EGE Ecole de Guerre Economique

Unis dans la diversité

La cyber sécurité un enjeu collectif

Romain GODUCHON Simona LEROUX Jean-William LIENG Édouard PETETIN

“The ignorance of one voter in a democracy impairs the security of all”

John F.

Le présent rapport a été conçu avec une mise en page hybride, afin qu’il puisse être consulté tant en version papier ainsi qu’en version numérique. Tous les textes soulignés sont interactifs. Les crédits pour les photos appartiennent à Adobe, à l’exception des images qui ont une référence.

Table des matières

Avant de présenter nos travaux de recherche, il est nécessaire de préciser quelques notions de vocabulaire.

Coordination, coopération, collaboration

Tout au long de ce mémoire, nombreux seront les termes contenant l'idée d'une action commune, d'un objectif commun ou d'un effort commun. Des mots tels que *coopération*, *collaboration* et *coordination* sont indispensables lorsqu'on parle d'alliances, de relations acheteur-fournisseur, de partenariats ou de missions communes. Bien qu'utilisés de manière interchangeable, voire avec peu de discernement[1], surtout dans le contexte du travail en équipe et des affaires, ces termes portent chacun une nuance particulière.

Une première différenciation entre ces termes vient du latin. La coordination (du latin *cum ordinare*) renvoie à l'action de mettre en ordre, organiser, avec d'autres. Il s'agit d'une action collective d'organisation. Pour la coopération et de la collaboration (du latin *cum operare*, et respectivement *cum labor*) le latin manque de précision car les termes renvoient respectivement à l'action de travailler et à la tâche.

De plus, rappelons que ces termes impliquent tous, mais à de degrés différents, les trois dimensions qui caractérisent les relations interpersonnelles[2] dans le monde des affaires et des décisions : l'attitude, le comportement et les résultats. Néanmoins, c'est peut-être l'objectif qu'ils poursuivent qui serait à-même de départager ces termes. L'usage que nous ferons de ces termes dans le mémoire sera donc fondé sur les définitions suivantes :

- La coordination désigne l'attitude, le comportement et le résultat liés à la formulation conjointe d'objectifs communs. Dans notre mémoire, cela renverrait aux prérogatives de la *European Union Agency for Cybersecurity* (ENISA), mais pas uniquement.
- La coopération désigne l'attitude, le comportement et le résultat liés à la mise en œuvre des objectifs tels qu'ils ont été convenus. On pourrait la désigner comme « mode opératoire de la coopération ». Elle renvoie à la poursuite d'intérêts mutuels et de bénéfices communs dans des alliances. Elle est aussi l'opposé de la compétition, ou de la concurrence. La question centrale de la compétition concerne la prévalence des objectifs privés par rapport aux objectifs communs entre les concurrents. Plus ces objectifs privés sont prioritaires, plus les chances d'émergence d'une coopération s'éloignent. La question de la coopération entre les acteurs privés, d'ailleurs concurrents directs, sera présentée de cette perspective.
- La collaboration renvoie au fait d'aider volontairement les autres à atteindre un but, commun ou non. Ces buts peuvent être altruistes, ou égoïstes - parfois même opportunistes, c'est-à-dire au détriment des autres partenaires – ou encore communs ou collectifs.

Cybersécurité

La cybersécurité réunit les activités visant à protéger les systèmes informatiques contre les attaques malveillantes ou l'espionnage. Elle englobe toutes les techniques et les outils mis en œuvre pour protéger les infrastructures mais aussi la confidentialité, l'intégrité et la disponibilité des données stockées ou échangées dans l'espace numérique. Plus largement, l'UE définit que la cybersécurité recouvre « les activités nécessaires pour protéger les réseaux et les systèmes d'information ainsi que les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces. »[3]

Pour atteindre ce but, l'UE s'est dotée en 2013 d'une *Stratégie Européenne de Cyber Sécurité*. Nous ne nous sommes pas intéressés à l'efficacité de cette stratégie. Sans doute améliorable, nous la considérons comme un texte fondateur de la cybersécurité européenne. Notre analyse fera souvent référence à cette stratégie et à la manière dont le manque, ou, au contraire, la présence d'une action commune impacte la capacité d'atteindre les objectifs de cette stratégie.

Périmètre géographique : quelle Europe considérer ?

L'Europe est également un concept qui englobe plusieurs réalités à préciser. Elle sera ici approchée selon trois dimensions.

Tout d'abord, l'Europe en tant que puissance macro-régionale. Au regard de l'enjeu mondial que représente la cybersécurité, il est tout d'abord naturel de considérer l'Europe comme une puissance régionale parmi les grandes puissances que sont les États-Unis, la Chine, et la Russie. Mais en plus de son rôle de puissance régionale, sa place dans l'OTAN ainsi que sa proximité avec les États-Unis est à rappeler.

La deuxième dimension de l'Europe est celle continentale, sans considérer l'Union européenne. Comme nous l'a démontré le conflit ukrainien, l'Europe, en tant que défenseuse de la démocratie, est pourtant solidaire d'un pays non-membre de l'Union européenne. Il y a une certaine solidarité territoriale, liée à des préoccupations sur la sécurité de l'Union européenne. Ainsi, l'entraide européenne en matière de cybersécurité fait partie de l'ADN des Européens, et cela se concrétise dans des interventions d'États membres de l'Union européenne auprès de pays non-membres de l'UE.

Enfin, l'Europe sera abordée en tant qu'Union Européenne, initiatrice du cadre réglementaire européen, fer de lance de la *Stratégie européenne de cybersécurité*.

Comme pour les termes précédemment définis, l'approche de notre analyse sera donc fondée sur la distinction de ces périmètres géographiques au regard des enjeux de coopération, collaboration, et coordination pour le déploiement de la stratégie cyber européenne.

L'Union européenne : contexte et rappel des missions de l'UE

Avant toute chose, il est important de rappeler que l'Union Européenne a pour mission historique de préserver la paix sur le continent, et ce depuis la fin de la Seconde Guerre mondiale. Elle en a pris en partie la charge à travers l'établissement d'un marché intérieur unique. Ce "marché économique commun" permet de faire converger les économies autour de rapports pacifiés, et ce en rapprochant les politiques économiques des États membres par la promotion d'un développement des activités économiques européennes (avec la balance économique européenne comme indicateur majeur). Par la suite, il est important de garder ces considérations en tête pour comprendre certains dysfonctionnements concernant le déploiement de la stratégie Cyber européenne.

L'OTAN

L'Union européenne a une place au premier rang à l'OTAN. Face à ce que l'on appelait il y a encore 30 ans le bloc soviétique, le vieux continent était le premier rempart face au communisme pour l'Amérique du Nord. Dans leur conquête de la suprématie mondiale, les États-Unis l'ont rapidement compris et ont mis en place des leviers commerciaux, financiers et militaires très puissants pour garder effective leur influence sur l'Europe.

L'UE s'est créé et développée en parallèle de l'expansion de l'OTAN, sans en être une concurrente mais bien plutôt une partenaire aux intérêts différents. Cette divergence était révélée lors du scandale « Fuck the EU » en 2014 : Mme Nuland, alors secrétaire d'État adjointe aux États-Unis pour l'Europe est en désaccord avec les décisions de l'Union européenne au sujet de la première crise ukrainienne. Aujourd'hui, l'Union européenne se construit et se développe tout en respectant la souveraineté immuable de chacun de ses membres, alors qu'avec les années 2000, l'OTAN se montre invasive : elle part en guerre en Afghanistan, et se positionne comme ennemie d'une Russie cherchant à retrouver sa grandeur perdue.

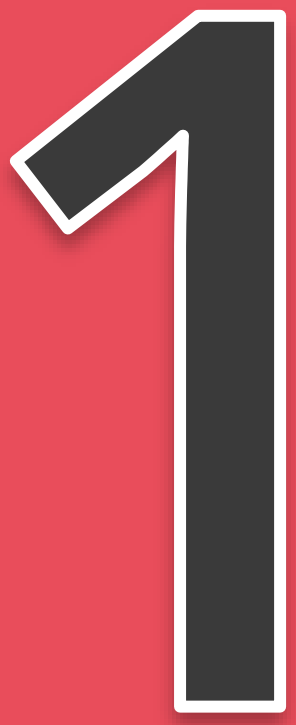
L'Europe reste attachée à une certaine indépendance commerciale et à une défense autonome gérée par chaque État membre sur son territoire, malgré la puissance militaire nord-américaine. En conclusion, l'UE n'est pas un État fédéral, et le Brexit démontre bien l'aspiration atlantiste de certains membres.

Prémices de l'analyse

Nous avons établi que l'une des missions principales de l'UE était d'assurer et de renforcer la démocratie et les droits fondamentaux des citoyens sur les réseaux numériques. Sans cela, leur sécurité et leur devenir pourraient être menacés, la liberté d'opinion ou de pensée pourrait être brimées. En effet, les nouvelles technologies qui impactent Internet (y compris celles à venir) sont des outils majeurs de déstabilisation… ou de renforcement de la démocratie. Désormais consciente de ces enjeux, l'Union Européenne a fait de sa stratégie de cybersécurité l'une des principales priorités. Elle le confirme d'ailleurs dans sa *Nouvelle stratégie de cybersécurité* en 2020.

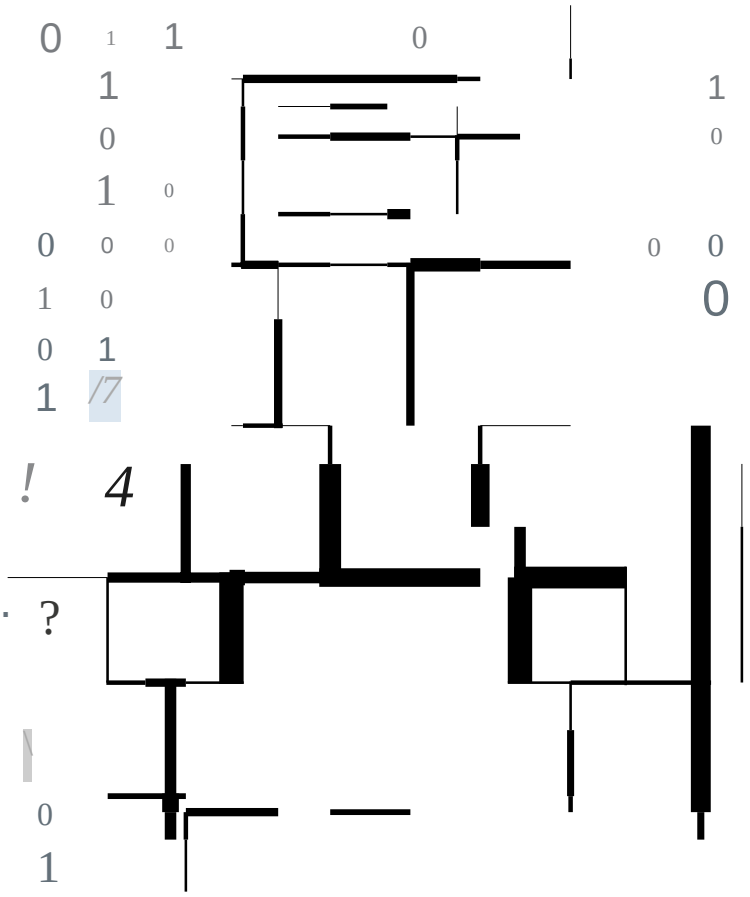
Mais qu'en est-il de la mise en œuvre de cette stratégie ? On pourrait mesurer sa pertinence au travers du nombre d'initiatives proposées, mais aussi à travers de la cohérence de ces initiatives. Comme nous allons le voir, la cohérence n'est pas seulement une question d'efficacité mais également de tenue sur le long terme. Elle pourrait se mesurer par la correspondance entre le positionnement des institutions et les objectifs de la stratégie, la conformité des initiatives opérationnelles à ces objectifs, et la qualité du lien entretenu, entre la rhétorique et la pratique.

Finalement, la cybersécurité met en avant certaines dichotomies sur lesquelles ce mémoire s'attardera. Parmi celles-ci : intérieur/extérieur, publique/privé, militaire/civil. De plus, la croissante mise en réseau de tous les pays et la dimension globale de la cybersécurité rendent floues les limites géographiques entre les niveaux mondiaux, européens et nationaux des menaces. Mais ce ne sont pas les seules limites à être troubles : le sont aussi le périmètre d'intervention des États, ainsi que la répartition d'éventuelles responsabilités. Évaluer la mise en œuvre de la stratégie cyber de l'Europe n'est donc pas aisé. Toutefois, les acteurs du secteur de la cybersécurité représentent une constante dont nous allons nous servir pour structurer notre analyse. Sur une dimension verticale, nous pouvons observer une hiérarchie : l'OTAN, l'Union Européenne (UE), les États Membres (EM) et les acteurs du secteur privé. Le plan horizontal, quant à lui, analyse les interactions entre acteurs de même niveaux hiérarchiques. Tout au long de ce mémoire, la coopération sera donc approchée, d'une part, verticalement, par l'étude des acteurs appartenant à des niveaux hiérarchiques différents ; d'autre part, horizontalement, entre acteurs appartenant au même niveau.



CHAPITRE UN

UNE STRATÉGIE CYBER À LA HAUTEUR DE LA MENACE



1.1. À la croisée des puissances mondiales

Le détournement d'Internet

En 1989, Sir Tim Berners-Lee créait le World Wide Web pour faciliter l'interconnexion et l'interopérabilité de systèmes informatiques universitaires aux quatre coins du monde. Trente ans après, la coalition *Contract for the Web* réaffirme la mission d'intérêt général du Web Wide World[1] :

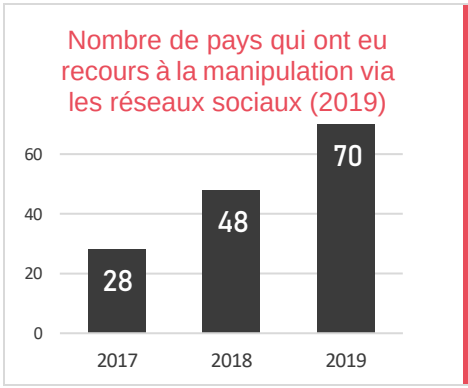
> *Le web a été conçu pour rassembler les gens et rendre les connaissances librement accessibles.*
>
> *Chacun a un rôle jouer pour que le web serve l'intérêt général.*

Avec le développement rapide des technologies émergentes qui permettent d'exploiter encore davantage Internet (5G, cloud, intelligence artificielle, chiffrement, blockchain, etc.), Internet offre des opportunités de croissance économique en termes d'innovation, de commerce et d'emploi jamais connues auparavant. Par exemple, rien qu'en Europe, la seule 5G devrait entraîner une hausse de 1 000 milliards d'euros€ du PIB européen entre 2021 et 2025. Elle pourrait donner lieu à la création ou à la transformation de 20 millions d'emplois dans tous les secteurs de l'économie [2] . Quant à elle, l'adoption généralisée de l'intelligence artificielle (IA) au niveau mondial, a le potentiel de générer une activité économique supplémentaire d'environ 13 000 milliards de dollars d'ici à 2030, soit un PIB cumulé supérieur d'environ 16% à celui de 2018. Cela représente une croissance supplémentaire du PIB de 1,2% par an[3].

Par ailleurs, avec la démocratisation de l'accès à Internet, des pans entiers de l'accès à l'information et à la culture connaissent des mutations très rapides. Si on considère qu'un adulte est actif en moyenne 16 à 17h par jour, l'internaute moyen passe 40% de ce temps sur Internet[4]. Et cette moyenne, qui a connu un allongement d'environ 4 minutes par jour pendant la seule année 2021, cumulant au niveau global 5 millions de jours de connexion additionnels, n'est pas près de se stabiliser.

L'accès à l'information a subi également des changements majeurs. 4 personnes sur 5 s'informent aujourd'hui sur Internet, avec une grande préférence pour les réseaux sociaux plutôt que les journaux papier, bien que la présence de *fake news*, *intox* et autres désordres informationnels ne soit plus à démontrer. L'enjeu du contrôle de l'information est donc central. L'outil était utilisé en 2019 par 70 pays, en augmentation de 150% en seulement 2 ans[5]. À ce contrôle de l'information au centre de l'attention se joignent les enjeux de la manipulation des masses et de possibles interférences étrangères ou domestiques. Les préoccupations portées sur cet accès à l'information ultrapuissants sont finalement justifiées par la mise en péril de la démocratie, et de facto, des droits fondamentaux des citoyens[6]. À une époque où la majorité du contenu informationnel mondial est distribué globalement par une poignée de plateformes, ne connaissant pas de frontière étatique, ces sociétés exercent un pouvoir monopolistique non seulement complètement disproportionné, mais surtout dangereux pour les démocraties à travers le monde. Et bien qu'ils affichent une image de toute-puissance, les États-Unis sont parmi les premiers à subir ces risques.

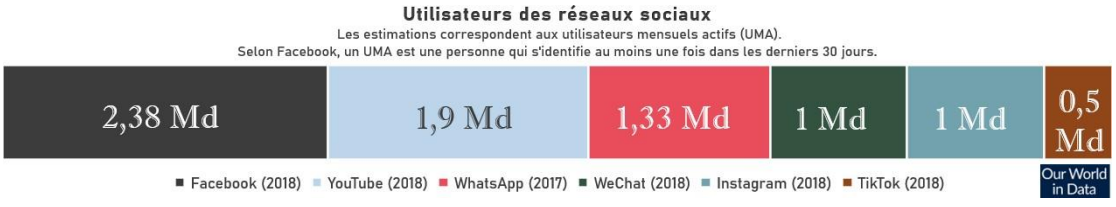
Données : Bradshow et al. 2019



150%

augmentation des pays utilisant des campagnes structurées de manipulation sur les réseaux sociaux.

Depuis 2019, le téléphone mobile est devenu le terminal de connexion le plus utilisé (55,5% du temps de connexion en 2022[7]) et ses utilisations se multiplient : accès à l'information, réseaux sociaux, jeu en ligne,



achats, démarches administratives, accès à la culture (offres de streaming), etc. C'est ainsi que de multiples usages, et une fréquence d'utilisation accrue créent davantage de vulnérabilités pour ces utilisateurs. Mais la sécurisation des smartphones est toujours plus complexe, comme Internet lui-même n'a pas été conçu avec la sécurité comme priorité. Le succès économique des réseaux sociaux est lié directement à l'accès à Internet. Les interactions humaines, toujours imprévisibles, ne sont pas à l'abri, voire sont parfois même victimes, de certains mécanismes psychosociaux exploités à dessein. Quelques éléments se retrouvent sur tous les réseaux sociaux : les biais cognitifs[8], l'intérêt pour le buzz, la soif de reconnaissance, les biais de l'intelligence artificielle[9], l'économie de l'*infox*[10]. Ces mécanismes sont très efficaces. Ils consistent à faire remonter dans le fil de discussion l'avis subjectif d'un internaute ou de son groupe plutôt qu'une information officielle, en théorie plus objective. Aussi, les algorithmes à la base de ces éléments participent à l'enfermement des internautes dans des bulles cognitives et informationnelles : les internautes se voient recommander les publications de groupes d'individus partageant les mêmes idéologies. Ainsi, les algorithmes des réseaux sociaux finissent par restreindre aux internautes l'accès à une grande diversité d'informations et de points de vue [11] . Ce risque est aujourd'hui bien réel, et son impact peut être dévastateur.

