métiers. Ses incidences ne se limitent pas aux branches orientées vers les technologies mais affectent tous les secteurs des sciences humaines et sociales (« *humanités numériques* »), des services, de l'industrie. Il est aujourd'hui possible d'être diplômé sans jamais avoir reçu de formation relative au numérique, aux transformations et aux risques qu'il engendre. Or les cyberattaques concernent l'ensemble de nos sociétés, des simples citoyens aux États.

OBJECTIF Renforcer la formation initiale et continue pour créer une compréhension commune des enjeux de la transformation numérique et des risques associés. Il est urgent d'inclure dans l'ensemble des cursus de formation, au sein des écoles et des universités de l'UE, une acculturation au numérique et à la sécurité numérique, en particulier dans les formations de haut niveau. S'agissant des cursus spécialisés, il s'agira de multiplier les échanges universitaires intra-européens afin de créer une conscience européenne commune face aux cybermenaces.

RECOMMANDATIONS

- Introduire des sessions de sensibilisation à la sécurité en ligne, ainsi que des cours de codage, à l'attention des plus jeunes dès l'école primaire. Les bases seront ensuite consolidées au collège.
- Créer une certification européenne standardisée garantissant un niveau de connaissance minimum à l'ensemble des étudiants, quels que soient leurs cursus, en matière de numérique. Elle se déclinerait en plusieurs niveaux, sur le modèle entre autres du TOEIC et du TOEFL, correspondant à l'enseignement secondaire (niveau 1) et supérieurs, en Bac +3 (niveau 2) et Bac +5 (niveau 3). Elle validerait la maîtrise basique des outils indispensables mais surtout la connaissance des usages, du fonctionnement et des risques associés. Cette certification vise à établir une « *culture générale numérique* », qui ne soit pas uniquement centrée sur les connaissances techniques, et à assurer à l'ensemble des secteurs de l'économie des compétences numériques minimales. Elle offrirait une première sensibilisation aux enjeux de cybersécurité et permettrait d'attirer des profils féminins vers des carrières technologiques.

- Valoriser l'ensemble des compétences non techniques (sciences humaines et sociales) liées à la cybersécurité dans l'organisation des compétitions ou challenges européens, en particulier l'European Cyber Security Challenge (ECSC) de l'ENISA.
- Développer une cartographie des formations en cybersécurité disponibles dans chaque État membre en Europe, sur le modèle de SecNumEdu de l'ANSSI en France. Cette initiative accélérerait le développement d'échanges universitaires intra-européens, avec l'octroi de bourses dédiées, qui faciliteront à terme l'interopérabilité des procédures et méthodologies techniques opérationnelles (détection, réponse à incident) entre pays européens dès les cursus de formation initiale.

ACCORDER **L'OFFRE ET LA DEMANDE** EN MATIÈRE **D'EMPLOIS DU NUMÉRIQUE**

3

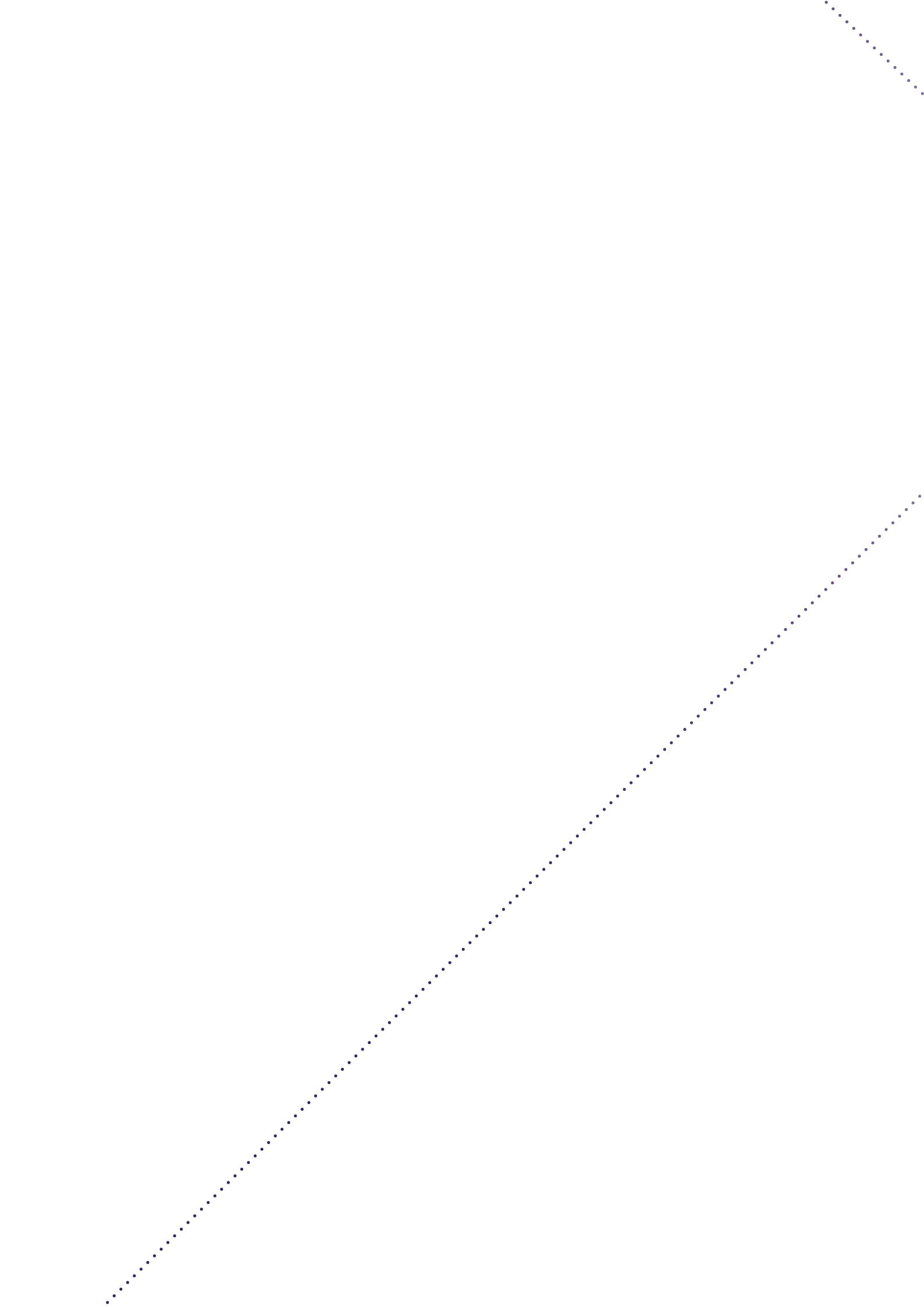
CONSTAT Si les chiffres peuvent varier, tous les observateurs s'accordent pour évaluer à plusieurs centaines de milliers le nombre d'emplois liés au numérique non pourvus à l'horizon 2025, notamment dans la cybersécurité, la science des données et l'intelligence artificielle. Cette pénurie concerne de façon plus large tous les profils STEM (sciences, technologies, *engineering* et mathématiques) et s'est encore aggravée avec la pandémie. D'ici 2030, 9 emplois sur 10 exigeront ainsi des compétences numériques. Or 44% de la population européenne (16-74 ans) ne maîtrisent pas les compétences numériques de base même si 79% se connectent régulièrement[4]. Le développement de ces compétences constitue donc non seulement une réponse au chômage, en particulier des jeunes, mais également la condition *sine qua non* d'une Europe puissance numérique. Toutes les politiques publiques sont vaines si la ressource humaine fait défaut.

OBJECTIF En cohérence avec le DigComp, cadre de référence de l'UE pour les compétences numériques, développer et soutenir l'offre de formation aux métiers du numérique en encourageant l'accès aux femmes, aujourd'hui anormalement minoritaires.

RECOMMANDATIONS

- Valoriser les métiers du numérique par une communication s'adressant en particulier aux femmes, notamment à l'occasion du mois européen de la cybersécurité, qui a connu sa huitième édition en 2020.
- Développer une politique des ressources humaines qui soit attractive et fidélise les jeunes Européens formés qui s'expatrient souvent vers le plus offrant, notamment outre-Atlantique.
- Concevoir une coopération avec les pays étrangers qui envoient des jeunes en formation dans les universités et les grandes écoles européennes, afin que ces États ne compensent pas, par une évasion de leurs élites, les insuffisances de l'UE, une fuite des cerveaux qu'elle-même cherche à contrer.

4. Monika Kiss, *Les compétences numériques sur le marché du travail de l'Union*, Service de recherche du Parlement européen, janvier 2017.



DIPLOMATIE ET STABILITÉ DANS L'ESPACE NUMÉRIQUE

Faute d'une gouvernance reconnue de tous, la criminalité et la conflictualité étatique ne cessent de se développer dans l'espace numérique. Des cyberattaques sont désormais suffisamment sophistiquées pour affecter depuis l'autre bout du monde le fonctionnement d'États, mais aussi d'entreprises, profitant de la numérisation accrue de nos sociétés. Si plusieurs exemples ont révélé le potentiel systémique et les impacts géopolitiques associés à l'utilisation malveillante de technologies numériques (WannaCry, NotPetya, Solarwinds…), d'autres, de plus faible intensité, menacent au quotidien la sécurité et la vie privée des internautes. En outre, la crise Covid-19 a rappelé que des vies pouvaient aussi être menacées, comme en témoigne la hausse d'attaques informatiques contre des hôpitaux. Vecteurs de risques pour la sécurité internationale, ces comportements irresponsables ont fait jusque-là l'objet – sans franc succès – de plusieurs tentatives diplomatiques visant à les réduire. L'Europe, forte de sa puissance diplomatique et normative, doit proposer une alternative fondée sur ses valeurs pour obtenir le consensus de la communauté internationale.

4 PROMOUVOIR UNE **VISION EUROPÉENNE** DU DROIT INTERNATIONAL DU CYBERESPACE

CONSTAT L'intérêt des Nations Unies à l'égard des menaces liées aux technologies de l'information et de la communication (TIC) sur la sécurité internationale remonte à une vingtaine d'années. Pour promouvoir la stabilité dans le monde, l'enceinte diplomatique a favorisé l'émergence de plusieurs initiatives – aux succès jusque-là modestes même s'ils sont encourageants – visant à instituer un comportement responsable des États dans le cyberespace.

Entre 2019 et 2021, deux projets ont reçu un mandat onusien pour formuler des recommandations en faveur de ces comportements. Le premier, sous l'impulsion de la Russie, a créé un groupe de travail à composition non limitée (OEWG) rassemblant 140 États. Le second, porté par les États-Unis, a établi en réaction le sixième groupe d'experts gouvernementaux (GGE) qui a réuni de manière plus exclusive vingt-cinq États.

Le quatrième GGE en 2015 s'est distingué en jetant les bases du cadre normatif en vigueur[5], sur lequel se fondent depuis toutes les discussions relatives à ce sujet, dont celles de l'OEWG. Ce cadre repose sur quatre *« piliers »* reconnus de tous : l'applicabilité du droit international au cyberespace, onze normes de comportement, des mesures de confiance, ainsi que le renforcement des cyber-capacités des États.

LES NORMES DES NATIONS UNIES SUR LE COMPORTEMENT RESPONSABLE DES ÉTATS DANS LE CYBERESPACE :

- Coopérer au niveau interétatique dans le domaine de la cybersécurité
- Examen de toutes les informations utiles
- Prévenir l'utilisation abusive des TIC sur les territoires nationaux
- Collaborer pour mettre fin à la criminalité et au terrorisme
- Respecter les droits de l'homme et la vie privée
- Ne pas endommager les infrastructures essentielles
- Protéger les infrastructures essentielles
- Répondre aux demandes d'aide
- Garantir l'intégrité de la chaîne logistique
- Signaler les failles informatiques
- Ne pas porter atteinte aux équipes d'intervention d'urgence

5. Nations Unies, Assemblée générale, Progrès de l'informatique et des télécommunications et sécurité internationale, A/70/174, 22 juillet 2015.

En mars 2021, l'OEWG a réalisé une prouesse diplomatique[6] avec l'adoption de son rapport final par consensus de tous ses participants. Pour autant, le groupe n'y formule pas de proposition substantielle sur l'applicabilité du droit international au cyberespace. Le document ne mentionne en effet ni le principe de *due diligence* ni le droit international humanitaire (DIH). L'application du DIH cristallise pourtant des tensions, ses partisans considérant que des cyberattaques contre des infrastructures critiques peuvent avoir un coût humain et ses opposants estimant qu'elle reviendrait à militariser le cyberespace[7].

Doté d'un mandat similaire, le sixième GGE est lui aussi parvenu à un consensus en mai 2021[8], avec quelques avancées. Si son rapport reconnaît que le DIH s'applique aux cyber-opérations en temps de conflit armé, la mise en œuvre de cette applicabilité reste à déterminer. Les débats autour de la reconnaissance des principes de *due diligence* et de souveraineté en règles juridiques sont en revanche restés en suspens[9].

La concurrence entre ces deux initiatives traduit néanmoins des conceptions différentes du cyberespace. Si certains pays cherchent à le contrôler dans la limite de leurs territoires, au nom du principe de souveraineté, d'autres le souhaitent libre, ouvert et sécurisé. Cette distinction induit respectivement deux tendances avec, d'une part, les États souhaitant créer de nouvelles règles contraignantes à travers un nouveau traité (Chine, Russie…), et, d'autre part, ceux qui défendent un *statu quo* en estimant que le droit international existant, complété de normes volontaires et non contraignantes, est suffisant [10] (États-Unis, pays occidentaux…).

L'Occident ne forme pour autant pas un bloc homogène. Des divergences existent, particulièrement sur la reconnaissance en tant que règle de droit du principe de *due diligence*[11]. Plusieurs pays européens tels que l'Allemagne[12], la Finlande[13] et la France[14] y sont favorables, à l'inverse notable des États-Unis.

6. Aude Géry, « ThucyBlog n° 118 – Ils l'ont fait ! Adoption d'un rapport par l'OEWG sur les progrès des TIC dans le contexte de la sécurité internationale : un succès diplomatique certain », *Centre Thucydide*, 5 avril 2021.
7. Arindrajit Basu, Irene Poetranto, Justin Lau, « The UN Struggles to Make Progress on Securing Cyberspace », *Carnegie*, 19 mai 2021.
8. Nations Unies, *Report of the Group of Governmental Experts on Advancing responsible State*, 28 mai 2021.
9. Michael Schmitt, « The Sixth United Nations GGE and International Law in Cyberspace », *Just Security,* 10 juin 2021.
10. *Op. cit.* Arindrajit Basu, Irene Poetranto, Justin Lau, 19 mai 2021.
11. Selon ce principe rappelé par le quatrième GGE (2015), les États ne doivent pas permettre sciemment que leurs territoires soient utilisés pour commettre des faits internationalement illicites à l'aide des TIC.
12. « On the Application of International Law in Cyberspace », The Federal Government, Germany, mars 2021.
13. « Finland published its positions on public international law in cyberspace », Finnish Government, octobre 2020.
14. Ministère des Armées, *Droit international appliqué aux opérations dans le cyberespace,* septembre 2019.

OBJECTIF Promouvoir une vision européenne de l'applicabilité du droit international au cyberespace, centrée sur les valeurs sur lesquelles est fondée l'Union, pour favoriser un consensus au sein des Nations Unies.

RECOMMANDATIONS

Faire émerger cette *« troisième voie »* européenne de l'applicabilité du droit international au cyberespace, entre celle des États-Unis d'une part et celle de la Chine et de la Russie d'autre part, implique de :

- Mettre en place une formation commune européenne de droit international pour favoriser les appréciations communes entre les États membres.
- Considérer le principe de *due diligence* comme étant la condition première d'une utilisation pacifique du cyberespace. La responsabilisation des États et la mise en cause de leur responsabilité internationale doivent bloquer toute velléité d'utilisation du cyberespace pour des stratégies indirectes.
- Identifier et adopter par ailleurs collectivement au sein de l'UE les règles les plus consensuelles, à commencer par l'interdiction du *hack back*, l'utilisation pacifique du cyberespace, et la protection des infrastructures critiques dont en premier lieu les établissements de santé.
- Rallier tous les pays ayant une vision similaire, ainsi que les *« swing States »* peu engagés dans les débats sur les normes, tels que l'Afrique du Sud, la Corée du Sud, l'Inde…
- Ne pas ajouter une brique supplémentaire à toutes les initiatives diplomatiques existantes, mais plutôt faire endosser par l'UE les recommandations de l'Appel de Paris afin d'orienter ses futures politiques publiques sur l'espace numérique et sa protection[15].

15. Commission supérieure du numérique et des postes, *Recommandations dans le domaine de la sécurité numérique*, Avis n°2021-03, Recommandation n°20, 29 avril 2021.

APPROFONDIR
LA BOÎTE À OUTILS CYBERDIPLOMATIQUE DE L'UE

CONSTAT La boîte à outils cyberdiplomatique (*EU Cyber Diplomacy Toolbox*) constitue le cadre pour une réponse diplomatique conjointe de l'UE en cas de cyberattaque la visant. Institué en 2017, cet instrument précise l'ensemble des mesures – notamment restrictives – relevant de la Politique étrangère et de sécurité commune (PESC) à mobiliser pour protéger l'UE et les États membres des actes de cyber-malveillance.

Cette initiative a été renforcée deux ans plus tard par l'introduction d'un régime de sanctions. Celles-ci comprennent des interdictions de voyager *« vers et au sein »* de l'UE, ainsi que des mesures de gel des avoirs avec l'interdiction entre autres de *« mise à disposition de fonds ou de ressources économiques*[16] *»*.

En juillet 2020, l'UE a imposé ses premières sanctions dans ce cadre contre six individus et trois entités (originaires de Chine, Corée du Nord et Russie), auxquelles ont été attribuées[17] les cyberattaques WannaCry et NotPetya, l'opération *Cloud Hopper*, et la tentative de piratage de l'Organisation pour l'interdiction des armes chimiques (OIAC)[18].

Toutefois, si des mesures restrictives sont prises contre les individus et entités impliqués dans des cyberattaques, il n'en demeure pas moins que l'attribution collective de ces dernières par l'UE est un défi, certains États membres souhaitant garder leur autonomie de décision.

En amont des attributions et des sanctions, la boîte à outils prévoit ainsi plusieurs mesures diplomatiques telles que la demande d'information ou d'actions correctives aux pays d'où émane une cyberattaque. Ce volet implique une densification à la fois du partage d'informations et des capacités d'analyse au sein du Centre de situation et du renseignement de l'Union européenne (INTCEN). Sur ce dernier point, le développement capacitaire doit reposer sur des exercices conjoints, davantage de synergies avec le secteur privé, ainsi que le maintien d'une coopération avec l'OTAN et le Royaume-Uni à la suite du Brexit[19, 20].

OBJECTIF Donner à la boîte à outils cyberdiplomatique une assise opérationnelle et en faire un instrument international d'influence, de dissuasion et de sanction, sur le modèle des décrets exécutifs aux États-Unis.

16. « Adoption des toutes premières sanctions économiques européennes en matière de cybermalveillance », *Hughes Hubbard & Reed*, 8 septembre 2020
17. Union européenne, *Règlement d'exécution du Conseil concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres*, 30 juillet 2020.
18. « EU imposes the first ever sanctions against cyber-attacks », *Union européenne,* 30 juillet 2020.
19. Stefan Soesanto, « Europe has no strategy on cyber sanctions », *Lawfare*, 20 novembre 2020.
20. Paul Ivan, *Responding to cyberattacks : prospects for the EU Cyber Diplomacy Toolbox,* EPC, 18 mars 2019.

RECOMMANDATIONS

- Renforcer le partage de l'information au sein de l'INTCEN pour consolider l'action non coercitive et l'influence de la boîte à outils cyberdiplomatique.
- Développer les capacités forensiques au niveau européen en coopérant davantage avec le secteur privé.
- Établir au niveau européen une liste noire des individus ou des entités ayant vendu des capacités offensives à des États, ou à d'autres entités sous sanction ou risquant de les utiliser à des fins contraires aux droits fondamentaux ou intérêts de l'UE et de ses États membres.
- Développer une stratégie de communication cohérente sur la boîte à outils cyberdiplomatique, qu'il s'agisse des actions qu'elle permet ou des décisions adoptées, en particulier via les États membres, pour renforcer leur poids politique et leur caractère dissuasif.

FAIRE ÉMERGER UNE **RÉGULATION DU MARCHÉ** DES **VULNÉRABILITÉS *0-DAY***

CONSTAT Une industrie cyber *« offensive »* permettant à des États, voire à des organisations criminelles ou terroristes non-étatiques, d'acheter *« sur étagère »* des vulnérabilités *« zero-day »* (*0-day*), c'est-à-dire n'ayant fait l'objet ni de publication ni de correctif connu, s'est développée en quelques années. Un véritable marché gris, légal mais non contrôlé par les propriétaires des vulnérabilités et éditeurs logiciels, s'est même structuré autour d'un écosystème comprenant des chercheurs en cybersécurité, des courtiers (*brokers*) ainsi que des entreprises privées vendant des solutions de surveillance (solutions dites *« Access-as-a-Service »*). Les premiers acteurs identifient les *0-day* puis, au lieu de les partager à l'éditeur de logiciel ou au fabricant de matériel en vue de leur correction, les vendent, accompagnées des exploits permettant de les utiliser de façon plus ou moins industrialisée, aux deuxièmes voire aux troisièmes pour en tirer les meilleurs bénéfices. Ce marché contribue largement à la prolifération d'un arsenal *« cyber »*.

OBJECTIF Capitaliser sur la puissance diplomatique et normative de l'UE pour contribuer à l'encadrement des acquisitions de vulnérabilités 0-day, en soutenant les discussions internationales, en particulier dans le cadre de l'Appel de Paris et aux Nations Unies.

RECOMMANDATIONS

- Développer un programme de gestion de vulnérabilités dans un cadre européen et le promouvoir auprès de l'allié transatlantique.
- Encourager la coopération entre les propriétaires des vulnérabilités et les chercheurs pour réduire les risques liés à une diffusion publique en promouvant des politiques de divulgation coordonnée[21].
- Identifier dans des *« listes noires »* les entreprises ayant vendu des capacités à des entités sous sanction ou susceptibles de les utiliser à des fins contraires aux droits fondamentaux ou considérées comme non légitimes par les États membres.
- Organiser des *bug bounties* pour encourager et encadrer la recherche en vulnérabilités en proposant une alternative financièrement intéressante pour les chercheurs en cybersécurité.

21. « Encouraging vulnerability treatment: Overview for policy makers », *OECD Digital Economy Papers*, n°307, OECD, Paris, 2021, pp. 24-25.

7 DÉVELOPPER UNE **COMPRÉHENSION COMMUNE** DES **CYBERMENACES**

CONSTAT En raison de la détérioration de la situation sécuritaire dans son voisinage, l'UE cristallise des attentes quant à son rôle dans la prévention de crise, la stabilisation et la paix régionales. La réalité est toutefois différente[22]. Bien qu'elle ait renforcé son architecture de sécurité et ses capacités grâce à la Politique de sécurité et de défense commune (PSDC), les États membres font finalement peu usage de ce cadre multilatéral, comme en témoigne le nombre modeste de missions et d'opérations associées en cours[23].

Les États membres se distinguent par des priorités et des perspectives différentes du fait de leurs différences de culture stratégique. Si ce pluralisme constitue un point fort de l'UE, qui dispose de surcroît d'une vision des dossiers internationaux à *« 360 degrés »*, il ne contribue toutefois pas à la cohésion intra-européenne. D'autant que les États membres votent régulièrement en faveur d'opérations européennes sans pour autant mobiliser les forces requises ensuite[24]. Face à ces impasses opérationnelles, plusieurs pays privilégient au multilatéralisme de la PSDC des *« coalitions de volontaires »*, un format qui permet de travailler de façon pragmatique avec les pays les plus *« volontaires et capables »*, au lieu d'attendre le consensus de tous.

Cette tendance traduit, outre l'absence d'adhésion à la gestion européenne de crise, l'incapacité de l'UE à proposer une réponse collective crédible. Or, dans le cyberespace, la définition d'une posture commune passe par une vision conjointe des menaces et des vulnérabilités : les Européens doivent pouvoir ensemble anticiper, détecter, comprendre, caractériser et, le cas échéant, attribuer les actions adverses. Cette méthode permettra *a minima* de limiter leurs effets et de reprendre l'initiative dans l'intention de décourager.

L'identification conjointe des cybermenaces est donc primordiale. Elle nécessite un cadre permettant aux États membres de désigner en toute confidentialité leurs adversaires, afin de mieux raisonner sur la façon dont ils se manifestent, car toutes les cyberattaques relèvent d'une stratégie et d'une intentionnalité.

L'Allemagne a lancé à cet effet le projet de la *« Boussole stratégique »* en 2020. Ces réflexions visent à clarifier les relations entre les États membres et à crédibiliser l'UE en tant que partenaire international. Elles doivent faire converger les Européens autour d'une analyse partagée de la (cyber)menace, point de départ à un dialogue européen et à l'identification des priorités.

22. Jana Puglierin, « La Boussole stratégique de l'Union européenne », *ECFR*, 9 avril 2021.

23. Douze missions civiles et six opérations militaires.

24. « Boussole stratégique : développement de bases stratégiques », *eu2020.de*, 25 août 2020.

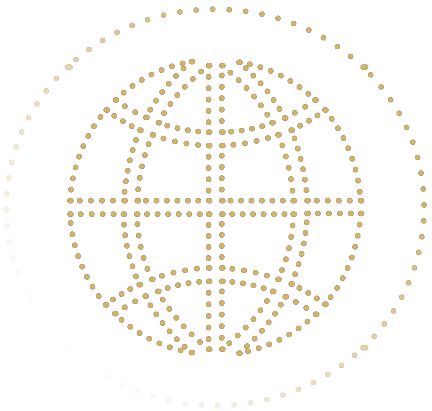
Cette compréhension commune ne pourra néanmoins être renforcée qu'en favorisant le partage d'informations, en créant la confiance et en assurant un niveau commun de cybersécurité entre les États membres. Sur ce dernier point, si le cadre législatif permet de garantir un seuil, les disparités de capacités opérationnelles doivent être réduites à l'aide de coopérations.

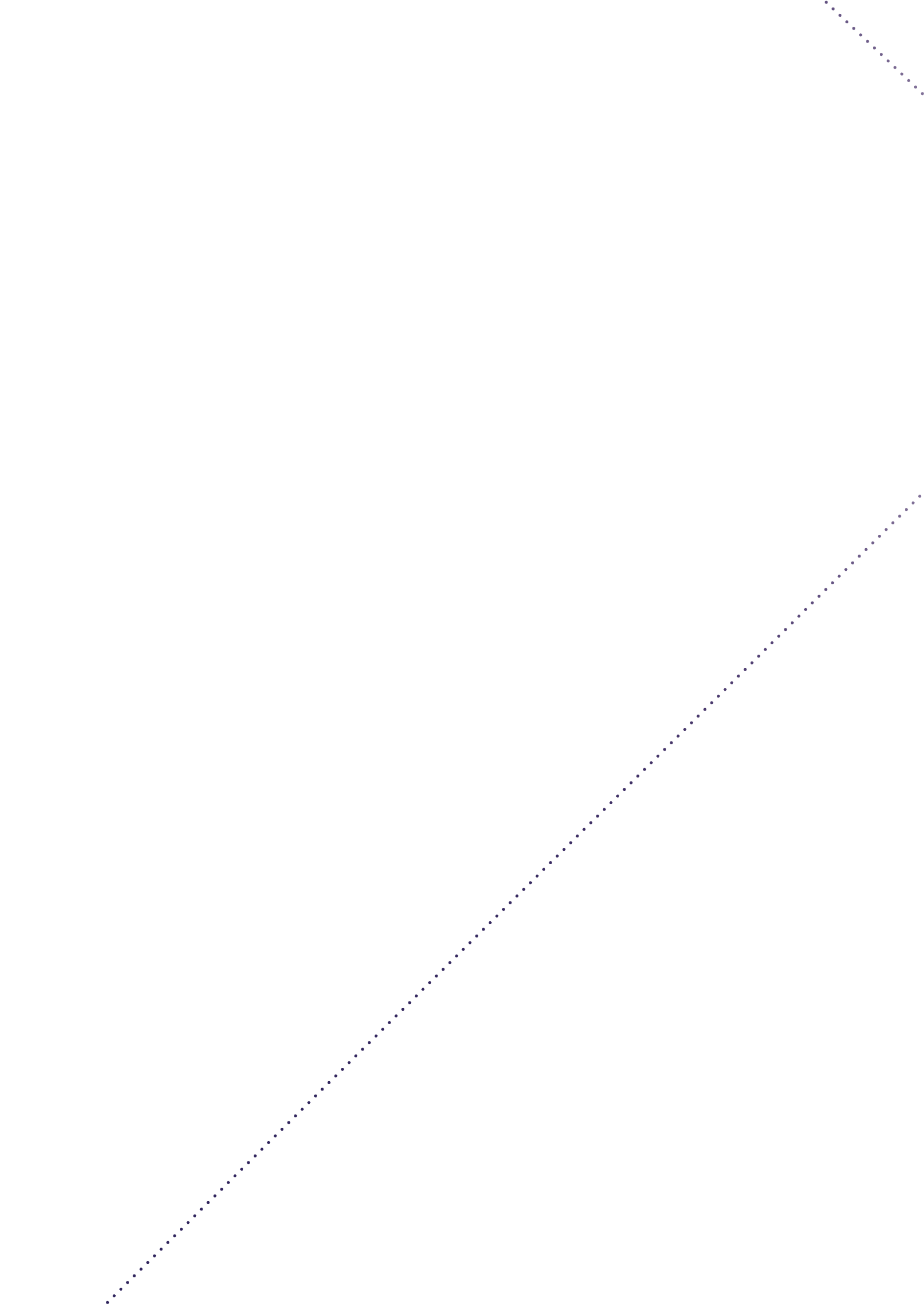
OBJECTIF Accélérer l'adoption de la *« Boussole stratégique »* qui constitue une étape essentielle au renforcement de la solidarité européenne face aux incidents cyber.

RECOMMANDATIONS

L'adoption et la mise en œuvre de la Boussole stratégique impliquent en amont de :

- Renforcer le dispositif collectif de connaissance de la situation cyber à partir du développement d'outils *ad hoc* au travers d'une base industrielle et technologique de défense européenne (BITDE).
- Étudier la possibilité de mobiliser le concours du secteur privé pour détecter les cybermenaces, dans la limite bien établie de leurs responsabilités et du niveau de confidentialité.





CYBERDÉFENSE MILITAIRE

Le cyberespace est le théâtre d'une conflictualité assumée au même titre que la terre, l'air, la mer et l'espace. Afin de mieux appréhender sa dimension militaire, l'UE a lancé l'élaboration d'une stratégie qui formalisera sa capacité à y conduire des opérations comme elle le fait dans les autres milieux. Cette feuille de route affirmera dès lors plusieurs volontés européennes en termes d'autonomie, de dissuasion, de continuum civilo-militaire, de coopération (en premier lieu avec l'OTAN), et de développement capacitaire. Le développement de la cyberdéfense militaire de l'UE pourra compter à ces égards sur un grand nombre d'acteurs dont les États membres, son état-major (EMUE) et l'Agence européenne de défense (AED). Pour autant, ce foisonnement d'intervenants, mais aussi de projets et d'initiatives, implique d'apporter coordination et cohérence d'ensemble, alors que les ressources sont aujourd'hui rares et insuffisantes.