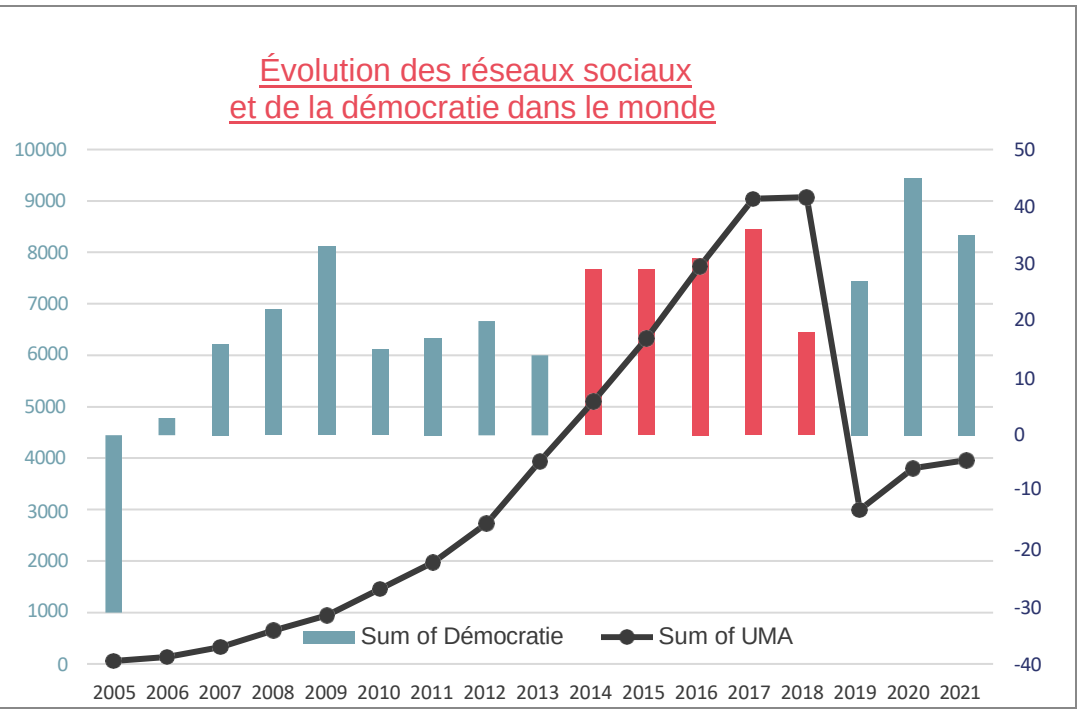
Dans ce contexte, celui qui contrôle l'information véhiculée par Internet peut, en théorie, manipuler une partie de l'opinion publique mondiale. C'est ainsi que *Les Printemps arabes* en 2011 ont aussi eu pour enjeux de permettre l'accès à la libre information. Si certains pays comme la Syrie se sont enfoncés dans la guerre, d'autres ont pris des mesures spécifiques et se sont davantage démocratisés, à l'exemple du Maroc. Cependant, pendant ces seize dernières années, alors qu'Internet montait en puissance, la démocratie, elle, n'a cessé de reculer. En 2021, 6,4% de la population mondiale vivait dans une réelle démocratie alors que plus de 37% de la population vivait sous un régime autoritaire[12]. Malgré ses valeurs fondamentales démocratiques, ainsi que le message d'utilité qu'il porte, Internet aujourd'hui est souvent l'un des outils principaux de mise à l'épreuve des valeurs démocratiques, et de déstabilisation des démocraties elles-mêmes. On en déduit qu'Internet est devenu, en peu de temps, l'épine dorsale de notre société et, potentiellement l'un des facteurs à l'origine du déclin de la démocratie à travers le monde[13].

Néanmoins, dans nos démocraties occidentales, l'accès à Internet est un droit protégé[14]. Ainsi, l'utilisation d'Internet peut aussi être vecteur d'émancipation citoyenne, en ce qu'elle permet la liberté d'accès à l'information, la liberté d'expression, et la liberté d'échange.

2014 -2019

évolution inverse du développement des réseaux sociaux et du recul de la démocratie

Depuis 2005, il n'y pas eu de recul de réseaux sociaux, ni d'élargissement de la démocratie.



Données : Freedom House et Our World in Data

Pour autant, Internet n'a jamais été un lieu à l'abri d'actes malveillants. Les attaques cyber sont nées avec Internet. Cependant, à partir de 2010, le cas Stuxnet rentre dans l'histoire, en faisant prendre

conscience que ces attaques ne sont plus uniquement perturbatrices (*disruptive*), mais bien destructrices. Ce changement de niveau d'impact fut majeur, et de telles attaques continuent d'impacter l'ordre public. Deux décennies après Stuxnet, les attaques par wiper[15] pullulent dans la guerre en Ukraine. Les aveux en 2013[16] de l'ancien agent de la National Security Agency américaine, Edward Snowden, ont prouvé que les États-Unis et les Britanniques utilisaient aussi Internet à des fins de renseignement et de surveillance[17]. La Chine a été accusée d'avoir détourné le trafic Internet à plusieurs reprises pour en extraire les données pendant des heures, voire des années[18], ce qui portait atteinte à la disponibilité et à la stabilité opérationnelle des réseaux. L'utilisation des réseaux sociaux en tant qu'outil de surveillance des masses est en cours de généralisation en Chine[19]. Plus Internet grandit et se démocratise, plus les flux de données se massifient, plus ces attaques sont vouées à se multiplier et à se complexifier à travers un *modus operandi* hybride. Le risque qu'Internet soit détourné de sa mission d'origine grandit chaque jour un peu plus.

L'escalade dans le niveau de complexité et de destruction des attaques menées par des groupes étatiques (APT) et des groupes criminels mettent potentiellement à risque la résilience et la disponibilité d'Internet pour plus de 5 milliards d'humains connectés à Internet (63,1% de la population) et quelques 4,7 milliards d'humains adeptes des réseaux sociaux (59% de la population) [20] . À cela s'ajoutent les millions d'entreprises à travers le monde pour lesquelles l'accès à Internet représente une condition *sine-qua-non* pour leur opérabilité et compétitivité[21]. Sans parler de la confidentialité des données y transitant, qui conditionne aussi de manière directe et presque instantanée, la confiance des utilisateurs.

La confiance numérique

La confiance semble être un facteur clé dans les choix des acheteurs et des usagers d'aujourd'hui. Il n'est donc pas risqué d'affirmer qu'en théorie, le jour où les internautes perdront définitivement la confiance dans Internet, 3 844 milliards de dollars[22] des flux de capitaux de l'économie mondiale pourraient partir en fumée. Et ce, car si Internet régit un nombre colossal d'interactions sociales, il en est de même pour les transactions économiques : en avril 2022, 63% de la population mondiale était connectée à Internet[23].

Avec des termes simples, on peut définir *la confiance* de la façon suivante : *« notre volonté d'être vulnérable aux actions des autres parce que nous croyons qu'ils ont de bonnes intentions et qu'ils se comporteront bien à notre égard.* »[24] Quand nous avons confiance en quelqu'un, nous attendons qu'il agisse dans un sens conforme à nos volontés. Le Professeur Alex Pentland, Directeur du Connection Science lab au MIT applique ce concept de confiance au secteur numérique[25] :

> *Human trust is understanding what a person's motivations are, and believing they've got your back. You can anticipate what they'll do. You know why they are acting the way they do. […] This is something that is forgotten very often in constructing digital systems. Data is the clearest example. I'm going to deliver this service to you, and then without really making it clear, we're going to sell your data on the side. That's a violation of trust. A consequence is that if I don't understand your business model and what you are offering me and what the value is to you, I can't trust you. It's that transparency in value, the relationship, and the motivations that are often left on the floor when people talk about digital systems. And that's, in many ways, the fundamental error. A breakdown in this understanding is a pretty good approximation for the situations I've seen where issues of trust come u*

En pratique, en 2021, seuls 3,5 Européens sur 10 affirment avoir confiance en Internet[26]. Et pourtant ils sont 80% à s'y connecter tous les jours. Les Français sont les plus méfiants (2 Français sur 10 confiants), les Polonais et les Grecques étant les plus confiants avec un score de 5,4/10. En 2018 aux États-Unis, 64% des adultes de plus de 65 ans affirmaient qu'Internet était une chose majoritairement positive pour la société. Cela représentait une baisse de 14 points par rapport aux 78% qui affirmaient la même chose en 2014[27].

La confiance dans Internet est un attribut difficile à évaluer à cause de la disparité des facteurs qui la conditionnent, et elle sera traitée plus en détail dans le dernier chapitre. Mais commençons à l'aborder ici. D'une part, les équipementiers connaissent très bien le sujet et proposent déjà un chiffrement en local, comme c'est le cas d'Apple à partir de l'iOS 8 et 9 qui chiffreraient localement et par défaut les données des utilisateurs, ce qui les rendraient inaccessibles à l'équipementier lui-même. Google propose

une solution similaire de chiffrement des données par défaut avec Android Marshmallow pour les terminaux qui supportent l'algorithme de chiffrement AES ;

D'autre part, à la suite des révélations de Snowden (2013), du scandale Facebook-Cambridge Analytica (2016), du vote de la *Nouvelle Loi anti-terroriste en Chine* (2015) et du *Cloud Act* aux États-Unis (2018) la question de la confiance envers certains systèmes de gouvernance a été longuement discutée et nous allons y revenir ultérieurement.

La confiance, l'adhésion de l'utilisateur est donc indispensable pour faire vivre Internet. L'infrastructure matérielle et les données sur lesquelles s'appuie Internet sont donc à protéger si l'on veut garder la confiance des utilisateurs, protéger et continuer à faire vivre les valeurs démocratiques dans le monde. La démocratie a toujours été l'apanage du vieux continent européen, d'où elle a été transmise aux États-Unis. Alors que les États-Unis ont depuis pris des décisions législatives contraires aux droits fondamentaux (maintien de la peine de mort ou de l'avortement, considéré illégal dans certains états), ou militaires (l'invasion d'Iraq), l'Europe en reste un fervent défenseur.

Comme évoqué précédemment, si Internet devait devenir le porte-parole de cette démocratie, la confiance des utilisateurs, quels qu'ils soient et où qu'ils soient, doit être sans faille. Entre le libéralisme américain poussé à l'extrême, au service de la création d'une puissance économique et militaire par la technologie, le régime autoritaire chinois qui se sert particulièrement des réseaux sociaux pour maintenir l'ordre en place et son pouvoir, et la Russie à l'esprit belligérant de contrôle de ses anciens territoires qui, pour ce faire, répand le désordre par la désinformation et la destruction, l'Europe s'érige en dernier lieu d'existence des droits fondamentaux. Elle reste peut-être la seule à les défendre encore.

Toutefois, les implications de l'actuel panorama géopolitique sont nombreuses pour l'Europe : les dépendances de l'Europe sont multiples et exacerbées par le conflit en Ukraine.

Cette Europe, qu'on peut qualifier de "colonie numérique des États-Unis et de la Chine" et dont on décrie souvent le retard technologique, saura-t-elle enfin prendre sa place entre ces trois pays susmentionnés à l'esprit fortement offensif ?

Les États-Unis : suprématie militaire et impérialisme technologique

À l'Ouest, aux États-Unis, berceau d'Internet, le *laissez-faire* d'un marché libre[28] et la manière dont l'antitrust y a été appliqué depuis les années 1970 ont ouvert la voie à la construction de monopoles technologiques. Plus récemment, ces monopoles ont été regroupés sous le nom de GAFAM (Google, Amazon, Facebook, Apple, Microsoft). L'économie est donc dominée par un nombre réduit d'acteurs surpuissants qui œuvrent à accroître les parts de marché qu'ils détiennent.

Tout au long du 20ème siècle, ces plateformes technologiques états-uniennes ont été protégées par un bouclier juridique conçu pour les sociétés Internet en vertu de la section 230 du *Communications Decency Act* (*CDA*) états-unien de 1996. Le *CDA* vise expressément à favoriser l'essor d'Internet, un internet bien différent de celui d'aujourd'hui, sans Facebook, ni Google, ni Twitter, ni Instagram. Mais il a été dépassé par la vague technologique, et ses failles juridiques évidentes ont été exploitées par les GAFAM pour leur propre intérêt. L'une de ces failles, la plus connue, résulte dans la distinction entre les "fournisseurs" de contenu (similaires aux journaux) et les "distributeurs" de contenu (similaire aux kiosques à journaux). Les distributeurs sont considérés comme des canaux passifs d'information et sont donc juridiquement responsables seulement de la publication et de la distribution des contenus, qu'ils sachent ou non que ceux-ci sont illégaux. Avec peu de contrôle et de médiation de la part du Gouvernement fédéral américain, les plateformes technologiques considérées comme des simples distributeurs sont en mesure de décider elles-mêmes de ce qui est autorisé ou non sur leurs plateformes, donc dans l'espace numérique, concentrant ainsi le pouvoir entre leurs mains. À titre d'exemple, en octobre 2020, les entreprises Facebook et Tweeter ont censuré une information publiée par *The New York Post* dénigrant le candidat Biden aux élections américaines[29]. Alors que plus de la moitié des internautes américains utilisent ces deux réseaux sociaux pour s'informer[30], cela a démontré une réelle ingérence de ces plateformes dans le processus d'élection américaine et leur aspiration à devenir les façonneurs d'opinion. Dans ces conditions, ces géants deviennent des puissances telles qu'il est difficile d'envisager une concurrence saine et loyale.

Aujourd'hui, avec la continuelle augmentation du trafic Internet, la donnée numérique devient le nouvel or mondial. Les États-Unis, après avoir permis la croissance exponentielle des GAFAM, en sont devenus les maîtres (notamment à travers les infrastructures Cloud). Cette grande quantité de données disponible presque gratuitement renforce leur puissance et leur emprise sur le monde. Le chiffrement des données aurait pu les freiner. Il n'en a rien été puisque le gouvernement états-unien ne s'est jamais défendu d'interférer avec la recherche universitaire en cryptographie ; il considère les algorithmes et les logiciels de chiffrement comme des munitions.

C'est originellement aux États-Unis que les guerres de cryptographie ont commencé dans les années 1970. Depuis, diverses tentatives montrent la volonté des États-Unis de s'assurer une fenêtre d'écoute : la puce Clipper[31] voulue par le président Clinton dans les années 1990, le séquestre de clé (*key escrow*)[32], la compromission des solutions protégées. Les vulnérabilités ainsi créées n'ont pas tardé à être exploitées. La vulnérabilité FREAK [33] permet encore aujourd'hui des attaques Man-in-the-Middle (l'homme du milieu) en raison des mauvaises décisions de sécurité prises vingt ans auparavant. En 2013, les révélations de l'ancien agent de The National Security Agency des États-Unis (NSA), Edward Snowden, confirment ces agissements et portent le dernier coup aux ruines de la confiance des Occidentaux dans les agissements des Gouvernements états-unien et britannique. Une deuxième guerre du code a commencé. *The Guardian*, à qui Snowden a confié ses documents, dévoile l'existence d'un budget de plus de 250 millions de dollars annuels[34] alloués à la NSA pendant plus de 10 ans ; et ce, dans un but de surveillance et d'écoute non seulement des états étrangers, une pratique courante, mais également ses

Classified briefings between the NSA and GCHQ celebrate their success at "defeating network security and privacy".

Capture d'écran d'une présentation du GCHQ

Photo :

The Guardian 2013

propres citoyens. L'agence de sécurité britannique, The Government Communications Headquarters (GCHQ), était également impliqué.

Écouter ses alliés et ses ennemis, depuis la Deuxième Guerre mondiale, est chose courante, les Britanniques étant reconnus comme très efficaces en la matière. Ce qui était en revanche nouveau c'était l'acharnement technologique afin de s'assurer une fenêtre d'écoute[35]. La stratégie, car il s'agit bien d'une vraie stratégie composée de plusieurs projets (Prism, Bullrun, Sigdev, Edgehill), un budget conséquent et un haut niveau de confidentialité, devait permettre l'écoute d'informations chiffrées transitant par Internet (câbles sous-marins) ou stockées par de fournisseurs de messagerie électronique : Microsoft (Outlook et Skype), Facebook, Yahoo, Google, Hotmail, Apple, Verizon, etc. Il s'agit d'un vrai assaut organisé et méthodique pendant plus de 10 ans contre ce que la NSA et le GCHQ considèrent comme « *the price of admission for the US to maintain unrestricted access to and use of cyberspace* »[36]. Sous le couvert de la lutte contre le terrorisme pour la NSA et de la maîtrise du cyberspace pour le GSHQ, les deux agences ont fait voler en éclats la confiance qu'avaient les millions d'utilisateurs d'Internet. Les entités privées et publiques, les entreprises et les états convaincus que leurs secrets, leurs données personnelles, leurs données de santé, bancaires, étaient à l'abri des regards des criminels et des gouvernements en été désabusés.

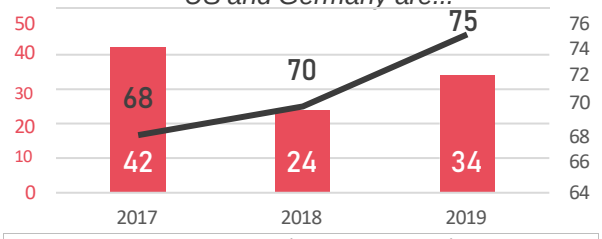
La série d'initiatives mis en place par la NSA peut créer des vulnérabilités de sécurité, d'autant plus qu'il ne s'agit pas d'un phénomène isolé. Entre 2017 et 2019, le projet de restructuration d'un quartier à Toronto a été confié à une filiale de Google, Sidewalks Labs[37]. Dangereusement proche du système de surveillance chinois, avec des pénalités et des récompenses, le projet appelé "une bombe contre la démocratie" a été finalement abandonné par Google suite aux enquêtes menées par la ville canadienne. Facebook, de son côté, a été déjà condamné en 2021 par l'état de l'Illinois pour utilisation illégale de données biométriques et doit faire face cette année à des accusations similaires de la part de l'état du Texas[38].

La Maison Blanche finit par reconnaître que les programmes de surveillance de la NSA n'ont pas permis d'arrêter le moindre terroriste. Pour cela, Edward Snowden les considère plutôt comme des outils de manipulation des masses, d'espionnage économique et d'influence sociale aux dépens de la confidentialité, donc de la démocratie et finalement de la sécurité.

34%

des Allemands pensent que les relations avec les États-Unis sont mauvaises

Source : Atlantik-Brücke 2019



Note:
Moins de 5% ne savent pas, ils n'ont pas été représentés.
Données: Sondages réalisés par Pew Research Center aux États-Unis entre 17-22 septembre 2019 (T4) et par KörberStiftung en Allemagne entre 9-28 septembre 2019.

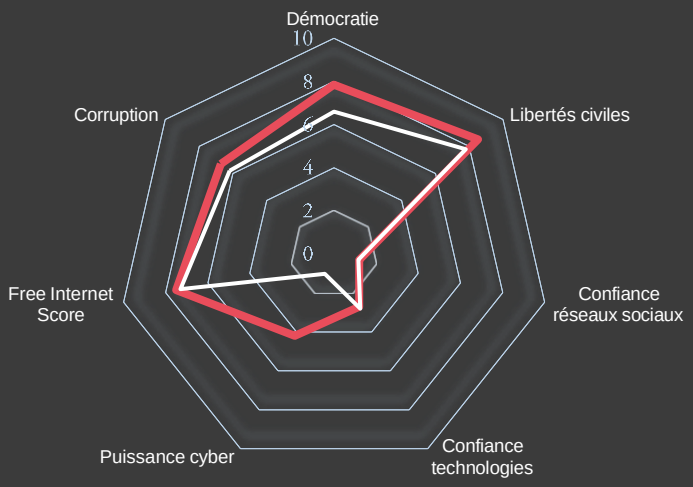
Bien que la coopération entre les États-Unis et la Grande-Bretagne ait fonctionné, l'effet obtenu s'est révélé contraire à leur vision. Afin de protéger les données contre de telles écoutes, les industriels ont renforcé la protection des données en transit et au repos en imposant du chiffrement de bout-en-bout par défaut (WhatsApp, Signal), ou entre correspondants utilisant la même solution (Office 365, ProtonMail), ou encore en rendant certains systèmes complètement muets (le dernier iOS d'Apple).

En Europe, la confiance envers les États-Unis connaît des fluctuations inédites, surtout après l'élection du président Donald Trump. Chez les citoyens allemands, l'appréciation est entièrement bouleversée dans le laps de seulement deux ans. À la question « *Comment évaluez-vous actuellement les relations entre l'Allemagne et les États-Unis ?* », à peine 1,8% pensent que la relation est plutôt positive (*sehr positiv*), 8,6% très positive (*sehr positiv*) et 5% ne savent pas (*weiss nicht*). 33,9% pensent que la relation est très négative (*sehr negativ*)[39].

La question d'une autonomie stratégique sur les technologies commence donc à faire son chemin dans les agendas européens. Les Chinois, eux, choisissent de mettre en place une stratégie plus radicale.

2021

—États-Unis* —Europe**



"By deliberately undermining online security in a short-sighted effort to eavesdrop, the NSA is undermining the very fabric of the internet"
Bruce Schneier, expert en chiffrement à Harvard's Berkman Centre for Internet and Society

"The reality is the U.S. private sector has eclipsed the government, which in some ways that can be good. The private sector can move with greater agility than the government".
Jim Langevin, D-R.I., chairman of the House Armed Services Committee's on Intelligence and Emerging Threats and Capabilities

**Les données Europe représentent la Moyenne des données de l'Allemagne et de la Hongrie. Toutes les données sont exprimées sur une échelle de 1 à 10.

*Données et ressources :

ECONOMIST INTELLIGENCE (EIU) - *Democracy Index 2021. The China Challenge* ©2022
TRANSPARENCY INTERNATIONAL – *Corruption Perception Index 2021* ©2022
IPSOS - *Global Trustworthiness Monitor. Is Trust in Crisis?* ©2021
BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS – *National Cyber Power Index* ©2022
FREEDOM HOUSE – *United States Country Overview (Internet Freedom Score)* ©2021

La Chine : un autoritarisme qui roule sur la *Belt and Road Initiative*[40]

Dès 1998, la Chine décide de protéger et d'isoler sa population de l'influence états-unienne et installe le *Great Firewall* (appelé également *Golden Shield Project*), signe un contrat de licence avec Microsoft pour un Cloud national exclusif, investit massivement dans le remplacement des technologies états-uniennes par des solutions chinoises et décrète l'IA et la 5G en tant que priorités nationales soutenues lourdement, politiquement et économiquement, par le Parti Populaire Chinois.

En 2015 avec la *Nouvelle loi anti-terroriste*, la Chine entérine l'obligation de donner accès aux systèmes informatiques et aux clés de chiffrement des entreprises étrangères au Gouvernement chinois. C'est là un aveu à peine voilé des intentions d'écoute, d'espionnage et de vol de propriété intellectuelle d'un régime autoritaire qui a su faire appel à la technologie pour éliminer ses opposants politiques.

Les caméras de surveillance, l'intelligence artificielle, le détournement du trafic Internet[41], la biométrie (les échantillons de voix et l'ADN) et le profilage par reconnaissance faciale ont été utilisés à grande échelle afin de surveiller les Ouïgours, ou de mettre en œuvre le crédit social dans le but de récompenser ou de pénaliser les comportements et les actions des entreprises[42]. D'une part, cela va de pair avec l'accélération des tensions entre ses propres champions technologiques (Alibaba, Baidu, Tencent, etc.), tout comme aux États-Unis par ailleurs. Mais le Gouvernement chinois a su reprendre promptement le contrôle en administrant une amende de 2,3 milliards d'euros à Alibaba pour abus de position dominante[43] et en l'obligeant ainsi à ralentir le pas. Autrement dit, en Chine, tout est dirigé par l'unique parti, car la technologie est un élément clé de sa politique de surveillance intérieure et de domination extérieure qui passe par la Belt and Road Initiative dont la Route de la soie numérique fait partie.

D'autre part, la Chine se bat depuis les années 2000 pour reformer le protocole IP à la base d'Internet afin de s'assurer plus de contrôle et de surveillance. Elle soutient le développement d'un nouveau protocole, New IP, qui permettrait le contrôle total du réseau. Pour cela, la Chine se sert d'un prétexte : l'architecture décentralisée d'Internet serait à l'origine de ses lacunes supposées. À travers Huawei et l'explosion des objets connectés (IoT) à venir, cela pourrait être réalisable si la solution technologique chinoise (New IP) était acceptée à travers le monde. Pour le Gouvernement socialiste Internet doit servir les intérêts du parti[44] :

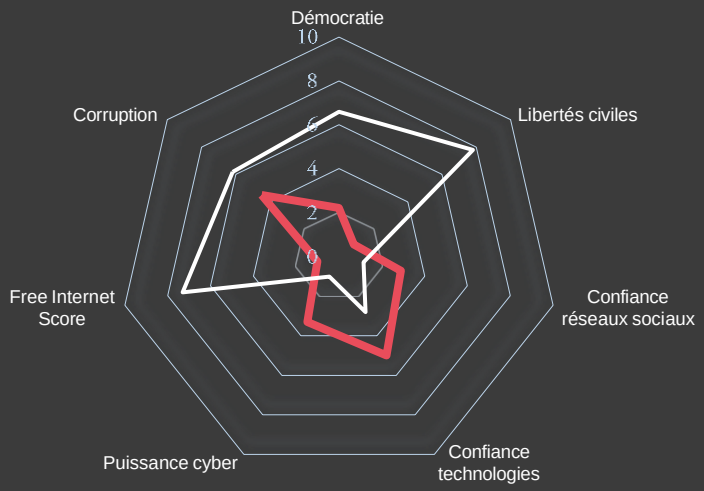
> *« La conception de l'infrastructure et des normes de l'Internet [est considérée] comme un élément central de sa politique étrangère numérique, et ses outils de censure comme une démonstration de faisabilité pour un Internet plus efficace, qu'il sera en mesure d'exporter. »*

La diplomatie numérique étant un autre chemin pour parvenir à ses fins de domination, la Chine soutient activement une alternative à l'alliance américaine *Clean Network* mis en place par le département d'État pour bloquer les technologies chinoises aux États-Unis, TikTok compris. La stratégie n'est autre qu'une stratégie de guerre profondément ancrée dans la culture chinoise, devenue une maxime pour les Chinois. Elle consiste à maîtriser tous les points d'accès non exploités. Dans le cyberespace, cela se traduit par des efforts considérables soutenus par le Parti communiste chinois à multiplier les *Points of Présence* (PoP)[45] dans des territoires démocratiques clé. China Telecom (CT) détenue par l'état chinois a pénétré les réseaux nord-américains au début des années 2000 et s'est depuis développé pour avoir 10 PoP, huit aux États-Unis et deux au Canada, desservant les deux côtes et tous les principaux points d'échange aux États-Unis. Grâce à cette présence, une grande partie du trafic Internet de l'Occident[46] est dirigée vers des serveurs et des télécommunications dont le propriétaire et exploitant est le Parti chinois. Ultérieurement, c'est à travers la diffusion de caméras de télésurveillance, à l'exemple de Hikvision et Dahua (+50% du marché mondial en 2020[47]), que les données sont collectées. La dernière entreprise en date est Huawei, désormais très bien implantée dans les réseaux de télécommunications européens et états-uniens depuis la 3G. À travers ces entreprises et tant d'autres encore, en 2022 le Gouvernement chinois supervise 3949 PoP dans le monde. Cela lui permet de gérer et d'interférer avec une grande partie du trafic Internet.

États-Uniens et Chinois utilisent donc Internet pour récupérer le plus de données possible. Edward Snowden décrivait encore plus intensément ce processus. Depuis toujours la donnée est le carburant du renseignement, qui, à son tour, représente un avantage tactique. Lors d'une vidéo de mars 2022, Snowden met en avant, de façon très claire, le lien entre confidentialité, sécurité et surveillance :

2021

—Chine* —Europe**



**Les données Europe représentent la Moyenne des données de l'Allemagne et de la Hongrie. Toutes les données sont exprimées sur une échelle de 1 à 10.

"Leave no access point unexploited"
China's maxim

"If our party cannot traverse the hurdle represented by the Internet, it cannot traverse the hurdle of remaining in power for the long term. […] At present, cyberspace has become a new field of competition for global governance, and we must […] push China's proposition of Internet governance toward becoming an international consensus."
General Secretary XI JINPING's strategic thinking, 2017

*Données et ressources :

ECONOMIST (EIU) - *Democracy Index 2021. The China Challenge* ©2022
TRANSPARENCY INTERNATIONAL – *Corruption Perception Index 2021* ©2022
IPSOS - *Global Trustworthiness Monitor. Is Trust in Crisis?* ©2021
BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS – *National Cyber Power Index* ©2022
FREEDOM HOUSE – *China Country Overview (Internet Freedom Score)* ©2021

“LES GOUVERNEMENTS CONSIDERENT LE PIRATAGE COMME ETANT LEGAL TANT QUE CE SONT EUX QUI LE PRATIQUENT.”

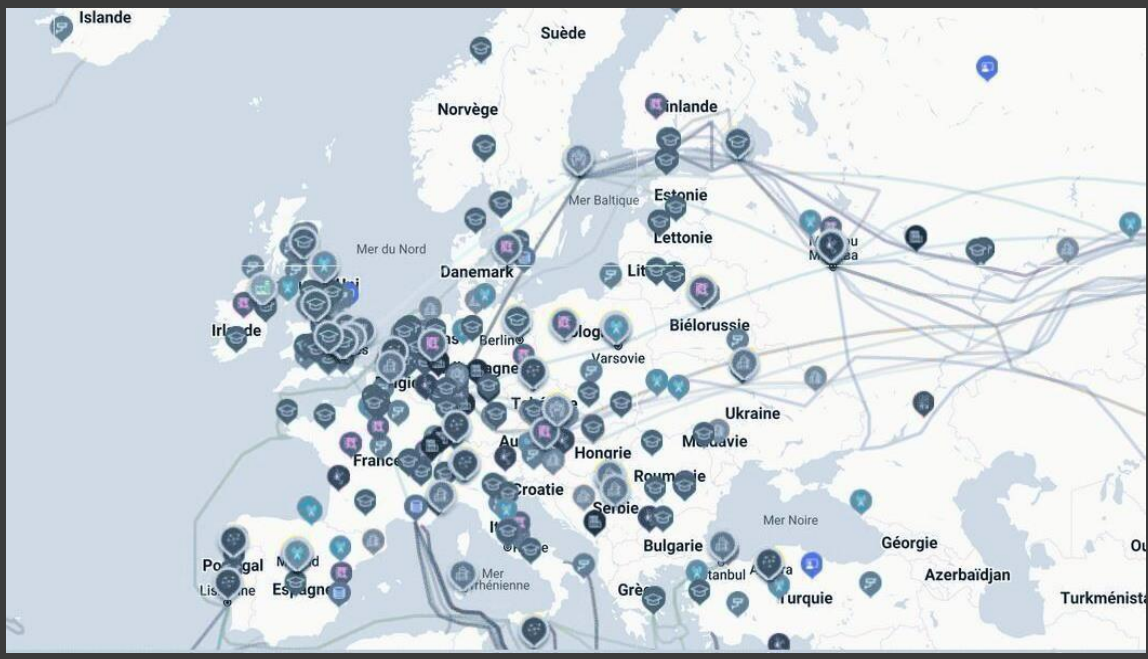
Edward Snowden[49]

“[Chinese companies] are going to continue to play a vital role in the ways in which governments, companies and citizens around the world connect with one another.

At the same time, however, it is important to recognise that the activities of these companies are not purely commercial, and in some circumstances risk mitigation is needed. The CCP’s own policies and official statements make it clear that it perceives the expansion of Chinese technology companies as a crucial component of its wider project of ideological and geopolitical expansion. The CCP committees embedded within the tech companies and the close ties (whether through direct ownership, legal obligations or financing agreements including loans and lucrative contracts) between the companies and the Chinese government make it difficult for them to be politically neutral actors, as much as some of the companies might prefer this. There is also a legitimate question about whether global consumers should demand greater scrutiny of Chinese technology firms that facilitate human rights abuses in China and elsewhere.

Governments around the world are struggling with the political and security implications of working with Chinese corporations, particularly in areas such as critical infrastructure, for example in 5G, and in collaborative research partnerships that might involve sensitive or dual-use technologies. Part of this struggle is due to a lack of in-depth understanding of the unique party-state environment that shapes, limits and drives the global behaviour of Chinese companies.”[50]

1154



1154 points de présence technologique chinoise en Europe (3948 dans le monde)

“Si personne ne sait ce que vous faites, personne ne peut prendre des mesures contre vous. Personne ne peut vous rendre vulnérable. Si vous êtes surveillé, documenté dans tous vos déplacements, non seulement vous perdez en confidentialité, mais vous perdez aussi en sécurité.”

EDWARD SNOWDEN
2021

La Russie : déstabilisation et discréditation des démocraties par mercenaires interposés

Voisine de l'Europe à l'Est, la Russie est à l'origine du retour de la guerre de forte intensité sur le sol européen suite à son invasion de l'Ukraine. Elle constitue aujourd'hui une menace directe, sur les plans militaire, économique (énergie, alimentation), cyber et politique (par la désinformation, par exemple). Dans l'espace cyber, la Russie mène une lutte offensive de façon anonyme. Elle manœuvre à travers des organisations "proxy" qui revendiquent leurs actions et leur position pro-russes[51]. Cela permet à la fois pour ces groupes de se positionner dans l'espace cyber et d'afficher leur succès. Mais la Russie n'assume pas ouvertement ces activités qui lui sont pourtant favorables en termes d'influence. Selon l'analyse de Tom Burt, vice-président de Microsoft en charge de la sécurité client, le lien avec l'offensive russe est évident car elles ont été coordonnées avec les attaques terrestres[52] :

> *The attacks have not only degraded the systems of institutions in Ukraine but have also sought to disrupt people's access to reliable information and critical life services on which civilians depend, and have attempted to shake confidence in the country's leadership. We have also observed limited espionage attack activity involving NATO member states, and some disinformation activity.*

En début d'année 2022, le groupe russe Conti[53] se revendique ouvertement proche du Kremlin et mène des attaques visant à déstabiliser des États principalement démocratiques. Suite au soutien officiel du Costa Rica à l'Ukraine, le pays subit depuis le mois d'avril une attaque cyber par rançongiciel imposant la mise en place de l'état d'urgence. Vingt-sept institutions ont été piratées dont le Ministère des finances : cela a eu comme conséquence l'absence de versement des salaires pour des milliers de fonctionnaires. Face au refus de payer la rançon de dix millions de dollars, le groupe de hackers russes a revendiqué l'attaque en toute impunité et il assume sa menace de renverser le gouvernement du Costa Rica. Le groupe russe n'est pas à son premier coup d'essai. En 2021 The Health Service Exécutive irlandais avait subi une attaque par rançongiciel exigeant vingt millions de dollars. Refusant de payer, le coût de l'attaque s'éleva à plus de cent millions d'euros.

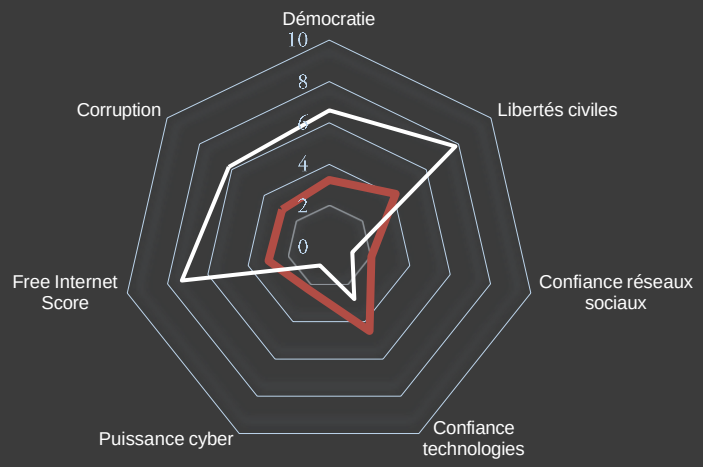
Cela concerne également les pays européens. Le 27 juin 2022[54] la Lituanie a dû faire face à une vague d'attaques par déni de service (DDoS), suite à l'application par le pays des sanctions européennes contre la Russie. Cette fois c'est le groupe russe Killnet qui s'en est pris aux institutions lituaniennes, en provoquant l'arrêt des services fiscaux et la délivrance de passeports pendant plusieurs heures. Cette attaque démontre la nécessité d'une coordination européenne dans la cyberdéfense afin de faire appliquer les lois européennes votées. En effet, si un seul pays a été attaqué, il s'agit bien d'une offensive contre une loi européenne et son application physique à sa frontière.

Mais la Russie est offensive même sans "sous-traitant". En effet certaines attaques non revendiquées ont profité uniquement à la Russie. Le jour de l'invasion russe sur le sol ukrainien, le réseau de satellites KA-SAT a été visé par une cyberattaque par l'exploitation d'une faille VPN du réseau ViaSat. Par la paralysie des satellites, cette manœuvre visant les administrations et les entreprises ukrainiennes a touché le territoire de l'UE en raison de son expansion. Le chef de la diplomatie européenne Josep Borrell a réagi en annonçant publiquement la toute première attribution de la part de l'UE :« *pour la première fois, au niveau de l'Union européenne, nous attribuons cette attaque à un acteur étatique, à la Fédération de Russie* ». Si le Kremlin ne revendique pas l'attaque, il faut noter qu'aucun état n'assume une offensive cyber. Il n'est pas clair si l'UE fut un objectif second ou une victime collatérale d'une cyberattaque incontrôlée.