8 RENFORCER LA **CYBERDÉFENSE MILITAIRE** DE L'UE

CONSTAT Les Européens aspirent à agir de façon autonome et collective en matière de cyberdéfense militaire[25]. Prévue par l'article 42.7 du TUE, la clause de défense mutuelle, la *« solidarité européenne »,* implique que les États membres peuvent se solliciter en cas de cyberattaque majeure contre l'un d'entre eux. Si les modalités de mise en œuvre restent à déterminer (type d'assistance, délais…), il demeure que l'UE dispose déjà d'une architecture couvrant l'ensemble du spectre des cyber-opérations, puisqu'elle se décline en une multitude d'entités lui permettant d'organiser, d'équiper et d'entraîner ses États membres : Politique de sécurité et de défense commune (PSDC), état-major de l'UE (EMUE), Agence européenne de Défense (AED), Coopération structurée permanente (CSP ou PESCO en anglais), réseaux de CERT…

Relevant de la PSDC, la CSP permet à un groupe d'États membres de prendre des engagements mutuels en matière de dépenses militaires, de programmes d'armements et de capacités opérationnelles. Ce cadre a dès lors permis l'émergence de quatre structures collectives de cyberdéfense, parmi lesquelles :

- Le Cyber and Information Domain Coordination Center (CSP/CIDCC), qui constitue, sur le plan opérationnel, l'embryon d'un centre de *command-and-control* (C2) des cyber-opérations militaires. Il ne réunit pour autant que quatre États membres en l'état (Allemagne, France, Hongrie et Pays-Bas) ;

- le Cyber Rapid Reaction Team (CSP/CRRT), en charge de l'alerte et de la réponse à incident. Cette équipe ne dispose toutefois pas des bases juridiques nécessaires pour intervenir au-delà de ses six seules nations participantes (Croatie, Estonie, Lituanie, Pays-Bas, Pologne et Roumanie).

Bien que les projets CSP permettent de développer l'interopérabilité européenne, la faible participation des États membres en limite les marges de manœuvre. L'AED pallie néanmoins ces carences, grâce à son rôle central en termes de formation et d'entraînement. Ses exercices tels que Cyber Phalanx, EU MilCERT Interoperability Conference (MIC) et CYBRID, permettent en effet de densifier et d'éprouver en conditions réelles les cyber-capacités opérationnelles des nations européennes.

25. Union européenne, *Vision partagée, action commune : Une Europe plus forte*, juin 2016, p. 16.

OBJECTIF Disposer d'un leadership fort et dans la durée afin de renforcer et d'assurer une cohérence de l'existant, plutôt que d'ajouter de nouvelles structures ou fonctions de cyberdéfense militaire, dans un contexte où les ressources humaines des États membres sont contraintes.

RECOMMANDATIONS

Le développement de la cyberdéfense militaire, ne pouvant se limiter à une seule présidence du Conseil de l'UE, implique une coordination globale et pérenne. La PFUE doit initier – si ce n'est poursuivre – une dynamique en faveur de son développement collectif. Deux priorités :

- Renforcer la coopération stratégique entre les autorités compétentes des États membres, grâce à la création d'un forum des Cyber Commanders, en complément de la traditionnelle CIS&CD Conference.
- Initier et soutenir la création d'un réseau européen de CERT militaires pour développer l'interopérabilité des États membres. Ce projet identifié dès 2014, mais délaissé depuis, est une opportunité de réunir des ressources nationales au profit d'une coopération fructueuse sur le plan étatique mais aussi de l'UE.

9 RATIONALISER LA **CYBERDÉFENSE EUROPÉENNE** PAR UNE **COMPLÉMENTARITÉ UE-OTAN**

CONSTAT La coopération de cyberdéfense entre l'UE et l'OTAN est limitée et en deçà de son potentiel. Par leur vingt et un membres communs, ces organisations font pourtant face aux mêmes défis et couvrent une zone d'action analogue, mais les échanges opérationnels ne sont pas au niveau de la relation stratégique.

En 2016, ces institutions ont signé une déclaration conjointe définissant les questions d'intérêt commun, qui sont depuis traitées à l'occasion d'un dialogue de haut niveau. Ce dernier se caractérise par une convergence forte sur, outre le risque cyber et les menaces hybrides, la Chine et la Russie entre autres[26]. L'UE et l'OTAN se confrontent en effet aujourd'hui à des acteurs ayant de plus en plus recours, pour obtenir des gains, à des stratégies hybrides combinant des moyens diplomatiques, informationnels, militaires, économiques et juridiques, selon une dynamique d'ensemble ambiguë et difficile à déceler ou à dénoncer[27].

Face à ces stratégies globales de puissance, dans lesquelles le cyber occupe une place grandissante, garantir la liberté d'action européenne implique d'investir le cyberespace. Si l'UE a pris du retard dans l'appréhension de cet espace de compétition, l'OTAN – dont l'essence même tient à la défense et à la cyberdéfense *de facto* des Alliés – l'a vite reconnu en tant que domaine opérationnel et s'est ainsi impliquée plus en amont dans la résilience de la majorité des États membres, contribuant à la sécurité de l'Europe.

Par des moyens financiers plus conséquents sur le plan militaire, l'Alliance dispose d'entités plus matures (Cyber Operations Centre, Cooperative Cyber Defence Centre of Excellence…) que celles de l'Union et pèse donc davantage sur le développement des cyber-capacités militaires des pays européens. Pour l'UE, qui a une approche plus large de la cyberdéfense, la dimension militaire n'est qu'un volet parmi d'autres.

OBJECTIF Rationaliser la cyberdéfense militaire de l'Europe en faisant interagir les avancées civiles de l'UE et l'expertise opérationnelle de l'OTAN. L'aspect dual du cyberespace implique en effet que les réglementations civiles soient parfois prescriptrices pour les applications militaires[28].

26. OTAN, *Les relations OTAN-UE*, Fiche d'information, Division Diplomatie Publique, mars 2021, p. 2

27. Ministère des Armées, *Actualisation stratégique*, 2021, p. 39.

28. Morgan Jouy, « Une cyberdéfense collective en Europe ? », Note de recherche, n°83, IRSEM, 2017.

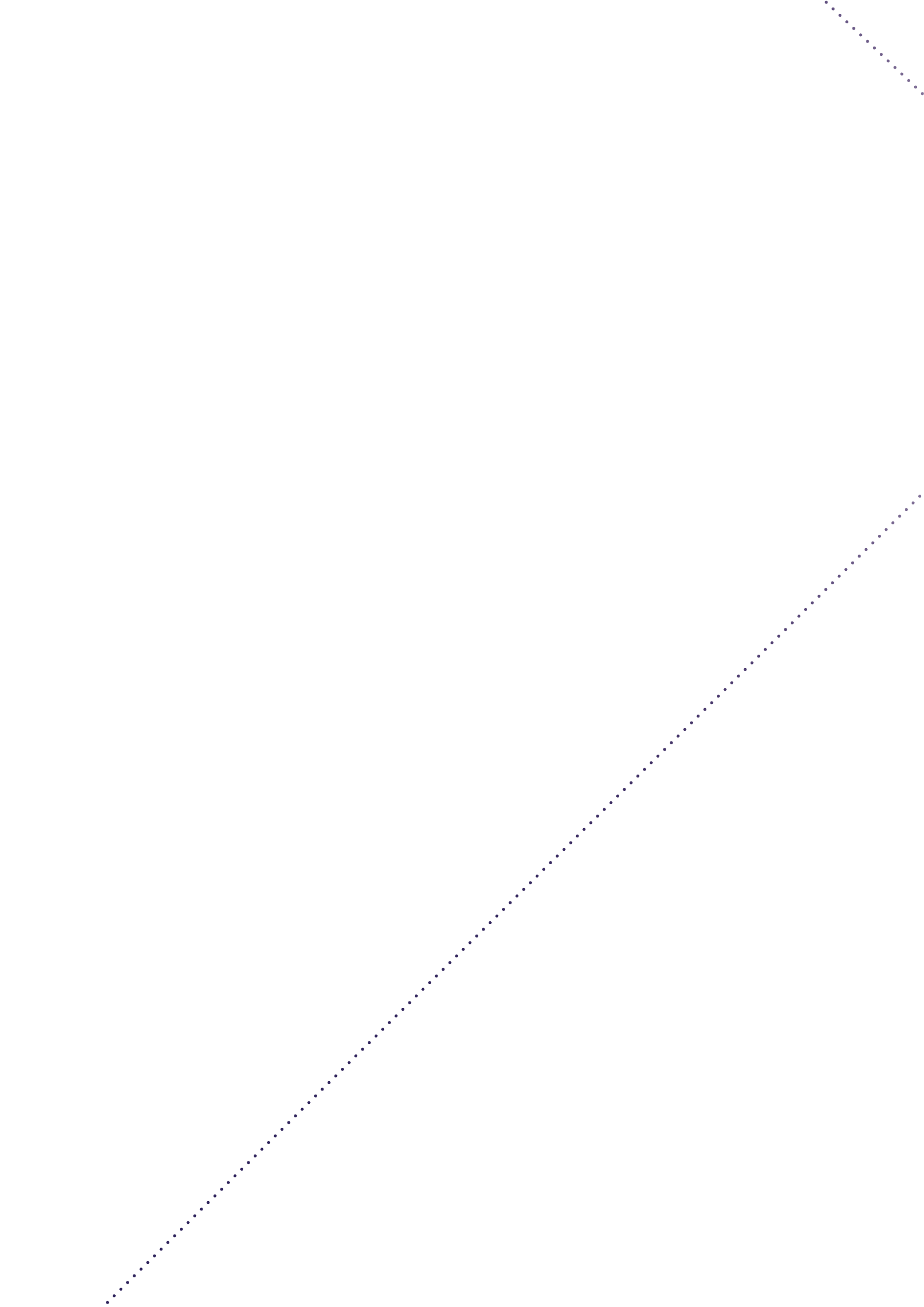
RECOMMANDATIONS

Face à des stratégies hybrides, la cyberdéfense militaire de l'UE ne peut se limiter à des réponses strictement capacitaires ou opérationnelles. Elle doit aussi contribuer plus généralement à la sécurité internationale par la promotion de mesures de confiance, en participant aux discussions sur l'applicabilité du droit international au cyberespace et en accélérant les synergies avec le secteur privé.

L'UE doit tout de même se renforcer sur le plan militaire, en coopérant davantage avec l'OTAN pour éviter les chevauchements d'activités grâce aux deux actions suivantes :

› Développer le partage de bonnes pratiques entre l'UE et l'OTAN dans le cadre d'opérations conjointes. Le théâtre le plus opportun à cet égard est la Méditerranée où les deux organisations sont actives.

› Assurer une complémentarité effective entre la clause de défense mutuelle des États membres de l'UE (article 42.7 du TUE) et celle de l'OTAN (article 5 du traité de l'Alliance) en cas de cyberattaque majeure.



LUTTE
ANTI-CYBERCRIMINALITÉ

La cybercriminalité est la *« criminalité du XXIème siècle*[29] *»*. Elle connaît depuis la crise Covid-19 une croissance exponentielle qui devrait se poursuivre dans les années à venir. La migration des délinquants vers le cyberespace s'accompagne de celle des États et d'organismes para-étatiques qui le pénètrent pour mener des actions situées en dessous du seuil de conflit armé. Celles-ci n'entrent pas dans le cadre juridique du droit des conflits armés, mais se distinguent de la cyber-délinquance classique par leur ampleur ou la nature des cibles visées. Les États-Unis viennent de hisser les rançongiciels au niveau du terrorisme, soulignant ainsi le niveau de gravité de certaines cyber-infractions. Sans remettre en cause la souveraineté nationale qui se manifeste en matière de défense et de sécurité, la lutte contre ces infractions appelle une coopération accrue entre les États membres, un renforcement des capacités nationales et européennes, ainsi qu'une législation commune qui favorise la recherche et l'obtention de la preuve numérique.

29. Thème du FIC 2007.

10 RENFORCER LES **CAPACITÉS DE LUTTE** CONTRE LA CYBERCRIMINALITÉ

CONSTAT La lutte contre la cybercriminalité a trop souvent été négligée, parfois sous prétexte de difficultés liées au caractère transfrontalier des infractions commises depuis des États *« cyber-voyous »*. Or des exemples récents (Avalanche, VPN Safe-Inet, Encrochat, etc.) démontrent que la coopération européenne peut être efficace, quand elle n'est pas nécessaire (avec le concours du FBI et d'autres polices étrangères).

OBJECTIF Renforcer les capacités de lutte contre la cybercriminalité de l'UE et de ses États membres, en faisant en sorte que chacun consente à des efforts en matière d'organisation, d'effectifs et de moyens.

RECOMMANDATIONS

Plusieurs pistes concrètes permettraient de densifier la lutte anti-cybercriminalité :

› Créer un Parquet européen spécialisé dans la cybercriminalité, à l'instar du parquet financier, pour lutter contre les cyberattaques visant les institutions de l'UE. Ce parquet doit acquérir des compétences dans le traitement et l'application de peines en matière de cybersécurité, sans toutefois empiéter sur les compétences qui relèvent du droit national[30]

› Mettre en place une plateforme commune de *cyber threat intelligence* à laquelle les forces de l'ordre des États membres auront un accès direct, simple et sécurisé. Un tel outil, qui vise à fluidifier l'échange rapide d'information, devra être ergonomique et accessible en plusieurs langues. Des formations pourront être mises en place pour apprendre aux différents services concernés à l'utiliser efficacement.

› Développer dans le cadre d'Europol (EC3) les capacités d'investigation forensique, pour une meilleure maîtrise notamment du *darknet* et des cryptoactifs, et faciliter l'imputation judiciaire des infractions.

30. Commission supérieure du numérique et des postes, *Recommandations dans le domaine de la sécurité numérique,* Avis n°2021-03, Recommandation n°4, 29 avril 2021.

› Favoriser la création d'un réseau européen de compétences pour améliorer les coopérations et synergies :

- en développant, au sein du Collège européen de police (CEPOL), des formations communes aux forces de l'ordre, aux CSIRTs et aux magistrats, en matière de lutte contre la cybercriminalité.
- en créant un e-Erasmus entre les écoles de formation des cyber-enquêteurs.
- en instituant une réserve européenne pouvant être sollicitée par un ou plusieurs États membres afin de renforcer les équipes (communes) d'enquête.
- en identifiant clairement la lutte contre la cybercriminalité dans les missions du futur centre de cybersécurité de Bucarest et de l'unité conjointe de cybersécurité.
- en institutionnalisant des coopérations opérationnelles entre États frontaliers en organisant des CCPD adaptés à la lutte contre la cybercriminalité.

› Rapprocher les acteurs de la cyberdéfense et de la lutte contre la cybercriminalité, selon les finalités de chacun, afin de faciliter, dans le respect de la souveraineté des États membres, l'échange du renseignement d'origine cyber et du renseignement d'intérêt cyber.

› Développer le partenariat public/privé, notamment pour améliorer la connaissance des phénomènes cybercriminels, les offreurs de sécurité et les assureurs ayant notamment une connaissance instantanée des cyberattaques utile à la réduction d'un chiffre noir qui pèse sur l'orientation des politiques publiques. Ce partenariat doit aussi être conçu dans un cadre plus opérationnel (notification des cyber-infractions, conservation de preuves, aide à l'analyse forensique).

› Instituer davantage les possibilités de détachements au sein des États membres pour les forces de l'ordre, ainsi que pour les CSIRTs nationaux et gouvernementaux.

11 PARVENIR À UNE **SOLUTION ÉQUILIBRÉE** SUR LA **CONSERVATION DES PREUVES**

CONSTAT Selon l'UE, 85% des preuves pénales sont numériques et plus de la moitié d'entre elles sont hébergées sur un territoire distinct du lieu de l'infraction. Il importe donc de pouvoir y accéder dans des conditions juridiques stables qui concilient les nécessités de l'enquête et le respect de la vie privée. Ces preuves doivent pouvoir être conservées pendant un temps suffisant, être accessibles rapidement sans porter atteinte à la souveraineté des États, y compris lorsque les requêtes viennent de pays non-européens.

En France, la jurisprudence de la Cour de justice de l'UE (CJUE) a été interprétée par le Conseil d'État de manière diamétralement opposée à la Cour constitutionnelle belge. Il importe que les États membres partagent une même législation. L'arrêt de la CJUE du 6 octobre 2020 s'est appuyé sur des textes conçus dans le cadre du Marché unique et pour le Marché unique. L'immixtion dans le domaine de la défense et de la sécurité nationale, relevant de la souveraineté des États membres, relève d'une approche fédéraliste qui ne fait pas consensus. Sous prétexte d'éviter une surveillance générale des contenus, la jurisprudence délaisse la victime pour laquelle les chances de remonter jusqu'à son prédateur sont désormais limitées.

OBJECTIF Se doter de mécanismes de collecte de preuves numériques, la criminalité et la délinquance étant désormais indissociables de l'espace numérique qu'elles visent ou par lequel elles transitent.

RECOMMANDATIONS

- Finaliser les travaux législatifs relatifs au règlement *« e-evidence »,* en favorisant le transfert rapide des données nécessaires à l'établissement des preuves numériques, dans le respect des prérogatives de l'autorité judiciaire et des principes fondamentaux liés aux données à caractère personnel.
- Profiter des conditions plus favorables de dialogue transatlantique pour faire avancer les négociations engagées en septembre 2019 entre l'UE et les États-Unis, afin de régler les difficultés liées aux transferts de données en matière pénale (contrariétés entre d'une part, le *CLOUD Act*, et d'autre part, le RGPD et la directive *« police-justice »*).
- Élaborer une législation européenne qui garantisse une séparation nette entre l'hébergeur des données, qui doit les conserver en toute *« cybersécurité »*, et le service demandeur, dont les réquisitions doivent être validées par un juge ou une autorité indépendante, comme le souhaite la CJUE.

DONNER UNE **NOUVELLE IMPULSION** À LA **CONVENTION DE BUDAPEST**

12

CONSTAT La Convention de Budapest est le seul texte international contraignant en matière de lutte contre la cybercriminalité. Ratifiée aujourd'hui par soixante-sept États, dont certains ne sont pas membres du Conseil de l'Europe mais sont signataires de la convention africaine de Malabo (2014), elle inspire près de 150 législations étrangères au total. La Convention de Budapest s'appuie sur des valeurs qui ne sauraient être remises en cause par un traité moins-disant que certains États souhaitent porter aux Nations Unies. Au moment où elle fête ses vingt ans, un nouveau protocole additionnel est en cours de finalisation.

OBJECTIF S'inscrire dans la dynamique de la mise en œuvre de son deuxième protocole additionnel pour faire de la Convention de Budapest l'instrument prépondérant dans la coopération transfrontière.

RECOMMANDATIONS

- Promouvoir sa ratification par des États non-membres du Conseil de l'Europe à l'aide de la cyberdiplomatie[31].
- Mettre en œuvre les recommandations de manière pragmatique, sans chercher systématiquement l'unanimité, par des accords bilatéraux (transfrontaliers en particulier), en partant du principe que l'exemple peut conduire à la généralisation.
- Poursuivre les travaux d'adaptation de la Convention de Budapest postérieurs au nouveau protocole additionnel, en recherchant *« l'interopérabilité »* des investigations numériques.

31. cf. recommandation n°4 « Promouvoir une vision européenne du droit international du cyberespace »

13 RENFORCER LA **LUTTE** CONTRE LES **CONTENUS ILLICITES**

CONSTAT Un contenu est considéré *« illicite »* lorsqu'il n'est pas en conformité avec le droit de l'UE ou celui des États membres. Selon les directives européennes, cette désignation couvre les publications faisant l'apologie du terrorisme, celles à caractère pédopornographique, les discours de haine, les escroqueries, et les atteintes aux droits de la propriété intellectuelle telles que le piratage audiovisuel. À l'ère numérique, ces contenus sont essentiellement produits et relayés à partir de plateformes d'intermédiation (réseaux sociaux, blogs, *marketplaces*, etc.), créées et opérées par des acteurs privés tels que Google, Facebook et Baidu.

En Europe, la directive e-commerce (2000) a délimité les responsabilités des fournisseurs de service en ligne, selon une distinction entre *« éditeurs »* et *« hébergeurs »*. Si les premiers sont responsables de toutes les publications sur leurs sites, les seconds le deviennent dès lors qu'ils sont notifiés de l'existence sur leurs serveurs d'un contenu illicite, qu'ils doivent retirer *« promptement »*. Les services d'intermédiation, qui ne comptaient que des milliers d'utilisateurs contre des millions désormais, ont alors été associés au régime des hébergeurs. Dans les premières heures d'Internet, les législateurs n'ont pu en effet prévoir ni le détournement à des fins illicites, ni la dimension *« systémique »* de certaines plateformes aujourd'hui.

Une telle réglementation favorise la diffusion de contenus illicites et les plateformes – surtout les plus importantes – ne sont pas suffisamment impliquées pour limiter ce phénomène. Une situation d'autant plus préoccupante eu égard aux manipulations de l'information qui se développent. En effet, une *fake news* se propagerait à une vitesse six fois plus élevée qu'une *« vraie »* information sur les réseaux sociaux[32].

Pour contrer cette dynamique, vecteur de menaces aussi bien pour la sécurité des usagers que pour la pérennité des démocraties, la Commission européenne a présenté en décembre 2020 le *Digital Services Act* (DSA). Thierry Breton en a précisé le fil conducteur[33] : *« ce qui est interdit offline doit l'être online »* et *« tous les contenus illégaux doivent être retirés »*. Le DSA vise ainsi à imposer de nouvelles obligations aux plateformes, parmi lesquelles la mise en place d'un mécanisme de signalement des contenus illicites (déjà en vigueur dans certains États membres), et d'un système interne de traitement des plaintes des usagers.

32. Peter Dizikes, « Study: On Twitter, false news travels faster than true stories », *MIT News*, 8 mars 2018.

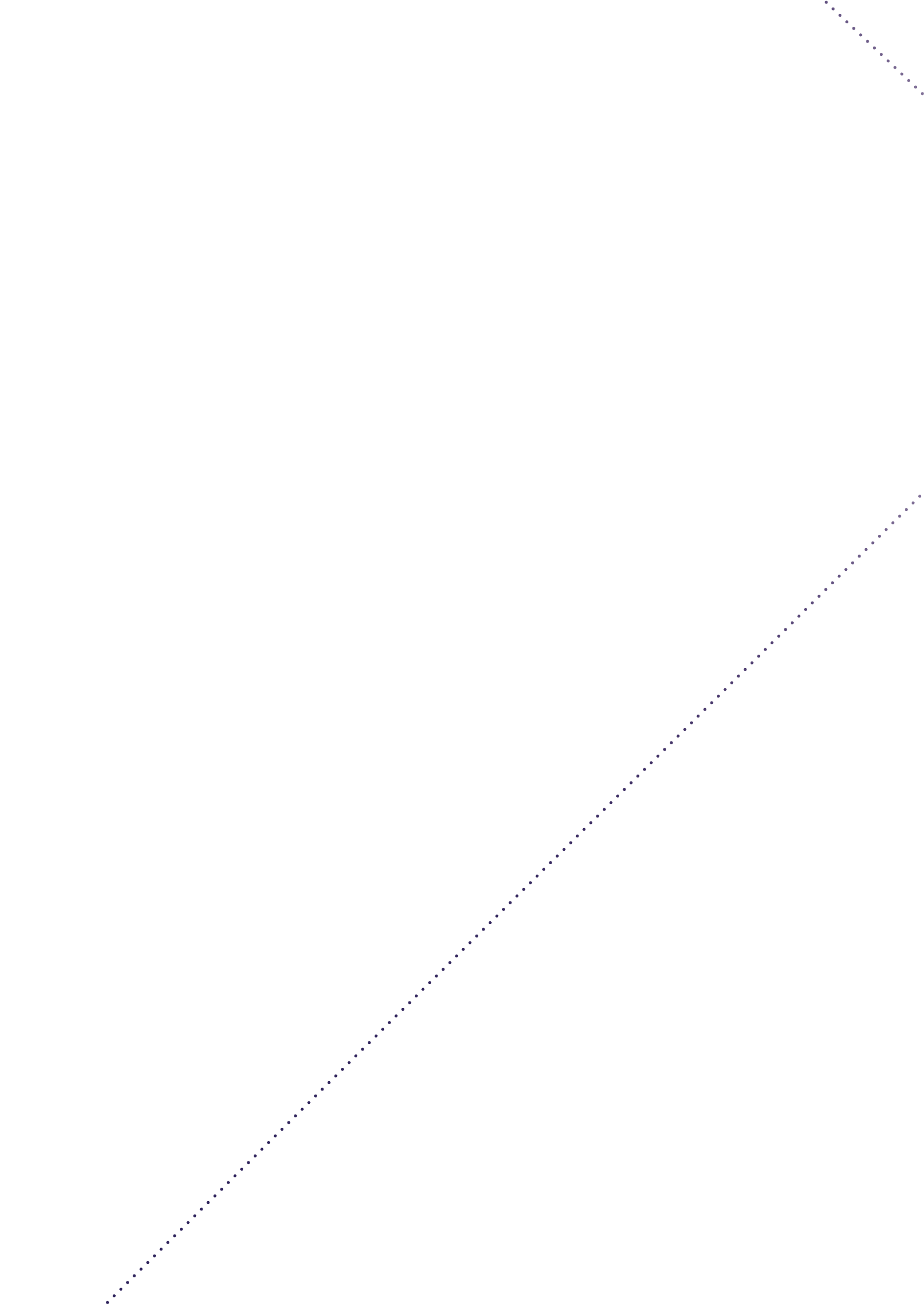
33. Virginie Malingre, « Thierry Breton : "Dans bien des cas, l'espace numérique est une zone de non-droit" », *Le Monde*, 22 octobre 2020.

Quant aux très grandes plateformes, elles relèveront d'une catégorie *ad hoc* intitulée les *« contrôleurs d'accès »* (*gatekeepers*), entendu comme ceux suffisamment structurants pour contrôler l'accès à un marché donné. Ces opérateurs devront entre autres évaluer et réduire les risques systémiques liés au fonctionnement et à l'utilisation de leurs services, réaliser des audits externes de leur niveau de conformité, et communiquer les paramètres utilisés dans leurs systèmes de recommandation de contenus.

OBJECTIF Associer tous les États membres à la finalisation du texte *Digital Services Act* (DSA) pour une adoption accélérée.

RECOMMANDATIONS

- Mettre en place une *« base de signatures »* de contenus illicites dans tous les États membres.
- Agréger ces bases de données à l'échelle européenne.
- Renforcer l'innovation en intelligence artificielle, qui devra toujours être au service de l'Humain, pour faciliter la détection et le retrait des contenus illicites.



CYBERSÉCURITÉ & RÉSILIENCE

Le renforcement du niveau de cybersécurité et de résilience collectif des infrastructures numériques européennes est un impératif opérationnel. Cette exigence, qui est au coeur de la nouvelle stratégie de cybersécurité de l'UE, devra se traduire à la fois par :

- L'adoption d'un cadre juridique et normatif encore plus volontariste pour améliorer la sécurité des infrastructures critiques (projet de directive NIS 2), et pour imposer une sécurité *« by design »* et *« par défaut »* aux éditeurs logiciels et aux fabricants d'équipements ;
- Le renforcement des capacités des institutions européennes, tant pour répondre à leurs propres besoins que pour développer une capacité de réaction aux incidents majeurs, qui viendra compléter les capacités de chacun des États membres et non s'y substituer.

14 IMPOSER **LA SÉCURITÉ** ***« BY DESIGN »***

CONSTAT Plus des trois quarts des applications logicielles comportent des failles de sécurité, dont un quart seraient d'un niveau de gravité élevé[34]. Et le nombre de vulnérabilités va croître de façon exponentielle avec l'explosion des objets connectés. Ces derniers ont souvent un niveau de sécurité très faible pour différentes raisons telles que les exigences du *« time to market »*, le marché global, le manque de compétences en sécurité, la complexité de la chaîne de valeur, l'absence de normes et des responsabilités peu établies. Les infrastructures de *cloud computing* ne sont pas en reste si l'on en croit les vulnérabilités régulièrement identifiées sur les grandes plateformes.

OBJECTIF Il ne s'agit plus seulement de certifier la fiabilité des équipements de sécurité mais bien de garantir la sécurité des produits et des services numériques ou intégrant du numérique, que l'on soit dans le monde des technologies de l'information génériques ou des technologies opérationnelles (OT) et systèmes cyber-physiques, où sécurité et sûreté sont intimement liées.

RECOMMANDATIONS

- Accélérer la mise en place de schémas européens de certification selon le cadre juridique adopté dans le *Cybersecurity Act*.
- Proposer des mesures législatives pour améliorer la cybersécurité dans tous les produits numériques, y compris les logiciels mis sur le marché intérieur. En juin 2021, le Parlement européen a privilégié à cet égard un règlement transversal suffisamment exigeant pour *« les applications, les logiciels, les logiciels intégrés et les systèmes d'exploitation d'ici à 2023*[35] *».*
- Faire adopter au niveau international le principe de responsabilité des éditeurs et fabricants, en particulier ceux systémiques, dans la conception et la maintenance de leurs produits.

34. Veracode, « State of Software Security v11 », juin 2021.

35. Parlement européen, *Stratégie de cybersécurité de l'Union pour la décennie numérique,* 10 juin 2021, p. 5.

Les engagements volontaires, comme le *Charter of Trust* de 2018, sont des initiatives positives mais ne suffisent pas. L'OCDE[36] et le CIGREF[37] constatent de part et d'autre la tendance chez beaucoup de fournisseurs à faire peser les responsabilités aux utilisateurs finaux, alors que ces derniers ne sont pas les plus à même de gérer la sécurité du risque associé aux produits.

› Ériger la *« sécurité par défaut »* en principe. Les applications doivent intégrer d'emblée le meilleur niveau de protection des données personnelles et de sécurité, sans que l'utilisateur n'ait à choisir d'options.

› Imposer aux éditeurs et fabricants un maintien en conditions de sécurité, à travers des mises à jour régulières, pour appréhender l'obsolescence des *« parcs installés »*. Cet objectif implique d'étendre aux entreprises les dispositions des directives européennes de 2019[38], relatives à la protection du consommateur, qui obligent les vendeurs à fournir des correctifs aux consommateurs finaux de services numériques. Cet engagement devrait courir après la fin de la commercialisation, les équipements étant souvent utilisés alors qu'ils ne sont plus vendus[39]. Le Parlement européen a aussi recommandé aux fabricants de communiquer en avance la période minimale durant laquelle ils fourniront des correctifs et des mises à jour pour que les consommateurs puissent choisir en connaissance de cause[40].

36. OCDE, « Enhancing the digital security of products: A policy discussion », *Digital Economy Papers*, N°306, 2021.
37. Courrier du 13 novembre adressé au Premier ministre de la République française.
38. Directives 2019/770/UE et 2018/771/UE du 20 mai 2019.
39. Sébastien Meurant, Rémi Cardon, « La cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ? », *Rapport d'information*, n° 678, Sénat, 10 juin 2021.
40. *Op. cit. Stratégie de cybersécurité de l'Union pour la décennie numérique,* 10 juin 2021, p. 5.