Que ces attaques cyber soient voulues ou non, elles permettent à la Russie d'affaiblir les pays européens. Cette faiblesse peut profiter ensuite aux autres compétiteurs sans que ce résultat soit le fruit de leur manœuvre qu'ils devraient diplomatiquement assumer. L'affaire Pegasus a suscité des tensions diplomatiques entre certains gouvernements pourtant alliés et partenaires à bien des égards. Les manœuvres cyber russes et des activistes pro russes contre l'Europe sont d'autant plus néfastes qu'elles profitent aux autres acteurs cyber. Ceux-ci profitent de la division européenne sans prendre aucun risque. L'attaque contre KA-SAT qui fut attribuée par l'UE, la Grande Bretagne et les États-Unis à la Russie n'a pour autant pas fait l'objet d'une sanction contre le Kremlin. Si l'activité cyber-offensive russe reste discrète, elle ne semble pas pour autant trop inquiétée. Les activistes pro-russes, en revanche, sont poursuivis par les états. Dans ce cas, la coordination et coopération transeuropéenne peuvent se révéler un atout majeur.

2021

—Russie* —Europe**



**Les données Europe représentent la Moyenne des données de l'Allemagne et de la Hongrie. Toutes les données sont exprimées sur une échelle de 1 à 10.

"L'équipe Conti annonce officiellement un soutien total au gouvernement russe. Si quelqu'un décide d'organiser une cyberattaque ou des activités de guerre contre la Russie, nous allons utiliser toutes nos ressources possibles pour riposter."
Groupe Conti - Phonandroid

"This is the first time I can recall a ransomware attack resulting in a national emergency [Costa Rica] being declared."
Brett Callow – Threat analyst, Emsisoft

*Données et ressources :

ECONOMIST (EIU) - *Democracy Index 2021*. *The China Challenge* ©2022
TRANSPARENCY INTERNATIONAL – *Corruption Perception Index 2021* ©2022
IPSOS - *Global Trustworthiness Monitor*. *Is Trust in Crisis?* ©2021
BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS – *National Cyber Power Index* ©2022
FREEDOM HOUSE – *Russia Country Overview (Internet Freedom Score)* ©2021

1.2. L'Europe victime de sa diversité et de ses dépendances

La politique de cybersécurité est une des préoccupations indirectes de l'Union Européenne (UE) depuis le début des années 1990, ce qui correspond au développement d'Internet. Cette politique trouve ses origines dans le domaine de la sécurité informatique et de l'information, puis elle s'est étendue vers une politique de cybersécurité globale réunissant non seulement la cybercriminalité, mais aussi la protection des infrastructures critiques et, plus récemment, la cyberdéfense. Dans les années 1990, les technologies de l'information et de la communication ont été considérées essentielles à la poursuite du développement économique et à l'achèvement du marché unique [55] et son association à une politique économique cohérente apparaît très tôt. L'UE aborde donc la cybersécurité non pas du point de vue sécuritaire (prérogative exclusive des États Membres), mais du point de vue économique, juridique et social, qui sont ses domaines d'action[56]. Il y a donc une définition des règles de concurrence et des accords commerciaux (domaines exclusifs) ou encore des modalités du marché unique, ainsi que de nombreuses mesures garantissant la protection des consommateurs, la cohésion économique, sociale et territoriale, l'emploi et les affaires sociales, la justice et les droits fondamentaux, les réseaux transeuropéens. Ce n'est que vers la fin des années 1990 que l'UE rajoute une logique de sécurité à la logique économique déjà existante, sous l'impulsion de l'intérêt de la communauté internationale pour la criminalité informatique[57], qu'il s'agisse de contenus illégaux et préjudiciables sur Internet, ou de la criminalité liée à la haute technologie. Il s'ensuit jusqu'au milieu des années 2000 une multitude d'instruments et d'initiatives non juridiquement contraignants[58] dans le but de sensibiliser les États membres (EM) et de susciter des préoccupations communes

En dépit de cette évolution, la cybersécurité n'est pas devenue une priorité absolue en matière de sécurité avant le milieu des années 2000 (même la *Stratégie européenne de sécurité* de 2003 n'en parlait pas). Ce changement est apparu avec la prise de conscience de la vulnérabilité grandissante aux attaques extérieures des systèmes et technologies de l'information, notamment aux attaques de nature terroriste[59]. Ce changement a conduit à deux résultats principaux : d'une part, le passage d'instruments non juridiquement contraignants à des instruments juridiquement contraignants, comme ce fut le cas de la décision-cadre du Conseil relative aux attaques visant les systèmes d'information[60] (l'ancêtre de la *Directive NIS*) ; et d'autre part, le renforcement de l'idée de cohérence comme condition d'efficacité et comme résultat souhaitable à atteindre au niveau de l'UE. Ces deux résultats résultent de la perception que la criminalité organisée et le terrorisme représentaient une menace évidente pour la réalisation d'une société à l'information plus sûre. Cette société était mise en péril par l'existence de lacunes et de différences, voire de fossés, entre les législations des EM, ce qui la rendait instable. Le niveau national a

été présenté comme insuffisamment équipé pour répondre de manière adéquate à ces menaces de plus en plus transnationales. C'est ainsi qu'une approche commune développée au niveau de l'UE, fondée sur le rapprochement entre les EM, a été présentée comme une réponse nécessaire[61]. Depuis lors, un effort clair a été fait pour consolider les activités de l'UE dans ce domaine, notamment en sensibilisant le public, en investissant dans une stratégie globale et cohérente et dans les instruments correspondants, tels que la *Directive NIS* et le *Cybersecurity Act*.

La notion de cohérence est au cœur même du projet européen. Réussir à faire converger plusieurs EM vers une vision et des missions communes ne peut se faire sans cohérence ou sans consistance (dans l'acceptation anglaise du terme d'absence de contradiction). Selon la Commission européenne (CE), la cohérence doit être assimilée à une "meilleure planification stratégique", à une "meilleure exécution et un meilleur impact" et à une "meilleure coopération"[62].

Bien que les concepts de *cohérence* et de *consistance* soient relativement clairs, ces concepts restent pourtant des notions abstraites difficiles à mettre en œuvre à une si grande échelle que celle de l'UE., selon l'avis d'un représentant d'une organisation européennes que nous avons interviewé en novembre :

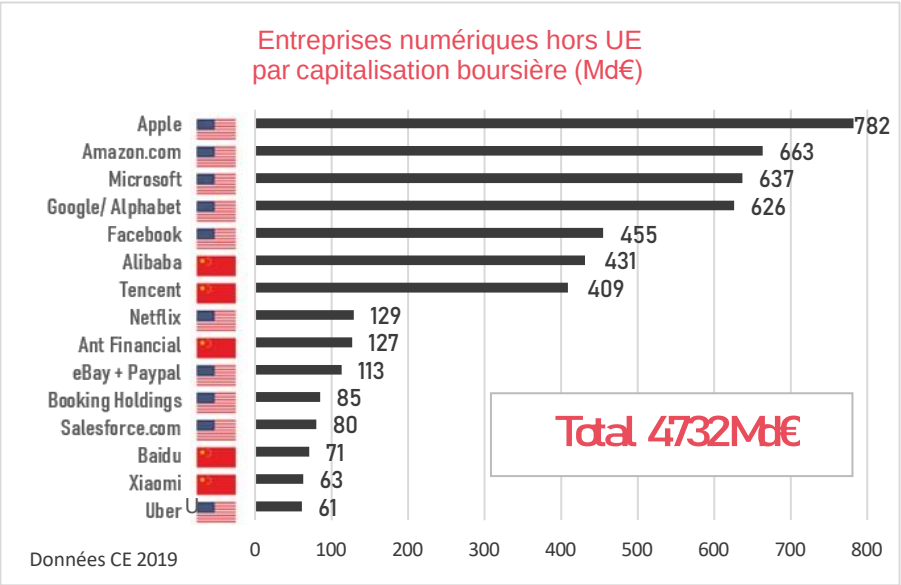
> *Sur le papier, ils sont tous d'accord avec la stratégie d'autonomie, mais lorsqu'il faut faire des choix, cela revient à comment chacun voit les choses. […] Les Américains font des offres qu'il est difficile de refuser.*

Évaluer le travail en commun des Européens dans la cybersécurité, reviendrait à évaluer la cohérence et la consistance de tous les acteurs dans ce domaine. Cela implique d'examiner à la fois la coordination institutionnelle et l'existence (ou non) de points de vue partagés sur la sécurité, les menaces et les réponses potentielles à travers les opérations concrètes. Autrement dit, considérer à la fois la rhétorique et la pratique.

Aussi, sur le terrain, les frontières sémantiques se montrent assez floues. Concrètement, dans le domaine de la sécurité et de la cybersécurité, l'UE a fait des progrès considérables en termes de cohérence : promotion de politiques communes, mise en œuvre de procédures pour développer des instruments communs, et d'encouragement des acteurs de la sécurité à travailler ensemble. Toutefois, les thématiques des conflits interinstitutionnels et inter-agences, de chevauchement de prérogatives et de manque de communication font preuve d'un manque de consistance qui devrait interpeller. Car il est désormais urgent de rattraper le retard.

L'étendue du retard technologique

Aujourd'hui en Europe, les solutions technologiques sont majoritairement états-uniennes, quand elles ne sont pas chinoises. Rien qu'en regardant dans les bureaux d'une administration publique en France, nous



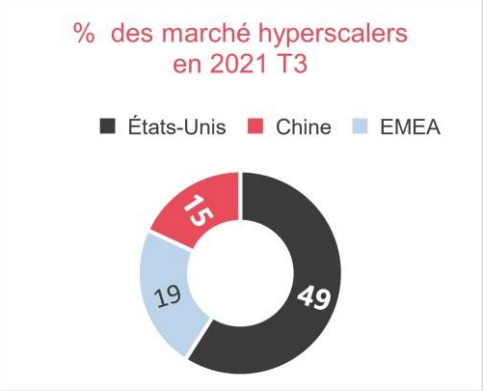
y trouverons des ordinateurs chinois ou états-uniens (Lenovo, Microsoft, IBM, Dell ou Apple), des puces Intel fabriquées aux États-Unis, un réseau 5G du chinois Huawei, des smartphones d'Apple, Google, Huawei, des applications bureautiques Microsoft ou Salesforce, de la messagerie électronique avec Google, Yahoo, Outlook, des réseaux sociaux américains ou chinois (Facebook, Instagram, TikTok) et des données stockées dans des bases de données d'Amazon, de Microsoft, d'IBM, etc. Ce n'est pas un hasard puisqu'il s'agit des 15 premières entreprises de technologies non européennes dans le monde (cf. graphique au-dessus)[63]. Toutes les générations d'Européens à commencer avec celles des années 1990 ont grandi, étudié, travaillé quotidiennement, avec ces solutions, à la maison comme au travail. Le pack Office de Microsoft est l'un des très peu dénominateurs communs de la myriade de plus de 30 000 des agents de l'UE, au point qu'il n'a pas été possible d'en changer, même si l'alternative était moins chère[64].

Au niveau global, 4 entreprises européennes font partie du classement des meilleures entreprises numériques en termes de revenus établi par Forbes en 2019 : les allemands Deutsche Telekom et SAP (19ème et 22ème respectivement), l'espagnol Telefónica (23ème) et le français Orange (27ème)[65]. Trois parmi ces quatre entreprises sont des entreprises de télécommunications. Pas étonnant, car l'excellence des opérateurs européens est une réalité historique. Au moment de la 3G, l'Europe était au-devant de la scène internationale avec un podium majoritairement européen : Ericsson, Nokia-Siemens, Huawei, Alcatel-Lucent et ZTE[66]. En 20 ans les équipementiers européens sont passés de 5 à 2 suite à des acquisitions spectaculaires, mais aucun géant européen des télécom n'en est résulté.

64%

hyperscalers étaient chinois ou états-uniens au 3ème trimestre 2021

Données : SdxCentral 2021



Par la suite, parmi les opérateurs, on note la chute de Telefónica, de Vodafone et la montée en puissance de Deutsche Telekom (Annexe I). En absence de solutions cloud européennes fiables et de grande capacité, la 5G, dans son implémentation autonome (*stand alone*), devra trouver des solutions européennes pour sécuriser et protéger l'information des citoyens et des entreprises européennes. Quant à l'IA et à la blockchain, l'Europe entretient un retard de plus en plus conséquent en ce qui concerne les investissements et le développement de solutions, et accumule un déficit de 10 milliards d'euros qui seraient nécessaires pour rester compétitive, selon la Banque Européenne d'Investissement [67]. Il est désormais clair qu'aucun champion national des nouvelles technologies n'a réussi à s'imposer au niveau européen, et encore moins au niveau mondial. Les données des Européens sont aujourd'hui sur des end-points (ordinateurs, smartphones), dans des plateformes edge (tours 4G, serveurs institutionnels) et, la plus grande partie, dans des data centers étrangers peu soucieux de la confidentialité. Au troisième trimestre 2021, le monde comptait plus de 700 *hyperscale data centers*, ou *hyperscalers* (des data centers de plus de 5000 serveurs) dont 49% sont États-Uniens et 34% sont Chinois, Japonais, Allemands, Britanniques ou Australiens[68].

Plusieurs raisons ont nourri ce retard : celles-ci ne sont pas que technologiques, mais surtout stratégiques et concernent la gouvernance géopolitique. Tout d'abord, la situation européenne n'est pas une surprise de point de vue culturel et historique. Berceau de l'État de Droit et des libertés individuelles, l'Europe, ni union ni état fédéral, est une entité administrative unique au monde, créée en 1948, dépourvue de toute velléité à devenir une puissance mondiale. Elle a été fondée avec un objectif principalement économique et pacifique : développer un marché commun et faciliter le libre-échange de personnes et de marchandises entre ses états membres. Par le moyen d'un attirail règlementaire conséquent, l'Europe assure, bien ou mal, un marché régulé pour la libre circulation des marchandises et des services entre les États Membres. Mais cette tendance est en train de changer ces dernières années.

En conséquence, l'UE a mis sur la table d'importantes ressources réglementaires et financières pour soutenir la transition numérique des États membres dans un marché qu'elle veut libre et équitable, ce qui ne peut aujourd'hui passer que par un marché régulé. De point de vue technologique, la recherche

européenne a toujours été active et efficace. Le *World Wide Web* est né dans les bureaux du Centre Européen pour la Recherche Nucléaire (CERN) et a permis les échanges entres les milliers de scientifiques de sa communauté. Dans le domaine de la cybersécurité, l'Europe domine le classement des meilleurs 20 antivirus au monde : Bitdefender (Roumanie), Avast, Trustport et AVG (République Tchèque), Eset NOD32 (Slovaquie), Avira et G-Data (Allemagne), F-Secure (Finlande), Panda (Éspagne), F-Prot (Islande), Sophos et Comodo (Grande-Bretagne).

Des avancées importantes ont été faites dans le domaine de la réglementation qui prouvent que l'Europe est en avance sur le plan réglementaire par rapport aux autres acteurs internationaux : « *Disparition du "roaming", protection des données à caractère personnel et donc des consommateurs, attribution de fréquences de radiocommunication et de communication sans fil au niveau européen, harmonisation des règles de sécurité pour les entreprises, fin du géo blocage, création d'un véritable espace européen de la donnée […], harmonisation des règles de réversibilité pour les opérateurs du numérique, détermination d'un régime de responsabilité harmonisé des divers acteurs du numérique, éditions de règles et de préconisations pour la rédaction des contrats de cloud computing, modification du droit d'auteur afin de mieux protéger les éditeurs de contenus, adoption du principe de neutralité de l'Internet, harmonis droit de l'informatique, etc.* »[69]. Avec le programme *Digital Compass 2030*, l'UE met la barre encore plus haut en formulant des ambitions à l'horizon 2030. Ces ambitions sont claires : tous les foyers de l'UE doivent disposer d'une connectivité gigabit, toutes les zones peuplées seront couvertes par la 5G, 10 000 nœuds périphériques hautement sécurisés et neutres pour le climat seront déployés, 75% des entreprises européennes doivent adopter les services de *cloud computing*, le *big data* et l'IA, plus de 90% des PME doivent atteindre au moins un niveau d'intensité numérique de base et le nombre de licornes européennes devra doubler. L'arsenal règlementaire censé réguler et protéger le marché européen des nouvelles technologies est déjà considérable : le *Règlement général sur la protection des données personnelles*, (*RGPD*), *The Path to the Digital Decade* (*Digital Compass 2030*), la *Directive NIS*, la *Directive DORA*, *Chips Act*, *Digital Markets Act*, *Digital Services Act, Cybersecurity Act,* la *Directive NIS2,* le *Cyber Resilience Act*, la *Directive CER* (Critical Entities Resilience), *Data Governance Act*, *AI Act*, etc.

Imaginons un monde de prospérité et paix relative, de croissance et de grandes avancées technologiques nourrissant un marché gouverné par de solides institution et, renforcé par de normes internationales. C'était notre monde après la chute du mur de Berlin. S'intéresser à qui possède la technologie, l'infrastructure aurait été secondaire. Mais cette conquête technologique, nourrie par la crise financière de 2008 qui a permis l'accumulation de liquidités dans les caisses des entreprises et des états, permet à des acteurs étatiques unipolaires de transformer les interdépendances de leurs ennemis en vulnérabilités. C'est ainsi que la protection de l'information devient de plus en plus un élément non seulement de compétitivité, mais un pilier indispensable à la sécurité des états. Et l'arrivée, pas si lointaine, des ordinateurs quantiques, ne fera qu'accélérer cette conquête.

Il est évident que les ambitions numériques à l'horizon 2030 vont considérablement élargir la surface d'attaque européenne. Toutefois, le marché de la cybersécurité est, lui aussi, majoritairement américain : Palo Alto, Cisco, IBM, Symantec, MacAfee, Microsoft, Amazon, FireEye, Imperva, Fortinet, CyberArk., etc. Le rapport *Repenser la défense face aux crises du 21ème siècle* publié par Bernard Cazeneuve et Nicolas.Baverez souligne que 80% des outils de cybersécurité en France étaient états-uniens ou israéliens en 2021. Bien que consciente de la maturité cyber très hétérogène des États Membres, qui représente un risque pour la sécurité des réseaux et des données, l'UE se doit de composer avec l'absence de champions domestiques dans la cybersécurité. Accusant un retard technologique irrécupérable, et en championne de la démocratie, l'Europe n'hésite pas à utiliser les outils démocratiques à sa portée : l'outil réglementaire, les directives. En 2018, l'UE met en place le *Règlement général sur la protection des données personnelles*. Il s'agit de la seule obligation réglementaire en vigueur à ce jour concernant tous les acteurs traitant les données personnelles des Européens.

Mais les vulnérabilités de l'Europe vis-à-vis des États-Unis sont nombreuses, et pas seulement technologiques. Dans le projet du conglomérat militaro-industriel états-unien qui agit de plus en plus sans l'accord des gouvernements américains, il y a peu de place pour des alliances et des amitiés (le retrait unilatéral des États-Uniens du Mali, le contrat des sous-marins australiens). Cela peut aller très loin. Lorsque le président Donald Trump a retiré les États-Unis de l'accord sur le nucléaire iranien, il a menacé de punir les entreprises européennes qui auraient suivi le droit international. Bien que les

gouvernements européens aient continué à soutenir l'accord, des entreprises européennes telles que Total et Airbus ont retiré leurs investissements en Iran, tandis que la société de paiements internationaux SWIFT, enregistrée en Belgique, a suspendu l'Iran de ses comptes, coupant ainsi le pays du système bancaire mondial. L'avis de l'Europe n'a pas compté dans cette affaire. Dans le contexte actuel d'invasion de l'Ukraine, les dépendances en matières premières vis-à-vis de la Russie sont autant de vulnérabilités qui ne mettent pas l'Europe dans une position confortable. D'ailleurs, certains grands groupes européens ont dû abandonner le marché russe (Mercedes Benz, BMW, Volkswagen, Adidas, Chanel, Louis Vuitton, Ikea[70]). Dans la guerre froide technologique avec la Chine, les États-Unis pourraient limiter le commerce et les investissements de l'UE en Chine de la même manière qu'ils l'ont fait avec l'Iran. Cela rappelle les menaces à peine voilées du président Trump vis-à-vis des Européens qui auraient choisi Huawei. Dans une telle situation, les échanges commerciaux d'une valeur d'environ 190 milliards d'euros/an pour la Russie et environ 1 milliard d'euros/jour pour la Chine seraient fortement perturbés. Et déplacer ces dépendances, de ressources ou technologiques, de la Chine vers les États-Unis, serait une erreur grave.