15 DÉVELOPPER UNE **CAPACITÉ EUROPÉENNE** DE RÉACTION AUX **INCIDENTS MAJEURS**

CONSTAT La plupart des pays européens ne disposent pas des capacités techniques permettant de détecter à temps et de réagir à des incidents majeurs. Or il n'existe à ce jour pas de procédure d'assistance et de structure de réaction commune susceptible d'apporter une réponse opérationnelle, mais aussi politique et diplomatique, en cas d'attaque affectant un ou plusieurs États membres. Comme le souligne Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en France, l'Union européenne (UE) doit pouvoir à son échelle *« rechercher une attribution collective »* pour se prononcer sur les actions adverses *« inadmissibles*[41] *»*.

La stratégie européenne de cybersécurité a proposé la construction d'un réseau de Security Operations Centers (SOC) au sein de l'UE. L'enjeu serait dès lors d'en mettre en réseau le plus possible afin de créer une connaissance collective, ainsi que partager des outils et les meilleures pratiques.

En juin 2021, une étape importante a été franchie avec la proposition de la Commission européenne de créer une nouvelle unité conjointe de cybersécurité[42, 43], installée à Bruxelles non loin du CERT-EU. Cette unité a vocation à assurer une réaction coordonnée face aux incidents de cybersécurité les plus graves.

OBJECTIF Veiller à la bonne articulation du dispositif européen de réaction autour des trois niveaux suivants :

- Les capacités internes des États membres. Celles-ci sont indispensables car la cybersécurité doit avant tout se traiter au plus près du terrain. Toute velléité de développer un *« parapluie »* cyber grâce auquel quelques grands États assureraient la protection des plus petits se heurterait par ailleurs à des préoccupations – légitimes – de souveraineté.

41. « Audition, à huis clos, de M. Guillaume Poupard, directeur général de l'Agence nationale de sécurité des systèmes d'information sur l'actualisation de la LPM 2019-2025 », *Assemblée nationale*, 8 juin 2021.

42. « La Commission propose la création d'une unité conjointe de cybersécurité afin d'intensifier la réaction aux incidents majeurs de sécurité », *Commission européenne*, 23 juin 2021.

43. « Joint Cyber Unit », *Commission européenne,* 23 juin 2021.

- La mise en réseau de ces capacités disponibles dans toutes les communautés de cybersécurité, y compris les forces de l'ordre, les armées et les services diplomatiques. Un réseau d'échange baptisé Cyclone (*Cyber Crisis Liaison Organisation Network*) a ainsi été mis en place par la Commission et l'ENISA en 2020. Ce réseau doit interagir de manière appropriée avec le réseau préexistant des équipes de réponse aux incidents de sécurité informatique (CSIRT).
- Une capacité commune. L'unité conjointe de cybersécurité mutualisera dès lors des moyens publics ou privés à la demande d'une nation européenne au titre de la solidarité entre les États membres. L'échange d'informations entre les SOC améliorera considérablement les capacités de détection des États membres.

RECOMMANDATIONS

› Finaliser la mise en place du dispositif le 30 juin 2023 et le rendre opérationnel d'ici le 30 juin 2022.

› S'inspirer de l'*European Civil Protection Pool* qui est le dispositif existant en matière de sécurité civile[44]. Cette plateforme fonctionne grâce à des capacités standardisées proposées par les États membres et validées par la Commission européenne. Vingt-cinq nations participantes ont proposé à ce jour près de 110 capacités, dont 77 ont été certifiées. Ces dernières sont donc déployables à tout moment, à l'intérieur et à l'extérieur de l'UE, sur demande d'un État membre auprès d'un centre de coordination, le Emergency Response Coordination Center (ERCC)[45]. Le mécanisme a été utilisé 102 fois en 2020.

44. « European Civil Protection Pool », *Commission européenne,* 28 mai 2021.

45. « Emergency Response Coordination Centre », *Commission européenne,* 28 mai 2021.

16 RENFORCER LA **PROTECTION DES SYSTÈMES D'INFORMATIONS** DE L'UE

CONSTAT L'Union européenne doit aider les vingt-sept États membres à élever leur niveau de cybersécurité. Elle doit également assurer la sécurité de ses propres systèmes d'information, qui seront d'autant plus ciblés que l'Europe cherchera à jouer un rôle de leader dans l'espace numérique.

Selon le directeur général de l'ANSSI, les institutions européennes sont en termes de cybersécurité elles-mêmes un point faible, car elles sont des cibles évidentes, surtout en matière d'espionnage, du fait de la puissance économique et diplomatique de l'UE. La protection des systèmes d'information et de communication de l'UE n'est ainsi pas une option : toute faiblesse porterait atteinte à la crédibilité de l'action européenne à l'égard des vingt-sept États membres.

OBJECTIF Renforcer les capacités opérationnelles des institutions européennes et sensibiliser l'ensemble des fonctionnaires européens à la cybersécurité.

RECOMMANDATIONS

- Renforcer les capacités du CERT-UE, en liaison avec l'ENISA, et de l'ensemble du réseau des CERT des États membres.
- Mettre en place un cursus dédié à la cybersécurité dans le tronc commun de formation des futurs dirigeants européens, notamment au Collège d'Europe.
- Créer une qualification obligatoire *« Sécurité numérique et cybersécurité »*, délivrée par l'ENISA, lors de la prise de fonction des fonctionnaires de l'UE. Si les premiers niveaux peuvent être réalisés via des MOOC, les derniers qui visent les hauts fonctionnaires seront à valider en formation présentielle.

RENFORCER LA **PROTECTION** DES **INFRASTRUCTURES CRITIQUES**

17

CONSTAT Adoptée en 2016, la directive NIS visait à garantir un niveau élevé de sécurité des opérateurs d'infrastructures critiques au sein de l'UE. Pour autant, sa mise en œuvre par les États membres a été hétérogène, entraînant des incohérences et des différences de niveaux dans la gestion du risque cyber. De plus, la transformation numérique, accélérée par la crise Covid-19, a densifié le paysage des menaces pour les États et les entreprises, auxquels il convient d'apporter des réponses adaptées et innovantes[46].

La Commission européenne a ainsi relevé, outre le niveau insuffisant de résilience des entreprises actives dans l'UE, plusieurs limites à la directive NIS[47]. Celle-ci ne permet en effet plus d'appréhender efficacement l'augmentation de la surface d'exposition aux cyberattaques. Pour répondre à ces constats, l'institution a présenté en décembre 2020 une proposition de révision (*« directive NIS 2 »*), qui n'est pour le moment qu'au début du processus législatif, puisqu'elle doit encore être approuvée par le Parlement et le Conseil.

Le projet de directive NIS 2 a vocation à couvrir davantage de secteurs (santé, transport, banques, énergie, espace, industrie pharmaceutique, agro-alimentaire...) et ce, notamment dans le numérique (infrastructures, médias sociaux, data centers...). Il propose ainsi de redéfinir les opérateurs de services essentiels en *« entités essentielles[48] »*, ainsi que les fournisseurs de services numériques (FSN) en *« entités importantes[49] »*.

En d'autres termes, les opérateurs d'infrastructures critiques seront soumis à de nouvelles obligations, visant à garantir la résilience de leurs réseaux et systèmes d'information. Ils devront dès lors adopter toutes les mesures techniques et organisationnelles appropriées pour gérer le risque cyber, y compris celui lié à la chaîne d'approvisionnement, en sécurisant leurs relations avec les fournisseurs et prestataires de services. Ils signaleront aussi aux autorités nationales, outre les cyber-incidents, les failles informatiques qu'ils auront eux-mêmes identifiées dans le cadre d'un programme coordonné de divulgation des vulnérabilités (CVD).

46. « Proposal for directive on measures for high common level of cybersecurity across the Union », *Commission européenne,* 16 décembre 2020.

47. « Joint communication to the European Parliament and the Council – The EU's Cybersecurity Strategy for the Digital Decade », *Commission européenne,* 16 décembre 2020.

48. Actuels opérateurs de services essentiels et sociétés relevant de nouveaux secteurs tels que l'agro-alimentaire, la R&D pharmaceutique, les fabricants de dispositifs médicaux et les services d'infrastructure numérique (*cloud computing*, services DNS...).

49. Les services postaux, les entreprises de gestion des déchets et les fournisseurs de services numériques (marchés en ligne, moteurs de recherche et réseaux sociaux).

Les États membres gagneront en pouvoirs de contrôle réglementaire et de sanctions. Ils pourront en effet suspendre la licence ou l'autorisation des activités d'une entité, en cas de manquements répétés.

OBJECTIF Finaliser le projet de directive NIS 2, en y intégrant toute la chaîne d'approvisionnement des produits numériques, et accélérer son adoption par les institutions européennes.

RECOMMANDATIONS

Les mesures suivantes permettraient de développer la robustesse de la directive NIS 2 :

- Doter les autorités nationales compétentes en cybersécurité d'un pouvoir d'injonction. Sur le modèle des États-Unis, les pays européens doivent pouvoir imposer aux entités relevant de leurs territoires des mesures correctives, dès lors qu'une faille aura été détectée dans leurs systèmes d'information. Les victimes auront 48 heures pour apporter les correctifs sous peine de sanctions. En effet, la plupart ne mesurent pas la gravité des messages d'alerte envoyés par ces autorités nationales[50].
- Imposer une fréquence minimale d'un an pour la réalisation, par les autorités nationales compétentes, d'audits de sécurité des réseaux et systèmes d'information des opérateurs d'infrastructures critiques.
- Intégrer les éditeurs de logiciels et les fabricants de matériels au programme coordonné de divulgation des vulnérabilités (CVD).
- Renforcer les obligations des fournisseurs de services numériques (FSN). Une attaque contre ces entreprises a des effets systémiques car elle ouvre aux assaillants un accès direct potentiel à tous leurs clients. Un volet « *cybersécurité* » pourrait ainsi être ainsi rendu obligatoire dans les réponses aux appels d'offres des FSN. Aussi longtemps que ce volet sera facultatif, les entreprises les moins disantes, qui n'incluent pas le coût associé, gagneront les contrats et seront vecteurs de risques[51].

50. « Audition, à huis clos, de M. Guillaume Poupard, directeur général de l'Agence nationale de sécurité des systèmes d'information sur l'actualisation de la LPM 2019-2025 », *Assemblée nationale*, 8 juin 2021.

51. *Ibid.*

ENCOURAGER LES **POLITIQUES** DE **DIVULGATION COORDONNÉE**

18

CONSTAT Les politiques de divulgation coordonnée de vulnérabilités permettent d'encadrer la découverte de vulnérabilités par des personnes extérieures aux organisations concernées. Elles proposent un cadre opérationnel clair qui protège aussi bien les personnes de bonne foi, soucieuses d'apporter rapidement des correctifs, que les organisations qui ont parfois besoin de temps pour développer et déployer les correctifs.

Or malgré leur intérêt, ces politiques sont peu nombreuses en France et plus largement au sein de l'UE. La situation est d'autant plus préoccupante que les vulnérabilités sont de moins en moins présentes dans le code. Elles se trouvent en effet essentiellement dans les configurations ou implémentations liées à l'utilisation de *frameworks* de développement et à la superposition de couches logicielles (*cloud computing*).

À la suite des attaques récentes contre SolarWinds et Colonial Pipeline, le Président américain a signé un décret exécutif imposant aux fournisseurs fédéraux de nouvelles obligations en matière de cybersécurité, en particulier la mise en place de programmes de divulgation coordonnée (*Vulnerability Disclosure Program*). La transformation numérique de toutes les activités augmente l'exposition potentielle à tout type de vulnérabilités. Certaines deviennent dès lors systémiques en raison de la faible diversité de solutions.

OBJECTIF Rendre obligatoires les politiques de divulgation coordonnée, en particulier pour la chaîne d'approvisionnement numérique dont les vulnérabilités ont le plus souvent des effets systémiques. Les opérateurs d'importance vitale, y compris ceux d'infrastructures critiques, doivent rapidement se saisir de l'opportunité de maîtrise des risques cyber associée à ce type de politique. Enfin, l'achat public doit montrer l'exemple en introduisant l'exigence de ces politiques de la part des fournisseurs actuels et futurs.

RECOMMANDATIONS

En cours d'élaboration, la *« directive NIS 2 »* ne peut se contenter de recommander la mise en place de programmes de divulgation coordonnée[52]. Elle devrait ainsi :

- Imposer, dans la mesure du possible, ces programmes aux entités *« essentielles »* et *« importantes »*, dont feront partie les fournisseurs de services numériques et certaines administrations publiques. Ces mesures doivent être vues comme une opportunité *« business »* permettant de restaurer une confiance mise à mal par les nombreuses attaques par rebond ces derniers mois.
- Ajouter un volet *« proactif »* encourageant la recherche de vulnérabilités dans un cadre structuré et éthique grâce à la mise en place de *« bug bounty »* au sein des organisations, la politique de divulgation coordonnée étant une approche passive.
- Créer un registre européen des vulnérabilités confié à l'ENISA, recensant les vulnérabilités signalées sur le périmètre de la directive NIS 2. Un tel instrument sera utile, tant pour améliorer la transparence du processus que pour la passation de marchés européens pour les entités adjudicatrices.

52. cf. recommandation n°17 « Renforcer la protection des infrastructures critiques »

AMÉLIORER LA **CYBERSÉCURITÉ TRANSFRONTALIÈRE**

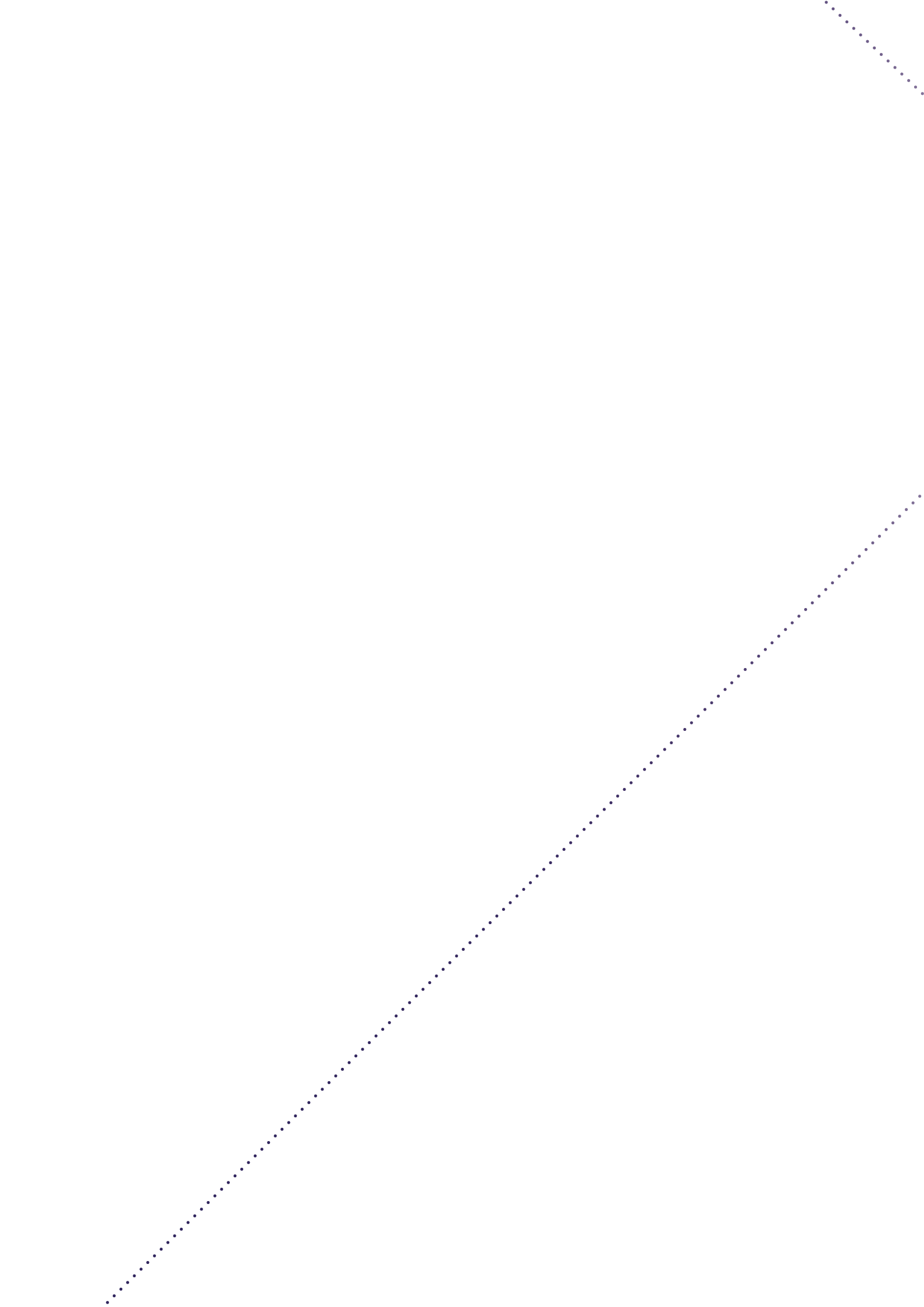
19

CONSTAT Les frontières internes de l'Union sont de plus en plus poreuses, tant les activités économiques se déploient selon des logiques de bassin, dominées par la proximité et les infrastructures. De ce fait, la cybersécurité d'un État ne s'arrête pas là où commence celle des autres, plus particulièrement des États frontaliers. Il convient donc, dans le respect de la souveraineté de chaque État membre, de renforcer la coopération opérationnelle transfrontalière. À l'instar des Centres de coopération policière et douanière (CCPD), dont le rôle en matière de lutte contre la cybercriminalité transfrontalière pourrait être davantage marqué, il convient d'imaginer des centres communs de partage de l'information.

OBJECTIF Créer à titre expérimental des CERT transfrontaliers, soit généralistes, soit sectoriels (énergie par exemple). Cette mesure reposant sur le volontariat des États membres pourrait faire l'objet d'une généralisation en cas de succès.

RECOMMANDATIONS

› Expérimenter dans un premier temps une entité transfrontalière qui travaillerait en liaison avec les CERT nationaux ou régionaux (en cours de développement en France), avec le CERT-UE et les forces concourant à la lutte contre la cybercriminalité.



POLITIQUE INDUSTRIELLE

L'Europe s'est pendant longtemps refusée à toute véritable politique industrielle pour privilégier l'intégration de son marché intérieur en travaillant sur l'offre (politique de la concurrence) et la demande (politique commerciale)[53]. La nouvelle politique industrielle en cours d'élaboration sous l'impulsion de Thierry Breton, commissaire en charge du marché intérieur, marque ainsi un tournant. Elle bénéficie de circonstances *a priori* favorables : au plan sociétal, la crise Covid-19 a révélé les dépendances industrielles de l'Europe et a entraîné une prise de conscience ; au plan économique, les États-Unis et la Chine ont adopté des politiques industrielles volontaristes, pour ne pas dire agressives, qui font de l'Europe leur *« terrain de jeu »* ; au plan politique, les concepts d'autonomie stratégique ou de souveraineté technologique émergent enfin du brouillard où ils étaient cantonnés depuis des années. Mieux, les traditionnels clivages entre les Européens s'estompent : l'Allemagne, qui s'est par exemple longtemps tenue à une stricte application du droit de la concurrence, partage maintenant le besoin de mettre en place une politique industrielle européenne.

53. Patrice Anato, Michel Herbillon, « L'avenir de la politique industrielle européenne », *Rapport d'information*, Assemblée nationale, 25 mars 2021.

20 CRÉER UN **INDICATEUR** DE **TRAÇABILITÉ NUMÉRIQUE**

CONSTAT La confiance des utilisateurs, condition clé de la transformation numérique et de l'adoption de nouveaux usages, est de plus en plus mise à mal par la multiplication des attaques et des fuites de données. Elle l'est d'autant plus en raison de la crainte de voir émerger une société de surveillance généralisée, qui suscite quelques inquiétudes, voire un début de rejet. Les premiers symptômes en sont d'ores et déjà perceptibles avec les technologies biométriques et l'intelligence artificielle. Enfin, la crise Covid-19 a mis en lumière les nombreuses dépendances européennes à des équipements ou à des flux numériques provenant de pays non européens.

Pour résumer, si *« l'usage »* reste le moteur principal de la transformation numérique, le consommateur final prend progressivement conscience de l'impact du numérique sur sa vie personnelle et professionnelle, ainsi que sur la société dans son ensemble. L'exode connu récemment par WhatsApp[54], suite au changement des conditions générales d'utilisation, montre en effet qu'il est de plus en plus réceptif à ces questions.

Pour entretenir et développer la confiance, l'information du consommateur est désormais une priorité. Celui-ci doit pouvoir choisir en connaissance de cause les produits et services numériques embarquant du numérique. L'utilisateur a besoin de transparence, notamment quant à la localisation et au traitement de ses données, à la chaîne de sous-traitants impliqués et aux conditions générales d'utilisation.

Au plan stratégique, ces dépendances doivent être identifiées pour assurer la résilience des activités, grâce à des plans de continuité, et leur réduction ou *a minima* leur équilibre doit reposer sur des politiques industrielles. Dans une économie numérisée et globalisée, ces dépendances ne constituent pas en soi un problème : elles le deviennent lorsqu'elles sont méconnues, imposées, non réversibles ou trop exclusives.

OBJECTIF Rendre les produits et services numériques transparents à l'égard des usagers.

54. « WhatsApp : pourquoi un tel exode des utilisateurs », *Le Monde*, 18 janvier 2021.

RECOMMANDATIONS

- Créer un indicateur de traçabilité numérique, sur le modèle des produits alimentaires, qui prendrait la forme d'un étiquetage établi par un tiers à partir des fournisseurs de chaque organisation.
- Décliner cet indicateur en trois parties : transparence de la chaîne numérique, conformité au règlement général sur la protection des données (RGPD), localisation du stockage et des principaux traitements de données en Europe.
- Favoriser l'intégration de cet indicateur dans la communication des entreprises, tant pour des activités BtoB que BtoC. De façon plus globale, ce dispositif vise à valoriser les entreprises jouant la *« carte européenne »* partout où cela est possible dans le cadre d'une approche *« name and fame »*.
- Rendre le score obligatoire dans le cadre des appels d'offres publics intégrant une dimension numérique grâce à un *« Buy European Digital Act*[55] *»*.
- Rendre la méthodologie pleinement auditable afin d'éviter le syndrome de la *« boîte noire »*, contre lequel cet indicateur de traçabilité cherche justement à lutter.
- Trouver un compromis entre la complexité de certains traitements et la lisibilité nécessaire à tout indicateur et disposer rapidement d'une masse critique pour s'imposer sur le marché.

55. cf. recommandation n°22 « Mobiliser l'achat public et privé ».

21 REDYNAMISER LE **SYSTÈME EUROPÉEN DE NORMALISATION**

CONSTAT Alors que l'Europe possède une longue tradition en matière de normalisation, force est de constater qu'elle a perdu le leadership qu'elle exerçait il y a quelques années en la matière. Or la normalisation est un outil d'influence et de politique industrielle majeur. Comme le souligne Mme Claude Revel, *« la norme/règle internationale est un des points d'application majeurs de l'intelligence économique et stratégique. Il est de plus en plus difficile de séparer le `technique' du politique, les choix techniques étant non seulement souvent issus de la volonté d'ouvrir des marchés ou d'en fermer aux concurrents, mais aussi reflétant des choix politiques voire idéologiques, en tout cas de société de ceux qui les promeuvent*[56] *»*.

La normalisation est en outre essentielle à l'harmonisation et au renforcement du marché intérieur. *Last but not least*, elle contribue à la défense des valeurs européennes. Face à la montée en puissance de la Chine qui a doublé, voire dans certains cas triplé, sa participation dans les groupes de travail internationaux entre 2011 et 2018, et domine aujourd'hui les discussions sur les technologies de reconnaissance faciale, il serait urgent que l'Europe puisse faire entendre sa voix. La normalisation est donc un levier stratégique qui ne doit plus être vu uniquement sous l'angle de l'interopérabilité et de l'intégration du marché intérieur.

OBJECTIF Accompagner la feuille de route industrielle de la Commission européenne en redynamisant le système de normalisation. Les organismes européens CEN, CENELEC et ETSI doivent disposer de davantage de moyens pour leurs travaux sur les enjeux numériques[57] et développer leur rayonnement international. Une présence renforcée dans les comités internationaux (ISO et IEC) est ainsi indispensable.

L'amélioration doit aussi être qualitative : pour s'adapter à la vitesse du progrès technologique et des nouveaux usages, les standards doivent être plus agiles et *« market responsive »*. Devenu trop complexe, le système de normalisation doit être simplifié et modernisé, comme le note le rapport *« Calling the shots »* élaboré par une commission présidée par l'ancien Premier ministre suédois Carl Bildt. Ces efforts doivent enfin s'inscrire dans le long terme, ne produisant des effets visibles qu'au bout de plusieurs années.

56. Claude Revel, *Développer une influence normative internationale stratégique pour la France,* 31 janvier 2013.

57. Seuls 20% des standards dits « harmonisés » proviennent aujourd'hui des institutions de normalisation, les autres étant issus du monde industriel.

RECOMMANDATIONS

› Décliner le cadre européen de certification institué par le *Cybersecurity Act* pour les équipements et les services numériques en plusieurs schémas de certification. La Commission pourrait inscrire, dans son prochain *« rolling plan »* annuel en matière de normalisation, le développement des schémas concernant l'Internet des objets (en cours d'élaboration), le *cloud computing* (document en consultation), les systèmes industriels, l'intelligence artificielle et les équipements de cybersécurité.

› Créer une certification des équipements de sécurité valable à l'échelle de l'UE pour décloisonner le marché intérieur et permettre aux industriels européens du domaine de diffuser leurs solutions et services sur l'ensemble du continent. Il est en outre nécessaire que toute réglementation européenne intégrant des sujets de confiance numérique, quel que soit le secteur visé, s'appuie sur le *Cybersecurity Act* pour les spécifications techniques de sécurité, afin d'éviter que chaque réglementation verticale ne vienne recréer de nouvelles règles et de nouveaux critères, dont il sera difficile d'assurer la cohérence.

22 MOBILISER L'ACHAT PUBLIC ET PRIVÉ

CONSTAT L'Europe investit des milliards d'euros en R&D, mais se fournit très largement à l'extérieur faute de réglementation instituant une préférence européenne dans certains domaines clés. L'un des leviers essentiels de toute politique industrielle digne de ce nom n'est donc pas utilisé pour encourager le développement de l'industrie numérique européenne.

OBJECTIF Pour favoriser le développement de l'industrie numérique européenne, l'objectif est de stimuler l'achat privé grâce à des mesures d'incitation, et l'achat public par une préférence européenne. Maintes fois évoquée, en particulier par Emmanuel Macron, l'adoption d'un *« Buy European Act »* sur le modèle du *« Buy American Act »* de 1933 est la seule mesure qui puisse réellement avoir un impact sur l'achat public. Il est d'ailleurs intéressant de constater que Joe Biden est non seulement en phase avec son prédécesseur sur ce thème, mais a même renforcé la notion de *« made in America »* (décret exécutif 14005) pour certains approvisionnements clés comme les semi-conducteurs, les batteries ou encore les principes actifs de médicaments et métaux rares. Le principe, qui n'a qu'une valeur politique, ne suffit pas. Il doit être gravé dans le marbre pour avoir une force juridique. Bien sûr, ce projet suscitera de fortes oppositions, en particulier en Europe du Nord. Il faudra donc sans doute se contenter d'une mesure appliquée par un nombre limité de pays, au moins dans un premier temps.

RECOMMANDATIONS

- Adopter un *« Buy Digital European Act »* qui instituerait pour tout achat public, dans le domaine numérique, que les prestations soient constituées d'au moins 50% de composants ou de services développés en Europe. Les composants étrangers ne sont pas exclus mais seront alourdis, lors de l'évaluation, d'une pénalité qui peut être augmentée si le concurrent européen est une PME. Sa pondération pourrait également être modulée en fonction des priorités stratégiques et des domaines considérés.
- Instituer un crédit d'impôt ou des mesures de sur-amortissement pour l'achat de services ou de solutions numériques européennes, notamment de cybersécurité, à des fins incitatives à destination de l'achat privé. Même si une telle mesure aura un impact sur le budget des États membres, son coût doit être mis *« en regard du coût de l'inaction pour la collectivité »*, souligne Philippe Vannier, Président de l'Alliance pour la confiance numérique. *« Créer un dispositif incitatif de type crédit d'impôt cyber doit être considéré par l'État comme un investissement, et non comme un coût. »*

› Favoriser des dispositifs d'achats mutualisés transnationaux permettant aux administrations de plusieurs États membres d'acheter ensemble. Cette condition est essentielle pour le développement de leaders européens. Le Conseil européen de l'innovation (EIC) pourrait avoir un rôle dans cette perspective.

23 RENFORCER **L'INVESTISSEMENT PUBLIC ET PRIVÉ**

CONSTAT L'investissement, qu'il soit public et privé, est un élément fondamental pour développer des entreprises leaders sur leurs marchés. Or l'Europe accuse toujours un retard important par rapport aux États-Unis qui captent très largement les investissements en cybersécurité en concentrant, dans le monde, 65% des opérations et 77% des 7,5 milliards d'euros levés (contre respectivement 24% et 12% pour l'Europe). Avec la crise Covid-19, les investissements captés par l'Europe dans ce domaine (pré-amorçage, amorçage, séries A, B, C… jusqu'au *« late stage »*) sont même repassés sous la barre du milliard d'euros en 2020 avec une baisse des opérations en un an[58].

Le ticket moyen des levées est également plus faible : 5,3 millions d'euros en Europe (6,5 millions en 2019) contre 13,5 millions aux États-Unis ou en Israël. Les conséquences sont sans appel : en 2020, sur les huit nouvelles licornes dans le domaine de la cybersécurité, six sont américaines, deux sont israéliennes[59]. Si cette faiblesse n'enlève rien au dynamisme de l'industrie européenne, qui est même de plus en plus attractive (comme le montrent les rachats récents d'Alsid et de Sqreen par les entreprises américaines DataDog et Tenable) malgré un marché intérieur très cloisonné, elle laisse cependant un sentiment d'inachevé.

OBJECTIF Mobiliser tous les instruments publics et privés pour accélérer la croissance des pépites européennes de cybersécurité, dont la taille est encore insuffisante et qui peinent non seulement à trouver les fonds nécessaires à l'amorçage mais aussi au développement, en particulier pour les grosses levées.

58. 183 opérations en 2018 contre 153 en 2019.

59. ACE Management, *Baromètre Ace de l'investissement européen en cybersécurité,* mai 2021.

RECOMMANDATIONS

Les fonds publics existants doivent financer en priorité des entreprises européennes :

- Accorder, via la Banque européenne d'investissement (BEI) et le Fonds européen d'investissement (FEI), des conditions plus favorables aux entreprises, y compris les PME et ETI. Ces dernières ont des difficultés à obtenir des conditions non excessivement dilutives pour leur propriété intellectuelle.
- Financer des projets industriels, notamment ceux de start-ups et PME, avec le Fonds européen de défense qui dispose d'un budget de 100 millions d'euros pour la cybersécurité (2021-2027).
- Investir dans des secteurs à forte intensité technologique, tels que la cybersécurité, en mobilisant le Conseil européen de l'innovation[60]. Lancé en mars 2021, ce fonds consacrera 3 à 3,5 milliards d'euros à des prises de participation directe[61] et 6 à 7 milliards à des prêts ou subventions.
- Recourir aux programmes *« Europe Numérique[62] »*, qui vise à apporter les technologies numériques aux entreprises, citoyens et administrations publiques, et *« Connecting Europe Facility[63] »* pour le développement d'infrastructures. Ces instruments, aux budgets respectifs de 7,5 milliards et 400 millions d'euros pour 2021-2027, constituent un label de confiance vis-à-vis de l'investissement privé.