Ces dix dernières années, l'Europe ne cesse de découvrir les implications géopolitiques des technologies : l'interférence des Russes dans les élections aux États-Unis en 2016, la désinformation lors du Brexit, le scandale Cambridge Analytica en 2018, la surveillance chinoise grâce à des caméras CCTV placées dans des aéroports, des mairies, des rues européennes. La récente pandémie de la COVID-19 et l'invasion de l'Ukraine par la Russie ont accéléré certaines tendances et ont mis au premier plan les enjeux qui ont fait se déplacer les technologies des places de marché aux champs de bataille. Et l'OTAN ne semble plus en mesure de défendre l'Europe, selon les dires du président Macron qui, en novembre 2019, évoquait la *« mort cérébrale de l'Otan »* [71], et un appel au *« réveil de l'Europe »,* celle-ci devant, selon lui, se doter d'une *« autonomie stratégique et capacitaire sur le plan militaire » tout en « rouvrant un dialogue stratégique, sans naïveté aucune […], avec la Russie »*. L'ancien Premier ministre norvégien et Secrétaire Général de l'Alliance affirmait en mars 2021[72] :

> *L'Union européenne n'est pas en mesure de défendre le Vieux Continent et ne doit pas affaiblir l'OTAN avec sa volonté d'autonomie.*

Les avis divergent, les intérêts étatiques de chaque membre également. L'UE ne peut pas ignorer l'OTAN, cependant, il faut rester lucide sur la volonté étasunienne de retrouver son hégémonie mondiale des années 1990. Bien que depuis toujours tiraillée entre la défense otanienne, européenne et nationale de chaque pays, les pays européens ne peuvent pas se contenter d'une sécurité, d'une protection de l'espace cyber européen dépendant de l'OTAN et donc des moyens américains. Un pays européen non membre de l'OTAN devra nécessairement pouvoir compter sur l'UE tel que l'Autriche ou l'Irlande, par exemple. De surcroît, en matière de défense des systèmes de l'information aucun pays n'a aujourd'hui des capacités qui lui assurent la souveraineté, comme l'affirmait lors de notre entretien Guy-Philippe Goldstein :

> *Si demain la France ou l'Allemagne reçoivent le traitement qu'a reçu l'Ukraine en termes d'attaque cyber, je ne pense pas qu'on pourra faire l'économie d'un appel au patron de Microso*

"*La sécurité commence chez soi*" dit l'adage ; le chemin pour y faire adhérer toute l'Europe est en revanche moins évident.

"Coincée" entre les États-Unis qui utilisent les données mondiales pour espionner et développer leur économie, et la Chine qui exploite les nouvelles technologies pour asseoir son autorité nationale et étendre son influence économique, voisine d'une Russie lancée dans une guerre cyber et conventionnelle destructrice, l'UE ne se propose pas vraiment comme une "voie de milieu" mais comme une alternative démocratique. Car l'Europe ne vise ni le pouvoir absolu, ni la reconquête d'empires perdus. Dépourvue de toute intention offensive, et quelque peu naïve quant à la réciprocité de l'alliance avec les États-Unis, l'UE s'est vue obligée de protéger les données de ses citoyens tout en formulant le souhait d'une autonomie stratégique.

Consensus autour d'une stratégie commune

Dans un effort de cohérence et de mutualisation des actions et des investissements dans le domaine de la cybersécurité, trois commissaires[73], suédoise, britannique et néerlandaise, ont lancé l'initiative d'une stratégie de cybersécurité pour l'Europe, il y a un peu plus de dix ans. Lorsque les instances de l'UE ont évoqué un projet de réglementation européen pour la sécurité des systèmes d'information, les EM ont accueillis le projet avec une certaine réserve. En effet, la sécurité et la défense sont des sujets régaliens, donc relevant de la compétence nationale, l'OTAN étant chargée de répondre à l'échelle macro-régionale. Il n'était donc pas intuitif d'avoir à l'époque l'état des réflexions actuelles.

Ces dernières années, traiter le sujet cyber à l'échelle européenne est devenu urgent et nécessaire pour deux raisons pragmatiques. La première est qu'une coopération forte à l'échelle européenne est le seul moyen de se parer raisonnablement à la menace cyber et les attaques qui sont, pour rappel, orchestrés à l'échelle mondiale par d'autres puissances macro-régionales reconnues pour leurs capacités cyber (États-Unis, Chine, Russie, pour ne citer qu'eux). La seconde raison, qui découle de la première, est de réduire l'écart de compétences, donc la vulnérabilité, et de résilience entre les EM, et les autres partenaires européens.

Le 7 février 2013 cette stratégie est publiée : c'est la *Stratégie de l'UE en matière de cybersécurité - Un cyberespace ouvert, sûr et sécurisé (EU-CSS)*. À travers cette stratégie, l'Europe vise à offrir aux européens une sécurité maximale dans le cyberespace[74] :

> *Une protection et une promotion efficaces des droits individuels, pour que l'environnement en ligne de l'UE soit le plus sûr au mond*

Cependant, il semblerait que la stratégie ait été perçue comme une notion à priorité variable par l'environnement technologique européen, par certains États membres et même par la Commission Européenne. Ainsi, le 16 décembre 2020, après les révélations de Snowden et pendant l'explosion du travail à distance imposé par la pandémie, la *Nouvelle Stratégie de Cybersécurité* a été mise à jour et constitue aujourd'hui la pierre angulaire de la politique de l'UE en matière de cybersécurité. Elle confirme de manière plus granulaire les objectifs annoncés dans la stratégie de 2013 dont l'atteinte permettrait de répondre tant à l'urgence qu'à la nécessité.

7 fév. 2013

de gauche à droite : Catherine Ashton (Royaume-Uni), Haute Représentante, Neelie Kroes (Pays Bas) Commissaire de la DG Connect et Cecilia Malmström (Suède) Commissaire à l'intérieur

1. Une Europe cyber résiliente

Face aux cybermenaces, tous les citoyens et toutes les entreprises doivent pouvoir bénéficier pleinement de services et d'outils numériques fiables et dignes de confiance. Il s'agit notamment d'accroître la capacité à opérer des choix autonomes dans le domaine de la cybersécurité afin de renforcer le leadership numérique et les capacités stratégiques de l'UE. Deux règlementations en cours d'élaboration doivent répondre à cet enjeu : The *Network and Informations System 2 Directive* (NIS2, cf. Annexe II) et The *Cyber Resilience Act*. La première vise à renforcer la version précédente et à mieux protéger les réseaux et les systèmes d'information tandis que la seconde concerne la résilience des objets connectés.

2. Lutte contre la cybercriminalité / Réduction drastique de la cybercriminalité

Un centre européen spécialisé dans la lutte contre la cybercriminalité a été créé au sein d'Europol pour aider les pays de l'UE à enquêter sur la criminalité en ligne et à démanteler les réseaux criminels. C'est la plateforme pluridisciplinaire European Cybercrime Centre (EC3). En plus de l'agence EC3, a été créé *Empact*, une initiative complémentaire en matière de sécurité menée par les EM dans le but d'identifier, de hiérarchiser et de combattre les menaces que représente la criminalité organisée internationale. En s'appuyant sur l'EC3 et la plateforme *Empact*, l'Europe se donne des moyens pour lutter sur le territoire européen contre cette cybercriminalité qui nuit à la confiance des consommateurs. L'enjeu de confiance numérique européenne passe donc par cette lutte contre la cybercriminalité, contre la fraude, mais aussi par le renfort de la sécurité des enfants qui naviguent sur Internet, et la mise en place sur la plan judiciaire et répressif de nouvelles règles censées faciliter et accélérer la coopération au sein de l'UE.

3. Stimuler la cyber diplomatie / Établir une politique internationale cohérente en matière de cyberespace pour l'Union Européenne et promouvoir ses valeurs fondamentales

Résolument en faveur d'un cyberespace ouvert, libre, stable et sûr, où les droits des individus, les libertés fondamentales et l'état de droit sont pleinement respectés, l'UE et les EM doivent se protéger contre les cybermenaces provenant de pays tiers, notamment au moyen d'une réponse diplomatique conjointe appelée The Cyber Diplomacy Toolbox. Cette boite à outils consiste à disposer de mesures préventives contre les cyberattaques et des sanctions partagées par tous les EM. L'approche diplomatique sur la cybersécurité consiste davantage à sanctionner en s'appuyant sur des mesures restrictives (gel d'avoir, interdiction d'entrée dans l'UE, etc.) plutôt qu'à faire valoir une cyberdiplomatie européenne "conquérante" qui aurait pour vocation d'influencer et diffuser ses intérêts.

4. Coopération en matière de cyberdéfense / Développer une politique et des capacités de cyberdéfense liées à Common Security and Defence Policy (CSDP)

Le cyberespace est considéré comme constituant le cinquième domaine de guerre, et il est aussi critique sur le plan des opérations militaires que les domaines terrestre, maritime, aérien et spatial. Il s'agit d'un domaine qui englobe tout ce qui concerne les réseaux d'information et de télécommunication, les infrastructures et les données que ceux-ci prennent en charge, ainsi que les systèmes, processeurs et contrôleurs informatiques. L'UE coopère en matière de défense dans le cyberespace à travers les activités de European Defense Agency (EDA), en collaboration avec ENISA et Europol. EDA aide les États membres à bénéficier d'une main-d'œuvre militaire qualifiée dans le domaine de la cyberdéfense et veille à ce que des technologies de cyberdéfense proactives et réactives soient disponibles. La coordination de la cyberdéfense, la coopération et la constitution des capacités de cyberdéfense sont les deux objectifs majeurs de l'UE en matière de cyberdéfense.

5. Financement et recherche / Développer une politique industrielle pour la cybersécurité

La cybersécurité constitue un élément important des programmes-cadres de l'UE pour le financement de la recherche et de l'innovation, *Horizon 2020*, et son successeur Horizon Europe. En mai 2020, l'UE a engagé 49 millions d'euros pour stimuler l'innovation dans le domaine de la cybersécurité et des systèmes de protection de la vie privée[75]. De plus, à travers son programme Digital Strategy d'ici à 2027, l'UE s'est engagée à investir 1,6 milliard d'euros dans la capacité de réaction en matière de cybersécurité et le déploiement à grande échelle d'infrastructures et d'outils de cybersécurité dans l'ensemble de l'UE, pour les administrations publiques, les entreprises et les particuliers. Enfin, la Roumanie accueille depuis 2021 The European Cybersecurity Competence Centre for Social Innovation. Il s'agit du principal instrument de l'UE pour mettre en commun et pour mieux coordonner les investissements dans la recherche, les technologies et le développement industriel en matière de cybersécurité. Les objectifs sont les suivants : soutenir les jeunes entreprises et les PME du secteur, renforcer la recherche et l'innovation, et contribuer à combler le déficit de compétences en Europe en matière de cybersécurité.

Dans son ensemble, la vision de l'UE se propose de donner vie à des actes législatifs et des entités qui régulent les acteurs économiques, facilitent et coordonnent toutes les parties prenantes de l'écosystème cyber afin d'assurer la sécurité des données de tous les européens, à l'instar de Maria, avatar créé par la Cour Européenne des Comptes pour illustrer la manière de l'UE de protéger la vie numérique d'une lycéenne de 15 ans (Annexe III).

La question qui se pose est de savoir si cela suffit pour faire naître une autonomie stratégique dans le secteur des technologies ? Car, cette autonomie est indispensable pour pouvoir œuvrer en faveur d'un internet ouvert, libre et en ligne avec les valeurs démocratiques. La souveraineté technologique européenne est directement conditionnée par la sécurité juridique des solutions utilisées en Europe. Cet

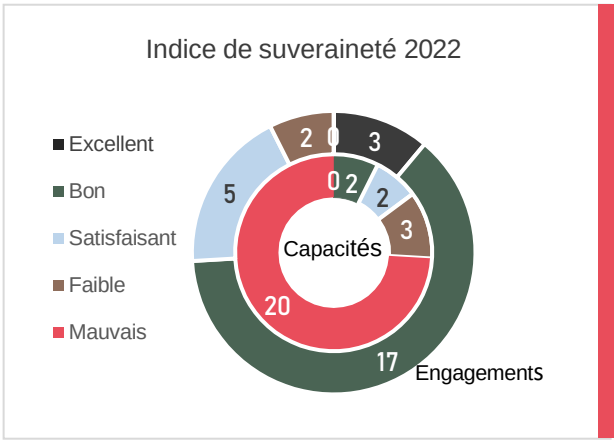
aspect doit être corrélé avec d'autres champs d'action car la technologie n'est pas la seule dépendance de l'Europe vis-à-vis des puissances mondiales.

Dans un classement réalisé en juin 2022 par The European Council on Foreign Relations, six domaines de dépendance ont été identifiés. Parmi les six, les technologies se placent en dernière position[76].

Les résultats de plus de trois quarts des États membres sont médiocres ou moins bons, tandis que ceux de plus d'un quart d'entre eux sont mauvais. Il est important de noter que les États membres obtiennent

Indice de souveraineté
Données : ECFR 2022

généralement un score nettement plus élevé en matière d'engagement qu'en matière de capacités, avec une moyenne de 6,8 et 3 respectivement. Cela reflète le fait que l'UE n'est pas à la pointe du développement technologique mondial dans de nombreux domaines mais que, ces dernières années, elle a fait preuve d'une volonté de façonner de manière décisive le marché européen des technologies. Les pays les plus attachés à la souveraineté technologique de l'UE ont des économies plus petites (Luxembourg, Finlande, Slovénie, Chypre, et l'Estonie) (cf. Annexe IV)[77]. Ces pays bénéficient particulièrement de la force du marché et de la réglementation de l'Union pour affronter la concurrence mondiale. Les premières 4 puissances économiques européennes, l'Allemagne, la France, l'Italie et l'Espagne se situent au mieux à la 10ème place grâce à la présence d'entreprises leader du secteur : Athos, Zeiss, Trumpf, Bosch, Infineon.



81%
des EM s'engagent pour la souveraineté

85%
des EM sont mauvais en capacités cyber autonomes

Données : ECFR 2022

Dans le contexte actuel de fragmentation du niveau de souveraineté technologique, il existe des défis qui nécessitent plus que la capacité combinée de quelques États, même très influents. Dans quelle mesure les problèmes de cette ampleur retiennent-ils l'attention et l'implication de chaque EM ?

Les chapitres qui suivent essayeront de répondre à cette question. Cependant une chose est certaine : la vision de l'Europe ambitionne clairement la mise en place d'un engagement *« avec la communauté des parties prenantes, en soulignant la nécessité pour tous ceux qui utilisent l'internet de jouer leur rôle dans le maintien d'un cyberespace mondial, ouvert, stable et sécurisé, dans lequel chacun peut vivre sa vie numérique en toute sécurité »*[78]. C'est aussi l'aveu d'une reconnaissance qu'individuellement personne n'y arrivera, leitmotiv de la Coalition *Contract for the Web*[79] :

> *The web was designed to bring people together and make knowledge freely available. It has changed the world for good and improved the lives of billions. […] Everyone has a role to play in safeguarding the future of the web.*

UNE COORDINATION INSTITUTIONNELLE À DIFFÉRENTES ÉCHELLES

CHAPITRE DEUX

2.1. Une coordination verticale complexe

Ces dix dernières années, les attaques contre les systèmes informatiques des entreprises privées, des États membres ou d'institutions européennes nous rappellent indiscutablement que la technologie est employée à des fins politiques, économiques et militaires. Dans ce contexte, l'UE a mis l'accent sur une approche commune de la cybersécurité. C'est une première étape nécessaire pour, entre autres, tracer une stratégie de coopération, s'aligner sur des règles communes et inciter à la collaboration. C'est ce que Helena Carrapico et André Barrinha appellent une coopération "institutionnelle"[1]. Celle-ci se révèle indispensable étant donné le caractère décentralisé de la gouvernance de la cybersécurité en Europe dû à la pluralité d'institutions, d'organismes, réseaux, agences nationales et européennes, et à la multiplication d'acteurs privés.

Dans la première partie de ce chapitre, il sera question de comprendre par une lecture verticale comment les institutions européennes (au sein de l'UE), les États Membres (EM) et les acteurs privés coopèrent et se coordonnent entre des niveaux de responsabilité différents, afin de définir ensemble le cadre et les outils indispensables au succès de la *Stratégie européenne de cybersécurité* (EU-CSS). Dans la deuxième partie, la même question sera abordée par une approche horizontale entre les acteurs situés à un même niveau de la hiérarchie. Tout au long de ce développement, nous nous accordons à considérer qu'un alignement entre les procédures et les politiques formulées, les instruments, et les acteurs représente la condition *sine-qua-non* d'une approche commune cohérente de la cybersécurité en Europe. Celle-ci, à son tour, pose les bases d'une définition partagée de la cybersécurité, des menaces qui pèsent sur elle, et des meilleures actions pour y répondre.

Une volonté de coopérer malgré un niveau de maturité hétérogène

La stratégie de cybersécurité européenne décline des objectifs formulés dans la *European Union Global Strategy*. Un impact "global" ne s'entend pas seulement dans un sens géographique : il fait également référence au large éventail de politiques et d'instruments que la stratégie européenne doit également promouvoir. Cette stratégie européenne se concentre tant sur les capacités militaires et l'antiterrorisme que sur les opportunités d'emploi, les sociétés inclusives et les droits de l'Homme.

Dans cette perspective, il faut évoquer l'intégration des questions de cybersécurité dans tous les domaines politiques ainsi que le renforcement de la dimension cyber dans les missions, les opérations de la *Common Security and Defense Policy* (CSDP) et le développement des plateformes de coopération. Au niveau vertical de la hiérarchie décisionnaire européenne, l'alignement des acteurs d'une perspective pluri-niveaux se définit plutôt comme une coordination qu'une coopération. La coopération serait dans ce cas synonyme de consensus (en anglais *consistency*) qui se définit par une absence de frictions, d'oppositions. Quel est le niveau de consensus qui existe entre les différents niveaux d'acteurs européens lorsqu'il s'agit de définir une approche commune de la cybersécurité européenne ?