Côté privé, même si la multiplication des attaques a déjà contribué à un regain d'intérêt pour les entreprises de cybersécurité, il est essentiel d'accélérer les investissements grâce à des mesures fiscales et réglementaires incitatives, ainsi que des fonds *ad hoc* susceptibles d'accompagner les entrepreneurs.

60. « La Commission lance le Conseil européen de l'innovation pour contribuer à transformer des idées scientifiques en innovations prometteuses », *Commission européenne,* 18 mars 2021.
61. Jusqu'à 15 millions d'euros en fonds propres pour 10 à 25% du capital.
62. « The Digital Europe Programme », *Commission européenne,* 2021.
63. « Connecting Europe Facility », *Commission européenne,* 2021.

24. FACILITER LES **TRANSFERTS DE TECHNOLOGIES**

CONSTAT Le lien entre la recherche académique et les entreprises ne fonctionne pas bien. Il n'existe ainsi que très peu de startups venant du monde académique[64]. Sur les 116 licornes européennes, seules 4 sont des *spin-off* universitaires[65]. Une large part de notre recherche, notamment dans le domaine numérique (intelligence artificielle, cybersécurité, etc.), ne débouche donc pas sur des projets industriels. La principale raison en est que l'entrepreneuriat académique est insuffisamment encouragé et que les chercheurs ne bénéficient que de peu de soutien lorsqu'il s'agit de transférer des travaux de recherche dans le secteur privé. Pire, ils sont souvent englués dans une bureaucratie lourde et inefficace qui les décourage. Autre obstacle : les revendications des centres de recherche et laboratoires universitaires en matière de propriété intellectuelle. Là où les universités américaines ne demandent que 5 à 10% du capital des entreprises créées, les universités européennes en demandent généralement de 25 à 50%. Même revendications sur les *royalties*, et ce alors qu'il faut parfois plusieurs années aux startups pour convertir les technologies en solutions opérationnelles.

OBJECTIF Fluidifier les transferts de technologies du monde académique vers le secteur privé. Les structures dédiées de Yeda (Israël) ou de Stanford (États-Unis) apparaissent comme des modèles à suivre. Le parc industriel de Stanford compte ainsi 150 entreprises employant 25 000 personnes. Même succès pour Yeda qui a la particularité d'être une entreprise privée, à l'origine de 73 entreprises dont les revenus cumulés atteignent 28 milliards de dollars[66].

64. Lire à ce propos : Nathan Benaich, « Universities in the UK and Europe have a start-up problem », *Financial Times*, 10 mai 2021.

65. On peut notamment souligner la réussite de Darktrace, pionnier de la détection des menaces, créée à partir de technologies développées à l'Université de Cambridge (Royaume-Uni).

66. « Yeda, Israël et le bureau de transfert de technologies de l'Université de Genève », *IsraelValley*, 7 février 2019.

RECOMMANDATIONS

L'appréhension de la propriété intellectuelle dans le numérique ne peut être la même que dans d'autres domaines tels que les biotechs : le développeur d'un code doit pouvoir en être propriétaire pour le mettre à jour en permanence sans avoir à gérer l'épineux problème de la copropriété. Les projets doivent donc être accompagnés par des professionnels de l'entrepreneuriat ayant une réelle vision du marché et des usages. Plusieurs pistes pour faciliter les transferts :

- Instituer un accord type de transfert de technologie prévoyant une part de capital limitée de 1 à 5%, ainsi que des montants réalistes pour les licences, qui ne peuvent en aucun cas démarrer dès les premières années, sous peine d'étouffer les jeunes pousses et de décourager les créateurs.
- Prémunir les structures de transfert de technologies contre tout risque de conflit d'intérêts. Pour cela, elles ne doivent pas se licencier à elles-mêmes les produits ou placer leurs propres salariés dans les entreprises qu'elles accompagnent. Les intérêts des différentes parties prenantes doivent être alignés et éviter autant que possible une asymétrie totale par rapport aux risques pris.
- Créer des systèmes d'alumni dynamiques, qui ne doivent pas être vus comme des *« porte-monnaies »* mais comme des *« mentors »,* pour favoriser l'imbrication du monde académique et de l'entrepreneuriat.
- Rapprocher le monde académique et les fonds d'investissement à des fins de financement de *« deep tech »* dont le développement demande des temps de maturation plus longs.

25 AMÉLIORER LE **SOUTIEN** À **L'INNOVATION**

CONSTAT Depuis 1984, environ 200 milliards d'euros ont été alloués par la Commission européenne à la R&D, dont 95,5 milliards au titre de Horizon Europe (2021-2027), 6,8 milliards au programme Europe Numérique et 1,8 milliards en faveur du mécanisme pour l'interconnexion en Europe. Si l'interdisciplinarité des projets soutenus constitue une force que le monde nous envie, le retour sur investissement de ces programmes est incertain en raison notamment de leur dispersion voire de la concurrence entre eux, du saupoudrage des financements, de leur gestion bureaucratique et de la dilution des responsabilités. En partant d'un objectif louable - protéger les deniers publics et éviter les fraudes -, le fonctionnement de ces projets a finalement annihilé toute appétence au risque, élément pourtant consubstantiel à la R&D.

OBJECTIF Concentrer les budgets de R&D européens sur certains objectifs clés (informatique quantique, IA, cybersécurité…) et éviter les actuelles mauvaises répartitions. D'autant que les montants alloués au numérique sont déjà sans commune mesure avec ceux des GAFA. Le budget du programme Europe Numérique ne représente par exemple que 1,8% des investissements d'Amazon en 2018, et celui annuel dévolu à Horizon Europe (13,6 milliards d'euros) est équivalent au montant R&D du seul groupe Alphabet[67].

RECOMMANDATIONS

Plusieurs axes permettraient d'éviter la mauvaise répartition des budgets de R&D :

- Instaurer une évaluation des projets, sans complaisance et sans considération de nationalité, dès un an après leur lancement pour identifier ce qu'il convient de garder ou non.
- Assurer une meilleure coordination entre les programmes existants, en particulier Horizon Europe, Europe numérique, et celui dédié au spatial, suivant l'exemple du Plan d'action lancé par la Commission européenne en 2021 pour améliorer les synergies entre les industries civiles, spatiales et de défense.
- Accélérer la mise en œuvre de la Facilité pour la relance et la résilience (NextGenerationEU). Pour ce faire, la politique de recherche de l'UE doit faire l'objet d'une meilleure gouvernance. Les missions du Conseil européen de l'innovation (CEI), récemment créé, doivent ainsi être précisées.
- Donner aux « *deep techs* » une place à part dans les programmes de recherche. Des challenges ou « *moonshots* » associant industriels, monde académique et administrations autour de grands défis thématiques doivent ainsi être développés, dans le sillage de ce que propose la Joint European Disruptive Initiative (JEDI), sur le modèle de Xprize, qui organise depuis 1994 des concours de grande envergure sur des thématiques à fort impact sociétal.

67. Ophélie Coelho, *Quand le décideur européen joue le jeu des big techs,* Institut Rousseau, juin 2021, p. 36.

FAIRE ÉMERGER DES **LEADERS EUROPÉENS** EN MATIÈRE DE ***CLOUD COMPUTING***

26

CONSTAT La souveraineté numérique recouvre deux notions : la souveraineté sur les données et la souveraineté technologique. En matière de *cloud computing*, l'Europe ne dispose aujourd'hui ni de l'une ni de l'autre[68], avec entre 50 et 70% de ses données qui seraient stockées aux États-Unis[69].

Les conséquences de cette dépendance sont multiples pour les organisations : la non-réversibilité, le syndrome du *« vendor lock-in »*, l'exposition à des lois extraterritoriales, les risques juridiques liés au RGPD, mais aussi *« l'ubérisation »* et la désintermédiation vis-à-vis des clients. Au-delà des données, ce sont des processus métier entiers qui sont progressivement transférés dans le *« nuage »* avec le risque de voir nombre de chaînes de valeur bouleversées au profit de plateformes numériques non-européennes.

Le pouvoir *« transformationnel »* du *cloud computing* doit donc être pris en compte à sa juste ampleur par les organisations. Le choix d'une solution répond bien sûr à des critères fonctionnels et techniques, mais il est aussi une décision stratégique engageante sur le long terme. D'autant que la dépendance au *cloud* ne fait que s'amplifier au fur et à mesure de la transformation numérique. Seulement 36% des entreprises européennes l'ont aujourd'hui adopté[70] mais leur nombre devrait doubler d'ici 2023.

Il est donc dangereux de se retrancher derrière le fatalisme en acceptant la dépendance européenne comme un fait établi. Si l'Europe a perdu une bataille en ne prenant pas à temps le virage du *cloud computing*, elle n'a pour autant pas perdu la guerre : elle dispose non seulement d'industries performantes et pleinement engagées dans la transformation numérique, mais aussi d'entreprises de services numériques et de fournisseurs de *cloud* dynamiques qui ont la capacité d'être compétitifs sur le marché mondial. Certes, il est indispensable de se positionner sur les *« game changers »* technologiques de demain que sont notamment le quantique et l'intelligence artificielle, mais le *cloud* étant le socle sur lequel s'enracineront ces technologies, il ne pourra pas y avoir de souveraineté numérique sans une maîtrise des infrastructures.

OBJECTIF Favoriser l'émergence de poids lourds européens en matière de *cloud* et de *edge computing*[71], tout en intégrant ces technologies dans les quatorze écosystèmes stratégiques identifiés par la Commission européenne.

68. Commission européenne, *Strategic dependencies and capacities*, 5 mai 2021.

69. Ophélie Coelho, *Quand le décideur européen joue le jeu des big techs,* Institut Rousseau, juin 2021.

70. Pour des dépenses estimées à 54 milliards d'euros en 2020.

71. Le *edge computing* consiste à traiter les données au plus près de leur source à la périphérie du réseau.

RECOMMANDATIONS

Si la souveraineté sur les données ne peut souffrir d'aucun compromis, l'UE n'a actuellement guère d'autre choix, sur le volet technologique, que de nouer des accords avec des partenaires externes pour conquérir une certaine maîtrise de ses infrastructures. Parce que le marché ne suffira pas à rétablir l'équilibre et à faire émerger des acteurs européens susceptibles de concurrencer les géants américains ou chinois, l'Europe doit en parallèle mobiliser rapidement tous les leviers possibles en matière de politique industrielle :

- Sensibiliser les acteurs et imposer la transparence. La localisation n'étant pas le seul critère de souveraineté des données, il s'agit aussi de savoir comment celles-ci sont stockées, utilisées et entraînées, par qui et dans quel cadre contractuel, et quelles lois extraterritoriales s'appliquent à un service *cloud* (indépendamment du lieu de stockage) qui obligeraient les fournisseurs à transmettre ou à divulguer les données des clients sur la base d'ordonnances légales non européennes.

- Labelliser les offres autour de principes clés que sont la réversibilité, la transparence et l'interopérabilité. Le projet Gaia-X joue un rôle essentiel de ce point de vue mais il faudra veiller à ne faire aucune concession si l'on souhaite que ce projet serve de « *rampe de lancement* » à la souveraineté technologique.

- Poursuivre les alliances industrielles dans le cadre de la nouvelle politique industrielle de la Commission européenne. Le lancement de celle consacrée aux données industrielles, au *edge* et au *cloud* vise à renforcer les capacités industrielles de l'UE sur le marché mondial et de promouvoir un modèle européen de *cloud computing* qui soit centré sur des valeurs telles que la souveraineté des données, ainsi que sur une approche technologique favorisant un traitement des données hautement distribué, sécurisé et économe en énergie. À cette fin, la Commission européenne devrait s'efforcer de promouvoir des synergies avec l'industrie, à l'image du projet Gaia-X, et des initiatives d'États membres telles que le projet important d'intérêt européen commun (PIEEC) sur les infrastructures et services *cloud*, qui est en cours de préparation. Ensemble, ces initiatives peuvent contribuer au développement et au déploiement de capacités de pointe en matière de *cloud* et d'*edge computing*, offrant ainsi aux entreprises et aux pouvoirs publics un véritable choix répondant à la fois aux normes les plus élevées en termes de performance, de protection des données, de sécurité et de durabilité. Les PIEEC, déjà utilisés pour la microélectronique et les batteries, permettent depuis 2014 aux États membres d'accorder des aides publiques à certains projets innovants. Si ce dispositif peut être utilement exploité pour faire émerger des leaders européens en matière de *cloud*, il doit néanmoins être simplifié et voir ses conditions d'éligibilité élargies. Il exige en outre des « *souches* » pré-existantes, une commande publique et privée, ainsi que toutes les compétences nécessaires. Une nouvelle gouvernance doit par ailleurs être trouvée : il s'agirait ainsi de substituer au Forum industriel informel, dont le mandat a pris fin en 2020, un comité exécutif susceptible de prendre des décisions[72].

72. Patrice Anato, Michel Herbillon, « L'avenir de la politique industrielle européenne », *Rapport d'information*, Assemblée nationale, 25 mars 2021.

FAVORISER LE DÉVELOPPEMENT D'UNE **IDENTITÉ NUMÉRIQUE EUROPÉENNE**

27

CONSTAT Seuls 59% de la population européenne et quatorze des vingt-sept États membres disposent d'un dispositif national d'identité numérique. Or les enjeux portés par l'identité numérique sont essentiels à plusieurs titres, notamment pour l'économie et le développement du marché intérieur (fondement juridique du règlement eIDAS), la citoyenneté européenne (éducation, accès aux soins, participation démocratique, libre circulation), ainsi que le développement d'une souveraineté numérique. Celle-ci est en effet indissociable d'une identité numérique commune ou d'un cadre d'identités nationales interopérables.

De manière générale, l'identité numérique permet un meilleur contrôle par l'utilisateur de ses données et un usage dynamique selon le contexte. Elle est un levier majeur de la transformation publique et de la simplification de la relation citoyen-État. L'identité numérique permet aussi de simplifier et d'optimiser les processus dit *« know your customer »* (KYC), de plus en plus courants, ou encore de développer des stratégies de santé électronique, de transport personnalisé ou de paiements sans friction.

La crise Covid-19 n'a fait que renforcer l'urgence d'une identité numérique européenne. Si rien n'est fait, l'adoption de solutions d'identification américaines ou chinoises privera l'Europe d'une intermédiation précieuse en termes de valeur ajoutée et de cybersécurité, ainsi que de capacité à faire respecter le droit européen sur l'espace numérique. Pour répondre à cette exigence, la Commission européenne s'est ainsi donné deux objectifs dans sa Boussole numérique pour 2030 : que 80% des Européens aient recours à une solution d'identification numérique et que tous les services publics de l'UE soient disponibles en ligne.

En juin 2021, la Commission européenne a proposé une nouvelle mouture du règlement eIDAS. Son texte prévoit de renforcer les obligations d'usage des identités numériques de confiance, tant au sein du secteur public que du secteur privé dit « *régulé* ». En parallèle, ses dispositions appellent à une plus grande flexibilité des attributs d'identité exigibles, ouvrant ainsi vers une plus grande diversité d'usages (banque, santé…). Outre la promotion du support mobile, la proposition envisage davantage de possibilités de certification des attributs d'identité par des services publics et privés, et propose la création de services de confiance numériques additionnels sur le plan européen comme l'archivage, y compris au niveau qualifié.

OBJECTIF Adopter des identités numériques de confiance de manière adaptée aux usages, *a minima* pour le secteur public et pour le secteur privé régulé.

RECOMMANDATIONS

- Favoriser l'adoption de la nouvelle mouture du règlement eIDAS de la Commission européenne.
- Encourager l'adoption des identités numériques par le secteur privé régulé en introduisant des exigences de conformité, de prévention des risques, de transparence et de lutte LCB/FT ou de prévention des risques cyber grâce à des niveaux de confiance homogènes minimum (identification, authentification/fédération), à l'image de ce qui existe pour le secteur financier (PSD2-CMF).
- Favoriser, outre les discussions avec le Parlement européen sur le projet eIDAS, les négociations entre les États membres pour déployer rapidement des projets-pilotes avec des financements du programme *« Europe numérique »*. L'objectif est de limiter les disparités entre les États qui resteront souverains sur la manière de les mettre en œuvre. Les projets-pilotes pourront également faire une large part aux systèmes d'identité décentralisés, ou auto-souverains, utilisant la technologie *blockchain*.
- Défendre, au plan international, l'adoption d'un standard ouvert et interopérable, comme OSIA[73], permettant aux États de choisir en toute liberté les fournisseurs d'identité tout en s'assurant d'une réelle interopérabilité en ligne avec les niveaux de protection de la vie privée et de sécurité requis par les Européens. La France et l'UE ne peuvent en effet rester indifférentes au mouvement *« d'API-fication »* qui atteint aujourd'hui les protocoles d'échange d'information d'identité comme hier les télécommunications ou l'*open banking*.

73. Le standard OSIA est porté par la Secure Identity Alliance.

ACCÉLÉRER LA MISE EN PLACE D'UNE **RÉGULATION DES ACTEURS SYSTÉMIQUES**

28

CONSTAT Les deux dernières décennies ont vu la montée en puissance d'une poignée d'entreprises à la tête de l'industrie numérique. Par leurs offres de services innovantes et diverses, ces acteurs se sont imposés, aussi bien en termes de nombre d'utilisateurs, de capitalisation boursière que de parts de marché, sur plusieurs segments au point de les structurer totalement (médias sociaux, *cloud*, systèmes d'exploitation...)[74].

Ces sociétés opèrent des plateformes numériques dont le modèle de développement repose sur la collecte des données personnelles de leurs usagers. L'effet de réseau inhérent pousse parfois à la monopolisation de services[75] et donne un caractère incontournable à ces entreprises qui en deviennent *« systémiques »,* avec en premier lieu les GAFAM américains (Google, Amazon, Facebook, Apple, Microsoft) puis les BATXH chinois (Baidu, Alibaba, Tencent, Xiaomi, Huawei). Le marché unique du numérique fait de surcroît l'objet de concentrations, perturbant ainsi le bon fonctionnement concurrentiel au risque de pratiques abusives.

Le démantèlement de ces acteurs - qui imposent leurs règles économiques, sociales, voire politiques - est souvent évoqué au nom des législations antitrust. Une telle perspective apparaît cependant peu probable compte tenu de l'avantage stratégique que représentent ces entreprises pour les puissances numériques et des difficultés techniques et financières qu'un démantèlement en bonne et due forme susciterait. Même si la captation de valeur par ces géants est bien réel, la dépendance de nos startups et entreprises à leur égard pour le développement de leurs applicatifs ne doit en outre pas être sous-estimée.

L'Europe ne prend pas la mesure de ce *« gigantisme »* du fait d'une régulation inadaptée au numérique. En 2011, l'UE a validé l'acquisition de Skype par Microsoft, qui concentrait alors à l'époque 85% du marché de la communication vidéo[76]. Cette opération est plus largement symptomatique d'un décalage entre sa politique industrielle et son droit de la concurrence, comme en témoigne son refus récent de la formation d'un poids lourd européen dans le ferroviaire, tout en laissant le leader chinois, soutenu par son État, pénétrer le marché intérieur. D'autant que la Chine ne permet pas en retour aux sociétés européennes du secteur de s'introduire dans le sien. Cette tendance traduit l'absence d'emprise sur les firmes étrangères[77].

74. Alain David, Marion Lenne, « Les géants du numérique », *Rapport d'information,* Commission des Affaires étrangères, Assemblée nationale, 2 juin 2021.

75. « DMA : un nouveau rôle pour les autorités de la concurrence », *Institut Montaigne,* 26 février 2021.

76. Commission européenne, *COMP/M.6281, Microsoft/Skype,* 7 octobre 2011.

77. Patrice Anato, Michel Herbillon, « L'avenir de la politique industrielle européenne », *Rapport d'information,* Assemblée nationale, 25 mars 2021.

Pour garantir des marchés *« plus justes »*, la Commission européenne a présenté le *Digital Markets Act* (DMA) en 2020, qui vise à doter les marchés numériques d'un environnement commercial plus équitable, en imposant des obligations aux acteurs systémiques et en favorisant l'émergence de petites entreprises.

OBJECTIF Renforcer les dispositions du *Digital Markets Act* (DMA) et en accélérer l'adoption.

RECOMMANDATIONS

Face au verrouillage des marchés numériques par les géants qui en contrôlent l'accès (*gatekeepers*), un DMA robuste permettra de renforcer la concurrence en introduisant une régulation *ex-ante*, en complément de l'intervention *ex-post* des autorités de la concurrence des États membres.

- Appliquer strictement le droit de la concurrence aux marchés numériques, tout en tenant compte des considérations stratégiques induites par la concurrence des acteurs systémiques.
- Préciser la distinction des prérogatives entre la Direction générale de la concurrence de l'UE (DG COMP) et les autorités nationales de concurrence afin de favoriser leur complémentarité et leurs synergies.
- Doter la Commission européenne d'un service d'intelligence économique[78], chargé de l'analyse des comportements des principaux concurrents étrangers, ainsi que des fusions-acquisitions pour limiter celles susceptibles d'être prédatrices pour les entreprises et l'innovation de l'UE[79].

78. *Ibid.*

79. France, Germany, Netherlands, *Strengthening the Digital Markets Act and Its Enforcement*, mai 2021.

CONCLUSION

Placée sous la devise ***« relance, puissance, appartenance »***, la Présidence française du Conseil de l'Union européenne (PFUE), qui se tiendra au premier semestre 2022, aura la charge de décliner ce triptyque sur le plan numérique, pour poursuivre, si ce n'est engager, une dynamique permettant à l'Europe de :

- **Assurer la *« relance »*.** Lors de la présidence française, l'UE devra mettre sur une rampe de lancement sa nouvelle stratégie industrielle, en mobilisant tous les leviers (achat public et privé, transfert de technologie...) pour accélérer sa transformation numérique et disposer d'une industrie dans ce domaine ;
- **Devenir une *« puissance »* du monde numérique.** Pour ne plus en être une simple *« colonie »*, l'Europe devra continuer de promouvoir un espace numérique régulé, équilibré et interopérable dans les enceintes diplomatiques, tout en développant ses propres capacités de cybersécurité et de cyberdéfense ;
- **Développer le sentiment *« d'appartenance »*.** L'Union devra, outre renforcer l'acculturation et la formation au numérique de ses citoyens, conduire des réflexions sur son *« identité numérique »* qui doit reposer sur la conscience d'un destin commun des États membres et sur des systèmes *ad hoc* interopérables.

Dans l'Europe numérique de demain, la cybersécurité doit être à la fois une clé de voûte et un fer de lance. Une clé de voûte pour assurer la résilience collective dans le contexte de transformation numérique. Un fer de lance pour défendre et valoriser les intérêts européens, dans un monde marqué par le *« retour des puissances »* et par des stratégies globales dans lesquelles le cyberespace occupe une place grandissante. Si la puissance ne peut pas être uniquement numérique, il ne peut y avoir de puissance sans numérique.

Loin de signifier un repli sur soi, **la souveraineté numérique à laquelle aspire l'Europe est au contraire une opportunité historique pour lui permettre de retrouver un sens,** tant en interne que sur la scène internationale.

Au sein de l'UE, bien que les sujets relatifs au numérique rassemblent plus qu'ils n'opposent, la recherche de consensus entre vingt-sept États membres demande toujours du temps. Face à l'urgence des enjeux, y compris en matière de politique industrielle, des coopérations et des associations *ad hoc* doivent être favorisées, afin de relancer rapidement le moteur européen. Les nouvelles alliances sur les technologies clés que sont les semi-conducteurs, le *cloud computing* et l'intelligence artificielle devront le montrer.

Dans le monde, l'UE a une voix à faire entendre face au duopole sino-américain. La protection des données personnelles, la transparence algorithmique, le refus du *hack back*, la lutte contre la prolifération des cyber-armes, la promotion d'un espace numérique ouvert, libre, stable et sûr sont autant de sujets sur lequel elle tente de tracer une voie médiane, refusant tout totalitarisme.

S'il est exagéré de dire que l'Europe est attendue, elle est toutefois regardée : cela ne lui confère aucun droit et crée au contraire des exigences.

Une exigence **opérationnelle** d'abord. Les Européens doivent être capables de répondre à la multiplication et à la sophistication des cybermenaces, ainsi qu'à toutes formes d'insécurité, y compris informationnelle, dans l'espace numérique, les démocraties étant par essence plus exposées aux manipulations de l'information. Une exigence **éthique** ensuite. Si des concessions peuvent être envisageables en matière de souveraineté technologique pour des raisons tactiques, la souveraineté des usagers sur leurs identités et données personnelles ne peut en revanche se marchander. Une exigence **politique** enfin. Pour accepter le progrès technologique et bénéficier de la mondialisation et de la transformation numérique, les citoyens européens attendent une Union forte et innovante.

Pour réussir, l'Europe doit agir dans la durée. Les six mois de présidence française ne seront qu'une anecdote historique. Comme le précise la stratégie numérique présentée par la Commission européenne en mars 2021, c'est toute la décennie qui doit être numérique, et la réussite des politiques d'aujourd'hui ne pourra être mesurée qu'en 2030. L'exigence est donc aussi méthodologique : il s'agira davantage d'approfondir, de coordonner, de mettre en réseau et de donner du rythme à l'existant, que de créer de nouvelles structures dans un environnement déjà foisonnant. Tout cela en coordination avec l'Allemagne, le Portugal et la Slovénie qui nous ont précédés, ainsi qu'avec la République tchèque et la Suède qui suivront.

Alors qu'il est souvent reproché à la France de ne voir l'UE qu'à travers le prisme de ses propres intérêts, il sera également nécessaire de se décentrer suffisamment pour défendre non plus des intérêts purement français mais européens. Il n'y aura en effet pas de puissance européenne sans des intérêts communs clairement définis.

Cette Europe de la cybersécurité devra enfin trouver un équilibre entre la nécessaire mutualisation des normes et des capacités et le respect de la souveraineté de chaque État membre, laquelle demeure intangible dès lors que des atteintes sont portées à la défense et à la sécurité nationale. Ainsi, plus de capacités à l'échelon européen ne signifie pas moins de capacités dans chaque État membre. Au contraire.

Cette Europe, plus collective et collaborative, concentre ses efforts sur la sécurité des infrastructures critiques, la protection du marché unique et, depuis peu, sur la régulation des contenus et des plateformes. Mais la lutte contre la cybercriminalité est encore trop négligée, même si l'UE joue un rôle important dans les progrès de la convention de Budapest et dans l'amélioration des conditions d'accès aux preuves numériques (règlement *« e-evidence »*). **La cybersécurité est un état obtenu en conjuguant la sécurité des systèmes d'information, la lutte contre la cybercriminalité et la cyberdéfense.** Chacun de ces trois piliers exerce un rôle essentiel si l'on veut créer un *« bouclier européen »*. En vérité, l'ambition serait davantage de créer une *« tortue romaine »* européenne, couvrant toutes les facettes de la menace, obligeant chaque État membre à créer lui-même son propre bouclier, interopérable avec tous les autres, renforcé en cas de besoin par un dispositif collectif de prévention, de répression ou de défense.

Les recommandations qui précèdent, issues d'une réflexion partagée avec de nombreux experts, français ou européens, issus du secteur public ou privé, peuvent sembler reprendre des idées déjà énoncées, des programmes en cours ou annoncés. Elles ne sont qu'une illustration de ce qui devrait sous-tendre la dynamique de la PFUE. **Cette présidence doit d'abord mettre en perspective la cybersécurité européenne, accentuer sa dimension politique et stratégique en replaçant le citoyen européen au cœur du débat.** Ce citoyen, consommateur, victime, attend de l'Europe qu'elle le protège, dans son identité, sa sécurité, son autonomie de décision. Sans renoncer au discours porté sur les organisations, les infrastructures, les entreprises, il importe d'associer le citoyen à une vision collective sur un futur européen porteur de progrès et de sécurité pour tous. **La présidence française doit donner du souffle à un moment où la crise sanitaire pousse au chacun pour soi.**

REMERCIEMENTS

L'Agora du FIC remercie toutes les personnes auditionnées ou consultées dans l'élaboration de ce livre blanc :

Henri d'AGRAIN, délégué général du CIGREF

Gilles BABINET, co-président du Conseil national du numérique (CNNum)

Bertrand BADIE, professeur des Universités à Sciences Po Paris

Karine BANNELIER, maître de conférences à l'Université Grenoble Alpes

Annegret BENDIEK, chercheuse associée au Stiftung Wissenschaft und Politik (SWP)

Bernard BENHAMOU, secrétaire général de l'Institut de la souveraineté numérique (ISN)

Paula BROUILLARD MOLINA, chargée de communication et médias à la DG CONNECT

Théodore CHRISTAKIS, professeur à l'Université Grenoble Alpes

Mireille CLAPOT, députée et présidente de la Commission supérieure du numérique et des postes (CNSP)

Tanguy de COATPONT, directeur général de Kaspersky Lab France

Christian DAVIOT, ancien conseiller Stratégie du directeur général de l'ANSSI

Olivier EZRATTY, consultant indépendant et spécialiste des technologies numériques

Guy de FELCOURT, Expert sur les questions d'identité numérique, co-organisateur de l'ID Forum

Général de brigade Éric FREYSSINET, Commandant en second de la gendarmerie dans le cyberespace, ministère de l'Intérieur

Jean-Noël de GALZAIN, fondateur de Wallix et président d'Hexatrust

Lieutenant-colonel Étienne GIRARD, chef du bureau UE de la Direction de la coopération internationale (DCI), ministère de l'intérieur

Benoît GRUNEMWALD, expert cybersécurité à ESET

Yoann KASSIANIDES, délégué général de l'Alliance pour la confiance numérique (ACN)

Wolfgang KOPF, Senior Vice President pour le groupe des affaires publiques et réglementaires à Deutsche Telekom

André LOESEKRUG-PIETRI, président de la Joint European Disruptive Initiative (JEDI)

Julien NOCETTI, chercheur associé à l'Institut français des relations internationales (IFRI)

Aurélien PALIX, sous-directeur des Réseaux et usages numériques à la Direction générale des entreprises (DGE), ministère de l'Économie et des finances

Général d'armée aérienne (2S) Jean-Paul PALOMÉROS, ancien commandant allié Transformation à l'OTAN

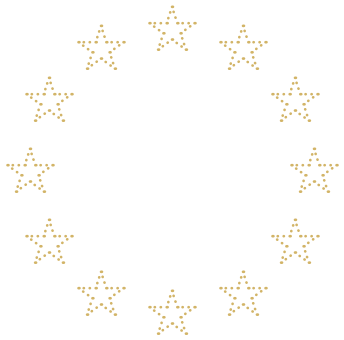
Sylvain ROURI, directeur exécutif, OVHcloud

Tadej RUPEL, ambassadeur et coordinateur national pour la numérisation IA et cybersécurité de la Slovénie

Rayna STAMBOLIYSKA, vice-présidente Gouvernance et Affaires publiques de YesWeHack

Général de division aérienne Didier TISSEYRE, commandant de la cyberdéfense, ministère des Armées

Les opinions exprimées dans ce livre blanc n'engagent ni les personnes précédemment citées, ni les institutions qu'elles représentent.



Agora FIC

FORUM-FIC.COM