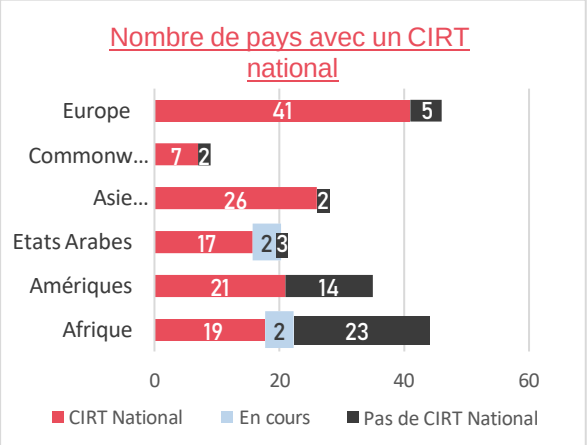
La vision de l'UE en matière de cybersécurité est d'offrir aux citoyens l'espace numérique le plus sûr au monde. Le *Global Cybersecurity Index* réalisé par l'ITU en 2020[2] confirmerait l'atteinte de cet objectif européen. Sur les 12 critères de maturité cyber, l'Europe est systématiquement l'élève modèle. Bien que l'Europe soit la meilleure dans chaque catégorie, peut-on pour autant affirmer que le citoyen européen bénéficie de l'espace numérique le plus sûr ? En comparaison avec le reste du monde, certainement. Mais est-ce suffisant ?

Au vu du nombre d'institutions en charge de la cybersécurité[3], il existe donc un intérêt évident à veiller à ce que la cybersécurité soit

Europe

le continent le plus mature

Données : ITU, *Global Cybersecurity Index 2020*



intégrée dans des domaines politiques plus larges, notamment dans les relations extérieures de l'UE et dans la politique étrangère et de sécurité commune. Ce qui est d'ailleurs le cas, la cybersécurité faisant partie des domaines prioritaires cités dans la *EU Global Strategy*, dès 2016. Des fonctionnaires européens et nationaux le confirment d'ailleurs lors de divers entretiens[4]. La naissance même de la *Stratégie Européenne de Cybersécurité (EU-CSS)* témoigne d'un effort commun entre les représentantes de trois institutions de l'UE : la Commissaire à l'Intérieur de l'époque, Cecilia Malmström, la Haute Représentante Catherine Ashton et la Commissaire de la DG Connect, Neelie Kroes, avec la contribution de la DG JUST.

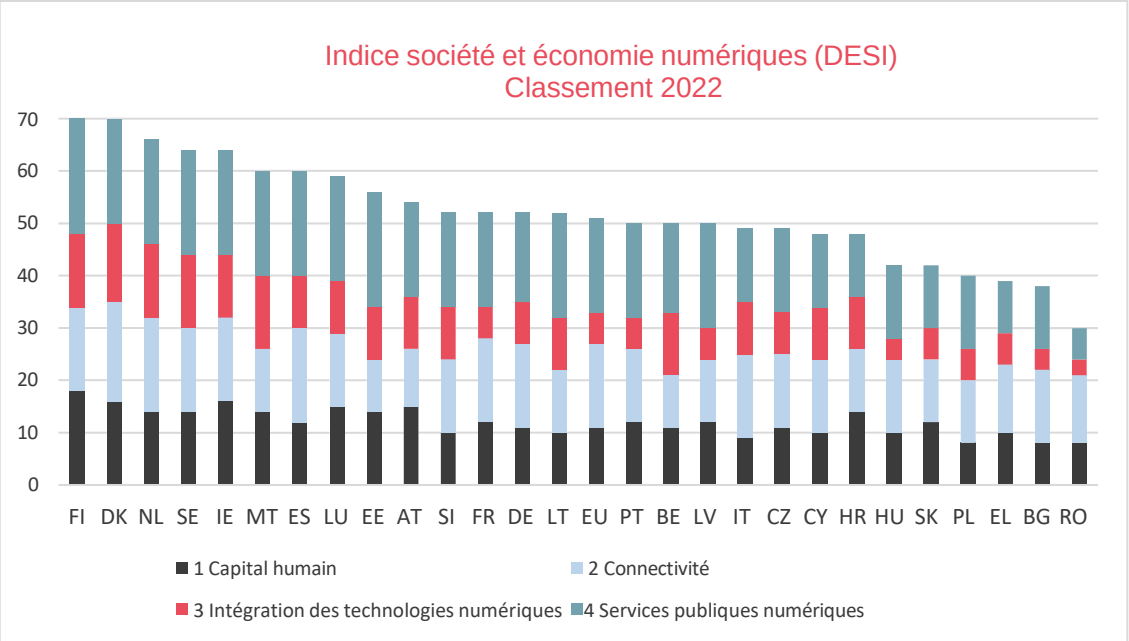
Aujourd'hui, une culture croissante de la coordination entre les institutions de l'UE est aussi visible par l'augmentation du nombre de documents officiels faisant référence à la nécessité d'une coordination plus étroite (*Directive NIS*, *EU-CSS, Cybersecurity Act*, *European Union Global Strategy*, *Digital Compass*, etc.) et par la représentation des organes de l'UE dans les conseils d'administration de l'EC3, l'ENISA et du CERT-EU, par exemple.

Concrètement, cette coopération s'exprime à travers la participation conjointe aux réunions du *Political and Security Commitee* (PSC) et du *Commitee on Operational Cooperation on Internal Security* (COSI) ainsi que dans les sessions communes du *Parliamentary Commitee on Civil Liberties, Justice and Home Affaires* (LIBE) et du *Commitee on Foreign Affairs* (AFET). Cela est également visible dans la représentation de l'ENISA dans le board d'EC3 et vice-versa. La volonté d'une meilleure coordination entre ces deux organismes s'est concrétisée dans un accord signé en 2014. L'atelier annuel ENISA/EC3, auquel participent les CSIRT, les Law Enforcement Autorities, l'ENISA et l'EC3 est le fruit de cet accord et a débouché dans la publication d'une taxonomie commune. D'une part, la *Reference Incident Classification Taxonomy*, facilite la communication sur les incidents cyber de grande envergure. D'autre part, elle facilite aussi l'alignement des définitions et des terminologies de la cybersécurité afin de permettre la catégorisation des institutions et des compétences existantes en Europe. D'autres initiatives de collaboration incluent la taxonomie eCSIRT.net2 qui a été développée en 2003, et la taxonomie eCSIRT.net mkVI3 qui est une adaptation de la taxonomie eCSIRT.net originale. Depuis 2018, une communauté cyber a pu ainsi se créer à travers les institutions européennes, fondée sur une culture commune de communication, de coordination et de partage. Toutefois, cette communauté fait aussi état, entre autres, de ressources limitées qui entravent la coopération inter- institutionnelle.

La diversité en termes de maturité cyber en Europe, tant sur le plan technologique, de gouvernance et juridique n'est pas une surprise et a été soulignée par le Conseil européen dès 2005[5] et confirmée lors de notre entretien avec l'ANSSI. Anne Tricaud, Cheffe de la Division internationale pendant la présidence française du Conseil, perçoit cette différence en matière de cybersécurité où, à différence de l'Allemagne ou de l'Espagne, la posture nationale est assumée par l'intégralité de l'administration française (entretien juillet 2022). Cette diversité est à l'image de la diversité culturelle de l'Europe, parfois un avantage, parfois une faiblesse. La maturité cyber est directement liée au niveau de numérisation des EM. En dépit des efforts déployés ces dix dernières années par l'UE dans la réglementation et l'aide aux investissements, la vérité est que le développement numérique à travers l'Europe reste assez contrasté et complexe car certains EM accusent encore des écarts importants (Danemark vs Roumanie à titre d'exemple (cf. graphique ci-dessous), comme le dote également Anne Tricaud de l'ANSSI[6] :

> *« Il y a aujourd'hui un sujet de différence de capacité entre les EM. Il y a des pays qui sont bien dotés, enfin, on est un grand pays, bien doté en termes de ressources. Quand on compare les ressources de la France et de l'Allemagne avec le Chypre ou Malte, ça n'a rien à voir. »*

La performance de certains critères du *Digital Economy and Society Index* de 2022, tels que la numérisation des PME, la 5G et les compétences digitales, est jugée insuffisante par la Commission Européenne. Or, il faut réunir des compétences et de la main d'œuvre, une infrastructure mobile performante et couvrante, l'acceptation d'une intégration du numérique dans la société et la digitalisation des services publics. Si un seul de ces critères est défaillant, l'impact est inévitable sur les autres et sur la sécurité entière des systèmes d'information.



Données CE 2022

Du point de vue de la protection de l'information, la 5G, les compétences digitales et les PME représentent de véritables enjeux qui seront analysés ultérieurement. En effet, comment réduire cet écart de compétences et de connaissances ? Sans un certain équilibre de compétences, il sera difficile de coopérer en matière de cybersécurité. Sans une maîtrise commune de la taxonomie cyber et des bonnes pratiques en matière de cybersécurité, il sera difficile de coopérer.

Coopérer : un impératif inscrit dans la stratégie

Pour éviter que chaque Etat Membre agisse indépendamment ou adopte une posture protectionniste, l'UE a posé un cadre réglementaire à travers des directives, règlements-cadre et feuilles de route censés assurer une vision commune pour la cybersécurité. La coordination et la coopération y sont inscrites en tant qu'objectif à atteindre. Déjà en 2005, le *Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems* est essentiellement rédigé autour de la nécessité de coopérer : « *La présente décision-cadre vise à renforcer la coopération entre les autorités judiciaires et les autres autorités compétentes, notamment la police et les autres services spécialisés […] définition commune […] approche commune […] coopération judiciaire […] Des mesures de coopération entre les États membres devraient également être envisagées, afin d'assurer une action efficace contre les attaques visant les systèmes d'information.*»[7] C'est d'ailleurs pour cela qu'une agence dédiée à la cybersécurité a été créé durant cette même période par *Regulation N° 460/2004* du Parlement Européen et du Conseil du 10 mars 2004 : The Union Agency for Network and Information Security (ENISA).

L'ENISA a pour mission d'aider les agences nationales à collaborer entre elles et *« vise à garantir un niveau élevé commun de cybersécurité dans toute l'Europe »*[8]. Il s'agit, pour l'ENISA, de faire converger des visions communes, et d'uniformiser des pratiques. Mais avant cela, il faut accompagner en priorité les états moins expérimentés afin d'attendre un niveau minimum de compétences et connaissances. Pour cela, l'ENISA collabore avec les autorités nationales des EM plus expérimentés. Elle met aussi en place des *capacity building* au service des états les moins matures. Cela peut prendre la forme d'une assistance mutuelle en cas de crise, ou tout simplement d'un partage de bonnes pratiques afin de sécuriser davantage les systèmes d'information et les infrastructures nationales. Pour ce faire, l'ENISA s'assure de la bonne maîtrise du processus par les spécialistes désignés au sein des EM, généralement au sein de chaque agence nationale. Elle s'appuie également sur des réseaux d'échange et de partage d'expériences et de bonnes pratiques, par le biais de réseaux européens de collaboration (CSIRT Network[9], CyCLONe[10], NIS Cooperation Group[11], etc.) dont certains

GDPR

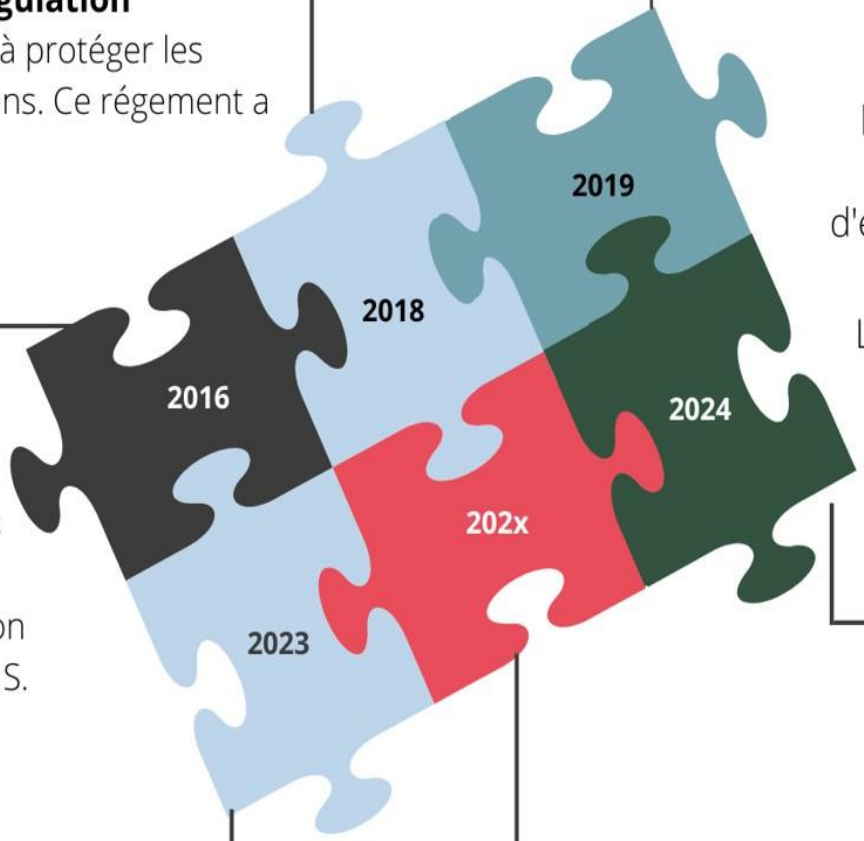
The General Data Protection Regulation
Obligatoire depuis mai 2018, il vise à protéger les données personnelles des Européens. Ce régement a une portée extraterritoriale.

NIS

The Network Information and Systems
Directive dédiée à la cybersécurité européenne imposant des objectifs de sécurité aux OSE et aux DSP traitant les données de l'UE. Création du CERT EU, ainsi que du groupe NIS.

NIS2

The Network Information and Systems 2
renforce la collaboration européenne existante, fruit de la Directive NIS, en élargissant son champ d'action, et en s'appuyant sur le secteur privé.



CSA

The Cybersecurity Act
confie à l'ENISA un mandat permanent, ainsi que de nouvelles responsabilités, notamment celle d'établir le cadre de certification de la cybersécurité dans l'UE. L'objectif est d'uniformiser le niveau de sécurité cyber en Europe.

DSA

The Digital Services Act
à venir

DMA

The Digital Markets Act
à venir

seront détaillés ultérieurement. L'objectif de l'ENISA n'est pas de devenir une super agence européenne qui aura à terme pour mission d'intervenir pour gérer des incidents et des crises cyber. Sa mission n'est guère opérationnelle. Elle doit cependant s'assurer que tous les EM suivent la feuille de route européenne. Il n'est pas inutile de rappeler que l'ENISA est l'agence européenne POUR la Cybersécurité, et pas l'agence européenne DE la cyber… La dialectique n'est pas anodine.

Avec la nouvelle *European Cybersecurity Strategy* de 2020, l'UE s'est proposée de réunir toutes les capacités technologiques des EM au travers d'une mission claire, et de construire une stratégie conjointe déployable lors du nouveau mandat de l'ENISA. Le rôle renforcé de l'ENISA est déterminant pour coordonner la mise en application des directives européennes et les process d'uniformisation auprès de toutes les agences et autorités locales au sein de l'UE. À partir de 2013, la coopération devient un objectif à part entière à atteindre. C'est l'année du début des discussions sur la future *Directive NIS*. La coopération devient l'un des trois piliers de la *Stratégie de cybersécurité* visant, entre autres, à renforcer la *« coopération pour faire progresser un cyberespace mondial et ouvert »*[12] à travers des outils tels que des initiatives, des politiques-cadre, des réglementations et des investissements.

Il est donc évident que la cybersécurité est considérée, par les institutions européennes et les EM, comme étant l'un des domaines de priorité dans la stratégie globale européenne. D'ailleurs, le sujet est régulièrement introduit dans les débats des autres domaines prioritaires de l'UE (sécurité, politique extérieure, innovation). Pourtant nos recherches ont montré que la législation ne suffisait pour à assurer la sécurité au sein de l'UE. Comme nous l'avons vu, la bibliothèque législative de la cybersécurité est consistante, et les organismes de gouvernance également. Lors d'une lecture plus attentive de ces textes législatifs, on remarque explicitement une harmonisation minimale plutôt que maximale en opposition avec l'objectif ambitieux de la *Stratégie EU-CSS* qui est d'assurer un niveau élevé de sécurité dans l'ensemble de l'UE. Ce signe de perte de "*consistency*" profite d'ores et déjà à certains acteurs. Si cette incohérence devait se poursuivre, des lacunes continueront à apparaître à mesure que le cyberespace évolue. Un risque d'implosion n'est pas à exclure, avec tout ce que cela pourrait impliquer au niveau de l'unité d'Internet.

Une perception culturelle de l'ennemi

Les rapports entre les EM, notamment au sein de l'UE et de l'OTAN et les grandes puissances numériques sont influencés par des facteurs historiques, culturels et géopolitiques. On note cependant une accélération du rythme avec lesquelles la perception de ces rapports change, conséquence, entre autres, du Brexit, du déroulement des dernières élections présidentielles états-uniennes, de la pandémie et du conflit en Ukraine. Désormais, le monde est constitué de partenariats stratégiques, sans alliance automatique. Anne Tricaud de l'ANSSI précise même que c'est fondé uniquement sur des intérêts[13] :

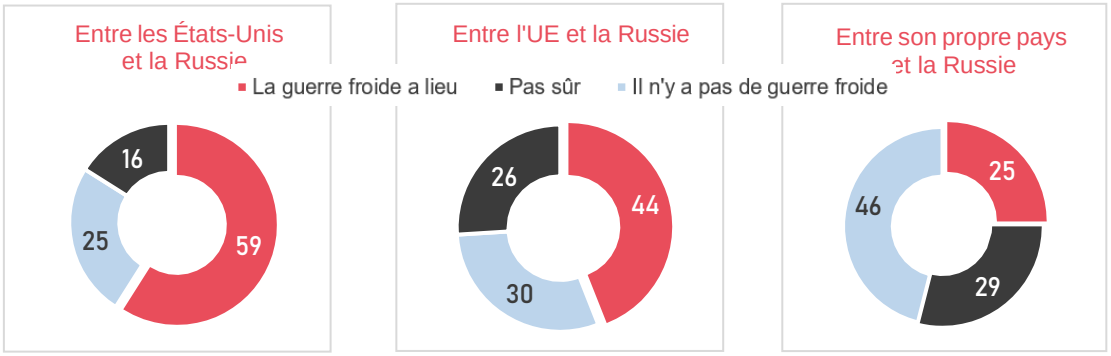
> *Il ne faut pas être naïf. Au contact avec les partenaires, ma devise est : on n'a pas d'amis, au mieux on a des alliés, au pire, des ennemis.*

Suite à ces évènements, les Européens tentent de suivre. Si la grande majorité confirme l'existence d'une guerre froide entre la Chine et les États-Unis, la plupart des Européens n'ont pas le sentiment que leur propre pays soit concerné par cette guerre. Cette dichotomie peut surprendre : une pluralité d'Européens sont nombreux à penser que l'Union Européenne est engagée dans la guerre froide avec la Chine, alors qu'ils sont aussi nombreux à ne pas penser la même chose de leur pays d'origine[14] :

> *Citizens are more likely to believe that a new cold war will be fought by Brussels and Washington rather than by Paris and Berlin, or Warsaw, Rome, and Madrid.*

Au sein du bloc européen, les écarts de perception sont évidents : seules la France et la Pologne pensent être en guerre froide avec la Russie, alors que la Hongrie, le Portugal, l'Autriche et l'Italie ne perçoivent pas de conflit avec la Russie. Par ailleurs, depuis 2019, l'UE considère la Chine comme " an economic competitor in pursuit of technological leadership and a systemic rival promoting alternative models of governance"[15] et les relations diplomatiques ne cessent d'empirer, malgré des échanges économiques considérables, d'ailleurs facteurs clé de la productivité européenne.

Pensez-vous qu'il y a une guerre entre … ?



44%

d'Européens croient qu'il y a une nouvelle guerre froide entre l'UE et la Russie.
Données : Datapraxis and YouGov (DE, FR, DK, ES, PL, PT, SE, IT, AT), AnalitiQs (NL), Alpha (BG), and Szondaphone (HU) 2021

ECFR

Ce sondage de 2021 illustre parfaitement le manque d'alignement entre la perception des citoyens vis-à-vis des alliés et des ennemis. Des écarts considérables existent également dans la perception des Européens à propos de la position de leadership de l'Allemagne ou des États-Unis. Vis-à-vis des États-Unis, trois catégories se détachent : 7 pays qui ne reconnaissent pas le leadership états-unien, parmi lesquels la France, le Royaume-Uni, l'Allemagne et l'Italie, ceux qui le reconnaissent, 13 pays parmi lesquels les Pays-Bas, l'Albanie et le Portugal et 6 pays qui ne savent pas[16].

0,85L'Europe de la cyberdéfense militaire se met en ordre de bataille, nous précise Sébastien Garnault, organisateur du Paris Cyber Summit[17] *:*

« La guerre en Ukraine nous a donné un dramatique exemple de ce qui pourrait advenir si on ne parvient pas à unir nos efforts. On constate avec ce conflit que, oui ! On doit faire front commun, car oui, les Européens font face à des menaces communes. Mais en revanche, nous ne sommes pas totalement prêts, au niveau européen, à se lancer dans un conflit ouvert dans le cyberespace. Une guerre hybride pour laquelle chaque pays devrait normalement apporter sa part. »

Dans cet esprit, le ComCyber a profité de la présidence française de l'UE pour proposer une coopération militaire entre les commandements européens : Military Computer Emergency Response Team Operational Network (MICNET). En novembre 2022, dix-huit pays membres de l'UE ont signé l'accord MICNET dont le but vise à renforcer la coordination et la réactivité des armées face aux attaques informatiques. Si l'UE construit sa cyberdéfense afin d'être indépendante et autonome, il s'agit également d'une volonté nationale de chaque EM. Cette volonté répond dans un premier temps à une nécessité sécuritaire mais aussi économique et politique. À titre d'exemple, en parallèle des manœuvres cyber de l'OTAN, l'Estonie a officialisé un partenariat avec l'armée de l'air américaine en 2016, afin développer un système d'analyse et de communication sur les menaces cyber. Cette coopération cyber bilatérale démontre que la coopération macro-régionale européenne peut être reléguée au second plan si elle n'apporte pas les attentes nécessaires à un pays membre dans le temps imparti. Il s'agit de la souveraineté européenne dans un espace pouvant être occupé par d'autres états, des groupes d'activistes, de terroristes ou d'individus agissant seuls.

Comme évoqué précédemment, au-delà d'un désir d'autonomie en matière de cyberdéfense, il s'agit concrètement de la crédibilité de sa politique, de son union entre 27 États Membres ainsi que de la continuité de la mise en application de ces lois. Ces perceptions et intérêts différents, voire opposés, mènent inévitablement à des motivations et des politiques différentes. Dès lors, la première priorité de l'UE est de faire naître une approche commune de la cybersécurité.

Le déploiement de la stratégie, la responsabilité des États membres ?

Dans le sillon de la naissance d'une cybersécurité européanisée – grâce au cadre législatif – et au mandat élargi de l'ENISA, des bases sont posées afin que les EM prennent en charge la cybersécurité au niveau national. Entre les différents niveaux de hiérarchie décisionnaire, l'absence de frictions, de chevauchements et de conflits est un critère d'évaluation de la cohérence des politiques. Mais avant

d'analyser cela, rappelons brièvement l'organisation et les prérogatives en termes de cybersécurité de l'UE et de ses EM.

La Commission Européenne (CE), organe exécutif de l'UE, s'emploie à faire de l'UE un acteur majeur de la cybersécurité. Les principales directions générales (DG) responsables de la cybersécurité sont les DG CONNECT (en charge du marché unique numérique) et HOME (responsable de l'union de la sécurité). La DG DIGIT est responsable de la sécurité informatique des propres systèmes de la Commission. Toute une série d'agences de l'UE soutiennent la Commission, parmi lesquels l'ENISA, le Centre Européen de lutte contre la cybercriminalité (EC3) et le CERT-EU, une équipe d'intervention en cas d'urgence informatique dans les systèmes informatiques de l'UE.

Les États Membres sont responsables au premier chef de leur propre cybersécurité et ils agissent, à l'échelle UE, par l'intermédiaire du Conseil de l'UE qui dispose de nombreux organes de coordination et de partage de l'information tel que *Questions liées au cyberespace*. Le Parlement européen agit en tant que colégislateur. Or il s'avère qu'entre États Membres et l'UE, le partage des actions dans le domaine de la cybersécurité n'a pas été assez pris en compte dans le règlement *Cybersecurity Act* qui, entre autres, confère des nouvelles missions à l'ENISA.

Les entreprises du secteur privé vont être impactées doublement par les ambitions de la Commission Européenne entérinées en lois européennes par le vote des EM. Une coordination minimum est dès lors souhaitable afin de pouvoir implémenter ces exigences.

Premièrement, les entreprises privées sont tenues à implémenter des mesures pour assurer un niveau minimum de sécurité à leurs systèmes d'importance vitale depuis la Directive NIS dès lors qu'elles reçoivent le statut de OES. Mais le processus est encore en cours. Alors que la *Stratégie EU-CSS* est présentée en 2013, la *Directive NIS* met trois ans à être adoptée. Les difficultés de sa négociation renvoient de façon claire à l'équilibre très subtil à atteindre entre le maintien de la souveraineté des États membres sur ces sujets très régaliens d'une part, et l'intégration dans une architecture plus resserrée de la cybersécurité européenne d'autre part, avec ce qu'elle implique de partage d'informations et de mise en cause d'aspects traditionnellement régaliens de l'action des États. S'inspirant de la *Loi de programmation militaire* française, l'Europe a défini dans cette directive des *Operators of Essential Services* (OES) ; il y est question notamment de porter le sujet cyber au niveau réglementaire pour ces opérateurs identifiés, aussi bien au niveau macro-régional que national, toujours avec l'appui et l'action des agences nationales.

L'enjeu est donc complexe : comment s'assurer que les réglementations européennes et nationales se complètent, et surtout ne se court-circuitent pas ? Pour cela, il a d'abord fallu distinguer les Opérateurs d'Importance Vitale (OIV) nationaux et les OES européens. Les OIV sont donc définis comme étant des opérateurs critiques pour la sécurité nationale, alors que les OES sont, quant à eux, définis comme critiques pour sécuriser le marché intérieur. Attention ici à bien saisir la différence : d'un côté, du point du vue national, il s'agit de protéger ce qui est critique pour la sécurité nationale ; de l'autre côté, du point de vue européen, il s'agit de protéger ce qui est critique pour la sécurité du "marché" européen. Il est ici très important de souligner cette distinction, et cette notion de "marché" en tant que point névralgique de l'UE. Cette différence de perception est renforcée par la diversité des postures géopolitiques des EM dont nous avons montré quelques aspects auparavant. Les EM aussi peuvent faire naître des frictions qui témoignent d'un manque de cohérence vis-à-vis de la *Stratégie EU-ECCS*. Ce sera lors de l'adoption du *Cybersecurity Act* en 2019 que les fissures deviendront plus visibles et l'incohérence fera son apparition à la vue de tous.

Deuxièmement, The *Cybersecurity Act* est un règlement qui introduit deux modifications majeures, comme rappelé précédemment : la création d'un schéma de certification pour les produits et les services de cybersécurité, ce qui a conduit tout naturellement à un élargissement des missions de l'ENISA. Le cadre européen pour les certifications de sécurité représente un véritable enjeu de sécurité et de confiance au sein de l'Union Européenne. La mission de l'ENISA est d'harmoniser les pratiques de certification des États membres, avec l'appui et la collaboration des agences nationales, pour permettre une reconnaissance mutuelle au sein de l'UE. Il s'agit là des premières actions pour le développement d'un tissu industriel privé se basant en partie sur la confiance. Ainsi, une prestation hollandaise certifiée sera reconnue aussi bien en Italie qu'en France ou en Finlande. Les produits, services et processus, qui auront vocation à être certifiés seront soumis à des schémas « thématiques » au regard de risques

identifiés : 5G, Cloud, IA, IoT, etc. Cette déclinaison a donc vocation à se faire en continu par les États membres, avec l'ENISA en qualité de rédacteur des schémas de certification et des procédures de mise en place de ces certifications. La nécessité d'une certification du niveau des sécurité des appareils qui se connectent aux réseaux européens n'est pas récente, mais elle a connu une impulsion particulière sous les présidences allemande en 2020[18] et française en 2021 du Conseil de l'Union Européenne[19].

Appliquer un schéma de certification défini par l'UE à un tissu industriel extrêmement hétérogène en ressources, et en développement a fait craindre un nivellement par le bas du niveau de sécurité. Cela d'autant plus que la légitimité même de l'ENISA était mise en doute. C'est l'une des raisons pour laquelle l'avancement de l'ENISA d'un statut simplement consultatif à des tâches cruciales, notamment l'harmonisation des règles de sécurité et la création de nouvelles normes communes ne s'est pas faite sans une opposition manifeste des sénateurs français et de l'ANSSI[20]. Ceux-ci lui reprochaient un manque de compétence avérée dans le domaine de la cybersécurité.[21]. La substitution de l'ENISA aux EM pour ce qui est de la certification et la défense nationale (à travers les OIV) était considérée en conflit total avec le principe de subsidiarité. L'ENISA récupèrerait également la prérogative de certification, se substituant alors aux agences nationales telles que l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI), ou l'agence fédérale allemande *Das Bundesamt für Sicherheit in der Informationstechnik* (BSI). Le Sénat français a ainsi estimé que la cybersécurité est intimement liée à la sécurité nationale, celle-ci étant une prérogative régalienne. Cette dernière n'étant pas soumise aux règlements européens, la cybersécurité ne devrait pas être contrôlée par un organe central, doté, qui plus est, d'un pouvoir de sanction. Car la nouvelle ENISA aurait eu, initialement, la capacité de déclencher des enquêtes techniques, à la demande de la Commission européenne ou de plusieurs EM, dans l'éventualité d'un incident affectant tout ou partie de l'UE. D'autre part, la crainte de se voir imposer un schéma de certification nivelé par le bas[22] ne plaisait ni aux Français, ni aux Allemands, qui avaient déjà des certifications exigeantes en place. La France a finalement voté en faveur du règlement. Par ailleurs, au niveau des EM, on remarque la Croatie, le seul pays qui n'a pas voté en faveur mais s'est abstenu. Serait-elle destinée à devenir un "passager clandestin" ?

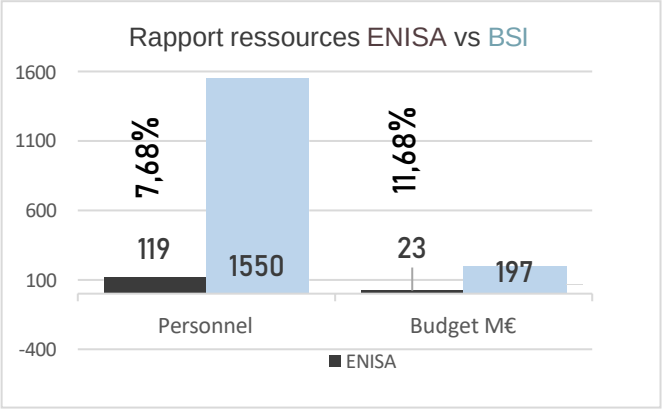
Certaines des initiatives de Bruxelles ne rencontrent pas l'adhésion des EM, ce qui témoigne des difficultés de Bruxelles à convaincre les EM de la nécessité d'une intégration plus poussée. Dans ce cas, des projets *à la carte* voient le jour et la participation est volontaire, comme c'est le cas des projets de l'European Defense Agency (EDA) tels que les projets PESCO sur lesquels nous reviendrons. En dépit des éventuelles critiques et oppositions qui ont pu agiter les EM, il est à noter que ces frictions n'ont pas empêché l'adoption des directives et règlements aujourd'hui en vigueur puisque ni la *Directive NIS*[23], ni le *Cybersecurity Act*[24] n'ont connu de vote contre, à l'image de nombreux votes dans le domaine du numérique où le consensus semble être la règle.

Priorité aux prérogatives et fragmentation des ressources

De nos jours, le paysage de la cybersécurité européenne est bien complexe car cela concerne non seulement des institutions nationales, mais aussi européennes. Rien que la cybersécurité en France est éclatée entre au moins 60 structures organisationnelles nationales[25] et européennes actionnables avant, pendant et après une crise ou un incident cyber (Annexe V). Pour l'Espagne la situation n'est guère différente. Bien que l'organisation soit différente, plusieurs ministères et organisations organisent la cybersécurité espagnole[26] qui est de la compétence de quatre ministères : le palais de la Présidence du Gouvernement espagnol, le Ministère de la Défense et du Renseignement, le Ministère de l'Intérieur et le Ministère de l'Economie.

L'Europe compte plus de 660 centres d'expertise en cybersécurité[27] parsemés à travers les EM. Un pareil arsenal d'agences, comités, groupes de travail ou d'échange, interpelle par son ampleur et sa réelle efficacité. D'autre part, l'effort (budgétaire, mais aussi politique) variable consacré par chaque pays pèse irrévocablement sur la solidité de toute la cybersécurité européenne. Fragmenter les instances consultatives en charge de sa gestion peut effectivement paraître illogique. Enfin, une telle variété et un si grand nombre d'organismes a, au moins en théorie, peu de chances de se montrer efficace dans son ensemble. Qu'en est-il en pratique ?

Lorsque ENISA avec 119 d'employés et 23 millions d'euros de budget en 2021[28] est chargée de coordonner 27 agences de cybersécurité nationales et de catalyser tout l'écosystème cyber européen, alors que la



Données 2021 AFP et BSI

seule agence fédérale allemande (BSI) compte plus de 1550 agents pour un budget de plus de 197 millions d'euros[29], questionner son efficacité et sa légitimité est plus que nécessaire.

Les projets de l'UE nécessitent également une assise financière solide et bien gérée. Mais en 2019, la Cour des Comptes Européenne (ECA) fait état d'un rapport de 1/10 entre les dépenses de certains EM exprimées en pourcentage du PIB et celles des États-Unis en matière de cybersécurité[30]. Enfin, certains EM peinent à trouver les moyens et l'expertise nécessaires à la création d'une telle autorité efficace. Au-delà des questions matérielles, des raisons culturelles et historiques peuvent également expliquer la réticence de certains pays à voir s'ériger de nouveaux organes responsables de la sécurité de l'information. Dans certains pays où les agences de cybersécurité sont bien implantées et dotées d'une véritable expertise, les caractéristiques mêmes de l'organisation étatique (fédéralisme, provinces autonomes) ou administrative peuvent constituer des freins, ou, au contraire, des aides non négligeables. Les ressources sont non seulement faibles mais également fragmentées, peu précises et rarement accompagnées de programmes de coopération gérés par les pouvoirs publics. La nature trans-sectorielle de la cybersécurité, ainsi que l'impossibilité de séparer parfois les dépenses cyber des dépenses informatiques en sont la cause. La Cour des Comptes[31] déplore l'impossibilité d'obtenir des statistiques fiables ni de la part du secteur privé ni du secteur public puisqu'elle estime à trois quarts le nombre des institutions supérieures de contrôle qui ne disposent pas d'une vue centralisée des dépenses publiques cyber. D'ailleurs, aucun EM n'impose d'écritures distinctes pour les dépenses de cybersécurité dans les documents financiers.

À défaut de connaître les budgets attribués et leur alignement avec les besoins, une optimisation des dépenses se révèle impossible. La Cour Européenne confirme l'absence d'un budget spécifique consacré à la stratégie de cybersécurité. Au niveau de l'UE, les dépenses en matière de cybersécurité sont plutôt financées par le budget général et le cofinancement des EM. Pas moins de dix instruments différents relevant du budget général de l'UE y contribuent, mais il est impossible de déterminer avec précision quels crédits sont utilisés à quelles fins. Les sommes allouées aux projets de cybersécurité se partagent entre plusieurs technologies sans priorisation réelle de ces technologies en lien avec la *EU-CSS*[32] (Annexe VI).

Bien que l'évaluation du budget alloué pour la cybersécurité aux institutions européennes reste une tâche impossible du fait de cette fragmentation, les ressources allouées sont souvent extrêmement faibles par rapport à d'autres domaines de sécurité et à d'autres régions du monde. Par exemple, pour 2023, le Pentagone a demandé que des fonds d'une valeur de 11,2 milliards de dollars soient alloués à la cybersécurité. À titre de comparaison, l'ENISA disposera d'un budget annuel de 24 millions d'euros en 2023, alors que *The European Cybercrime Centre* (EC3), au moment de sa création en 2013, avait un budget initial de 7 millions d'euros et comptait 40 employés. Suites à des entretiens avec des représentants des institutions européennes, les chercheurs Carrapico et Barrinha concluaient en 2017 à une gestion déficitaire[33] :

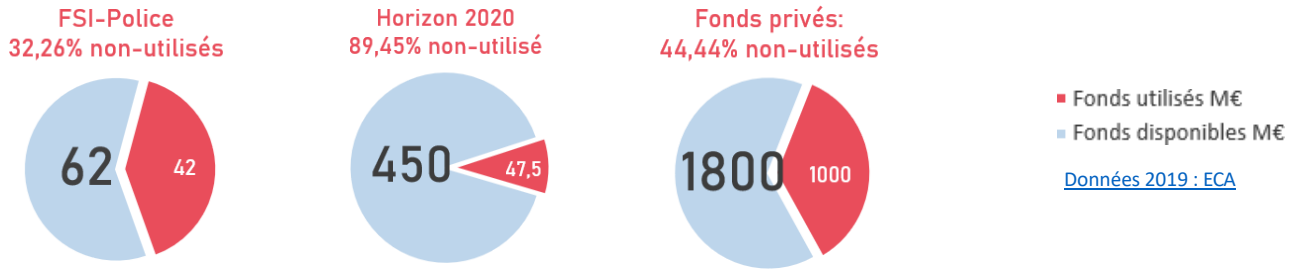
> *There are co-ordination problems between, but also within institutions, which are related to the historical evolution of the different cybersecurity areas, as well as the perception that each area still experiences different separate challenges. It is not unusual to find projects whose objectives clash with those of other institutions (Interview, European Parliament, 2016). Furthermore, states, via the Council, seem to be more reluctant than other institutions (such as the European Parliament) to enhance EU powers in this area (Interview, CERT EU, 201*

Cela est également valable pour les aides aux investissements. L'absence globale, au niveau de l'UE, de suivi des financements - quels crédits sont utilisés, par qui et à quelles fins - ajoute une probabilité élevée de distribution inégale et peu pertinente entre les différents secteurs d'action de la cyber (gouvernance, risque, technologie). Ainsi, des technologies critiques pouvant recevoir moins de soutien que d'autres plus "à la mode" ou plus profitables. Cette fragmentation des ressources humaines et

financières et cette dissipation organisationnelle mènent, au bout du compte, à un manque de visibilité et de transparence qui entravent l'accès aux financements. C'était le cas du partenariat public-privé contractuel (PPPc) conclu en 2016 pour stimuler le secteur de la cybersécurité en Europe. Après une période de 18 mois (sur les 4 années du partenariat), les fonds octroyés au titre d'*Horizon 2020* s'élevaient à 67,5 millions d'euros sur les 450 millions d'euros injectables par le programme et à 1 milliard d'euros des 1,8 milliard d'euros supplémentaires que le PPP aurait dû attirer de la part du secteur privé[34].

La lutte contre la cybercriminalité sert aussi d'exemple, puisqu'elle bénéficie du soutien du volet Police du *Fonds pour la sécurité intérieure* (FSI-Police). Le FSI-Police a consacré 62 millions d'euros entre 2014 et 2017 pour financer des études, des réunions d'experts, de collecte de données et des activités de communication. Dix-neuf EM sur 28 ont fait appel à ces subventions, pour un montant total de 42 millions d'euros.

Le 20 juillet 2022, la Commission Européenne a annoncé le financement à hauteur de 1,2 milliard d'euros de 61 projets collaboratifs de recherche et de développement dans le domaine de la défense. Le Fond Européen de la Défense (FED) soutiendra les projets de capacité haut de gamme tels que la conception d'avions de combat, de chars, navires ainsi que le nuage militaire, l'IA, le cyberespace. Cette initiative vise également la R&D des PME européennes. Les projets sont sélectionnés selon les priorités en matière de capacités de défense convenues par les EM dans le cadre de la politique de sécurité et de défense communes (PSDC).



Si le commissaire au marché intérieur Thierry Breton vantait justement cet investissement *« Nous dépensons mieux en dépensant collectivement. Les États membres et l'industrie européenne de la défense en bénéficieront tous, quelle que soit leur taille »*[35], il est impératif de ne pas s'en contenter. Cette initiative devra se répéter avec des sommes encore plus importantes pour assurer l'autonomie de chaque pays membre de l'UE dans l'espace cyber. Une coopération macro-régionale et politique est donc nécessaire dans le champ de bataille du cyberespace où la souveraineté est primordiale par souci d'indépendance stratégique, selon le général de division aérienne Didier Tisseyre,[36] :

> *Vous m'avez demandé ce qu'il en était de notre souveraineté, notre indépendance, notre autonomie nationale. L'autonomie stratégique nationale coûte cher. Nous sommes autonomes sur le plan du chiffrement, par exemple. Ce sont des chiffreurs français, avec des composants français, toute une procédure française, et cela a un coût. Cette cyberprotection régalienne, c'est la moitié des investissements budgétaires en matière de cyber au sens large.*

En juillet 2022 la Commission Européenne confie 500 millions d'euros à *European Defense Industry Reinforcement through common Procurement Act* (EDIRPA). Suite à l'invasion russe sur le sol ukrainien, cet outil répond aux besoins militaires les plus urgents et les plus critiques tout en incitant les EM à travailler conjointement et éviter le piège de la concurrence. À travers les besoins militaires il reste à évaluer si du matériel informatique dédié à la cyberdéfense a été acquis grâce cet investissement.

Par ailleurs, la fragmentation organisationnelle rend difficile la mise en place d'une stratégie trans-nationale cohérente au service des besoins de l'Union. La création en 2021 du *European Cybersecurity Competence Centre and Network* (ECCC) devrait répondre à cet impératif de gestion centralisée des fonds de cybersécurité dans le cadre du prochain cadre financier pluriannuel 2021-2027. La coopération avec le *Network of National Coordination Centres* (NCCs) aidera les parties prenantes à tirer le meilleur parti des ressources et de l'expertise existantes en matière de cybersécurité dans toute l'Europe, et notamment dans les 660 centres de compétence présents dans les EM. C'est un excellent exemple de coopération institutionnelle verticale entre un organisme de l'UE et ses EM qui vise, après tout, la construction d'une forte communauté cyber européenne.

Mais lorsque les ressources budgétaires doivent couvrir un grand nombre d'agences et les ressources humaines s'éparpillent à travers nombre d'organisations, leur insuffisance est plus que flagrante. Certaines procédures d'achat de matériel ou d'embauche de nouveaux talents sont lentes alors que le paysage cyber change sans cesse. Dans ce contexte il faut saluer la solidarité des EM qui accompagnent financièrement la participation d'experts nationaux dans le cadre de la *Force d'action anti-cybercriminalité européenne* (J-CAT) du centre EC3 d'Europol. Mais cela n'est pas soutenable dans la durée et peut détourner certains états de ces missions. Si la solution d'un déploiement temporaire, au cas par cas, avec certains financements d'Europol et du cadre du cycle politique de l'UE permet à davantage de pays de participer, cela reste un rafistolage difficile à comprendre vis-à-vis de l'ambition en matière de sécurité numérique affichée par l'Europe.

Cependant, l'UE aspire à avoir l'environnement en ligne le plus sûr du monde. La réalisation de cette ambition requiert des efforts considérables de la part de tous les acteurs concernés et impliqués. Mais les EM se trouvent à des niveaux de ressources, de compétence et de préparation très variables. Pour certains pays comme la Bulgarie, la Hongrie, la Roumanie, la cybersécurité est un sujet de discussion récent alors que d'autres états comme les Pays-Bas et l'Estonie en ont un passé déjà bien riche. Cela crée des situations où certains états (France, Italie, Pays-Bas, Allemagne) poussent pour un cadre de cybersécurité plus renforcé que celui prévu aujourd'hui, alors que d'autres pays souhaitent une coopération subrégionale. C'est l'exemple des pays de Visegrad plus l'Autriche qui en fondant *The European Cyber Security Platform* (CSCSP) veulent promouvoir la coopération entre les CERT et les CSIRT respectifs. Dans ces conditions, la coordination n'aboutit que rarement et l'approche n'est plus globale. Elle risque de se fragmenter et de favoriser le développement d'une cybersécurité à deux vitesses. Le risque est que le cadre légal ne soit plus respecté et que des monopoles industriels se substituent, à travers leurs lobbies, à la voix de l'UE.

En 2019, la Cour des Comptes Européenne a interrogé les institutions supérieures de contrôle nationales sur leur expérience en matière d'audit de la politique de cybersécurité. La moitié des répondants n'en avaient aucune. Le rapport met en avant des différences des audits d'un pays à l'autre[37] :

> *Independent oversight of the implementation of cybersecurity policy differs between Member States. We surveyed national audit offices on their experience in auditing this field. Half of all respondents had never audited the area. For those that had, the main focus of audits had been on: information governance; protection of critical infrastructure; information exchange and coordination between key stakeholders; incident preparedness, notification and response. Among the subjects less covered were awareness-raising measures and the digital skills gap.*

Les 12 pays interrogés cumulent 43 audits réalisés entre 2013 et 2019, dont 35 ont été rendus publiques. La France et le Danemark sont les plus assidus, avec 7 et 6 audits respectifs, suivi par le Royaume-Uni et la Pologne avec 5 audits chacun. Certains États recueillent des informations sur le cyberespace mais l'UE n'a pas formulé le besoin de consolider aujourd'hui ces données. L'ANSSI par exemple enregistre uniquement les données concernant les attaques contre des organisations publiques et partiellement sur les OIV. Les données relatives aux acteurs industriels, surtout les PMI, sont difficiles à rassembler donc sont peu collectées. De surcroît, la sécurité nationale est encore trop souvent invoquée comme raison de non partage de l'information. Anne Tricaud de l'ANSSI précise que le partage est toujours lié à un intérêt précis : « On partage parce qu'on a intérêt de partager et parce qu'on a protégé la manière dont on partage. Mais on ne partage pas pour partager ». C'est un partage validé par une gestion des risques préalable et non pas par la confiance réciproque. La *Directive NIS* tente d'harmoniser et de solutionner ces arguments mais elle a le défaut de ne viser que très peu des acteurs du tissu industriel et économique européen. La Cour des Comptes attire donc l'attention sur le fait que les résultats sont rarement mesurés et peu de domaines d'action peuvent être évalués. Les preuves concernant l'impact de choix politiques font défaut, ou sont ambiguës en l'absence de données fiables concernant l'ampleur des bénéfices potentiels obtenus par la coopération ou les coûts de son absence. Définir des critères d'évaluation pertinents n'est pas simple. En outre, de manière générale, le domaine de la cybersécurité n'est pas structuré par des procédures facilement quantifiables, ce qui fait que l'évaluation rigoureuse n'est pas encore devenue la norme. Il est donc nécessaire de passer à une culture de la performance intégrant des

pratiques d'évaluation et un système normalisé de rédaction de rapports écrits. Actuellement, le mandat de l'ENISA ne couvre ni l'évaluation, ni le suivi de la situation, ni l'état de préparation de l'UE en matière de cybersécurité. Les rares évaluation du déploiement des politiques EU, la *Directive NIS* et la *5G Security Toolbox* ont été faite par la Commission.

Mais des prérogatives seulement tournées vers l'évaluation quantitative des impacts des politiques européennes ne résolvent pas le problème car pour quantifier il faut suffisamment de mesures, de données, de statistiques fiables, et ce pour pouvoir suivre et analyser les tendances et les besoins. Pour ce faire, l'ENISA multiplie les outils. Elle publie en 2014 *An Evaluation Framework for National Cyber Security Strategies*. C'est un cadre d'évaluation pouvant se montrer utile lors de l'évaluation de la conformité des EM à la *EU-SS* mais qui se réduit à une liste des cases à cocher. En 2018 suit un outil d'évaluation de la stratégie cyber destiné aux EM : *National Cybersecurity Strategies Evaluation Tool*. Il s'agit d'une centaine de questions auxquelles répondre en une trentaine de minutes et qui permettrait, en fonction des priorités stratégiques choisies par l'EM, de formuler des mesures d'amélioration. Cet outil a le mérite de permettre une mise en route interactive et simple. Cinq ans après sa mise en ligne, nous n'avons pas trouvé d'information quant à l'utilité ou à l'usage de cet outil, ne serait-ce qu'en nombre de connexions à la page internet de l'outil. L'évaluation des mesures implémentées reste finalement rare, difficile et toujours facultative.

États membres – secteur privé : une frontière qui persiste

L'interdiction des équipements chinois par certains pays offre une opportunité de développement pour les vendeurs et les petits acteurs européens adeptes des solutions de virtualisation open source. C'est aussi l'occasion d'une coordination entre l'UE et le secteur privé. Ainsi, en novembre 2021, cinq grands groupes de télécommunications, Deutsche Telekom, Orange, Telefónica, Telecom Italia (TIM) et Vodafone Group, ont formé l"Alliance Open RAN et ont publié un rapport commun pour souligner l'urgence d'une coordination sur l'Open RAN. Le rapport, qui s'adresse aux décideurs politiques, aux États membres et à l'écosystème au sens large, conclut que, pour que l'Europe reste compétitive à l'ère de la 5G mais aussi de la 6G, l'Open RAN doit devenir un pilier de la politique industrielle et de la stratégie Digital Compass. Le rapport souligne également le risque que l'Europe prenne du retard par rapport au reste du monde - il y a 13 acteurs majeurs de l'Open-RAN en Europe contre 57 ailleurs - la majorité des télécoms européens étant aux premiers stades de développement sans relations commerciales en place. Ces opérateurs sont des partisans actifs de cette technologie. En juin 2021, ils ont également exprimé leurs priorités techniques pour l'Open-RAN dans un livre blanc. Ce document regroupe les exigences communes de DT, Orange, TIM, Telefónica et Vodafone, suite au protocole d'accord qu'ils ont signé précédemment. Le livre blanc est conçu pour montrer aux fournisseurs où se concentrer pour permettre des déploiements européens basés sur les calendriers des opérateurs.

Qu'est-ce que l'Open RAN ?

Open Radio Access Network se propose de casser la logique traditionnelle selon laquelle le réseau mobile repose sur une pile (*stack)* - radios, matériel, logiciels - issue d'un même fournisseur. Son objectif est donc la désagrégation à travers la virtualisation open source et du matériel « white box ».

Pour les opérateurs, Open RAN ouvre la porte à une réduction des coûts et du time-to-market, à plus d'innovation et à moins de dépendance. Avec la multiplication des points de chute potentiels, la sécurité devient aussi un enjeu majeur, tout comme la qualité de service.

Il est important que les opérateurs de télécommunications travaillent en collaboration avec les fournisseurs afin que tous aient les mêmes attentes, y compris la prise en charge des modèles d'intégration "mix and match" afin d'éviter le verrouillage des fournisseurs. Des projets de collaboration se mettent en place justement dans cet esprit réunissant opérateurs américains, japonais, coréens, allemands, britanniques et français[38]. La réponse de l'Europe a été publiée le 11 mai 2022 à travers le Rapport *Cybersecurity of Open Radio Access Networks*. Selon ce rapport, la technologie Open RAN offre des opportunités réelles mais présente également des risques de sécurité, surtout à court terme, de par la complexité qu'elle rajoute, dans un environnement peu mature. L'Europe décide donc d'attendre que les vulnérabilités soient mitigées avant de soutenir à plus grande échelle l'Open RAN.

Il ne faut pourtant pas oublier que l'Open RAN repose sur une désagrégation du matériel et du logiciel et donc sur le Cloud. Une approche Open RAN à grande échelle peut entraîner un nouveau verrouillage des fournisseurs pour les opérateurs de réseaux mobiles du côté matériel, principalement Intel (qui équipe

la majorité des plateformes), et du côté du Cloud publique. Aujourd'hui, les sociétés de logiciels (dont beaucoup sont des start-up) sont pour la plupart états-uniennes[39] et parfois israéliennes, mais elles sont souvent financées par les États-Unis ou dépendent de ce pays. Cela signifie qu'en fin de compte, à vouloir éviter les Chinois et attendre que l'Open RAN gagne en sécurité, on est en train de déplacer le verrouillage des fournisseurs vers les États-Unis. Sans parler de l'occasion manquée de prendre le leadership et de développer une offre industrielle à l'échelle du continent.

La cohérence européenne à l'épreuve du dumping chinois

Le manque de coopération n'est pas la seule cause d'un manque de cohérence, concept regroupant ici un alignement entre la vision et l'action. Aujourd'hui, la situation politique, économique et sociale est particulièrement instable et le manque de visibilité sur l'avenir est certain. Dans de tels moments, le manque de communication peut porter préjudice à cette cohérence tant recherchée par les institutions européennes. Ce fut le cas lors du dumping économique exercé par le chinois Huawei en Europe.

Pour les entreprises de télécommunications qui achètent des équipements de réseau - et les gouvernements nationaux qui les réglementent - les risques de sécurité associés aux équipements Huawei sont difficile à quantifier. Mais le coût associé au choix d'un autre fournisseur (Ericsson, Nokia ou Samsung) et au renoncement aux incitations lucratives que Pékin offre aux clients de Huawei est immédiat et mesurable. Et pour cause, celui-ci affiche en Europe des prix si concurrentiels qui pourraient presque ne pas couvrir la fabrication du matériel[40]. Toutefois, en 2015 la Chine et l'UE ont signé une déclaration commune sur la coopération stratégique sur la 5G, s'engageant à la réciprocité et à l'ouverture en termes d'accès aux réseaux 5G, de financement de la recherche et d'accès au marché[41]. En 2017, la Chine a adopté une loi sur le renseignement national[42] stipulant que toutes les organisations et les organisations et citoyens chinois doivent collaborer au renseignement national, avec des garde-fous en matière de secret Après les États-Unis, En mars 2019, le Parlement européen[43] a également exprimé ses inquiétudes quant au fait que les fournisseurs chinois de 5G chinois pourraient présenter un risque de sécurité juridique pour l'UE.

La pésence massive en Europe de Huawei est rendue possible par le soutien apporté par la Chine à Huawei et à ses états clients à travers les banques étatiques chinoises. Elle en a fait son champion national en lui fournissant des subventions directes et indirectes (222 millions d'euros de subventions gouvernementales, dont 64 millions d'euros pour la recherche et le développement[44]), notamment une part de marché garantie en Chine, la gratuité de la bande passante[45] et des crédits arrangeants accordés à travers les banques d'État chinoises[46] - qui réduisent les coûts opérationnels, accélèrent la mise sur le marché des produits 5G de Huawei et lui permettent de fixer des prix bien inférieurs à ceux de ses concurrents. *« C'est un niveau de subvention gouvernementale directe pour une entreprise qui serait inédit aux États-Unis ou en Europe »*[47], a déclaré Stephen Ezell, expert en politique technologique mondiale à l'Information Technology and Innovation. Pour cause, en 2010 le Commissaire européen au commerce, Karel De Gucht, a ouvert une enquête sur les pratiques anticoncurrentielles de Huawei. Selon les conclusions du rapport, l'entreprise vendait ses produits à un prix inférieur à ce qu'il lui en coûtait pour les produire[48] :

> *Il était clair que Huawei faisait du dumping. […] Nous avions de nombreuses preuves. Et nous sommes arrivés à la conclusion que cela nuisait à l'avenir et aux perspectives à long terme de nos entreprises européennes.*

Bien qu'elle n'ait jamais publié ses résultats, la Commission a conclu que Huawei pratiquait des sous-enchères allant jusqu'à 70 % par rapport à ses concurrents, a précisé Karel De Gucht. Malheureusement, au lieu d'appliquer des remèdes commerciaux, la CE a conclu en 2014 un accord avec Pékin selon lequel Pékin promettait d'accorder un meilleur accès au marché chinois à Ericsson, Nokia et Alcatel-Lucent pendant que la Commission promettait de ne pas agir sur les subventions chinoises qui faussent le marché.

Neuf ans après, les équipementiers européens possèdent à peine 4% du marché chinois. En 2022, les parts de marché d'Ericsson en Chine ont encore chuté brusquement. La décision de la Suède d'interdire les équipements chinois pour la 5G en est la principale cause. Dans ce cas précis, entre l'enjeu économique et l'enjeu sécuritaire, le premier l'a emporté. Les entreprises privées savent qu'un environnement incertain peut limiter la consommation, l'investissements, la recherche. Les politiques et réglementations mises en place par l'Europe vis-à-vis des nouvelles technologies sont nombreuses, mais les arbitrages politiques de la Commission Européenne insinuent le doute quant aux réels intérêts poursuivis par l'UE.

Consensus autour de la certification européenne

Bien qu'en retard sur le plan industriel, on envie à l'Europe la capacité d'évaluer et de certifier la sécurité d'un matériel ou d'un service. Dans ce contexte, la décision de l'EU de coordonner la définition de normes de cybersécurité communes constitue une solution de promotion du savoir-faire technologique et du leadership industriel de l'Europe en faveur d'une meilleure interopérabilité des systèmes. L'enjeu d'une certification commune vise directement l'interopérabilité des systèmes dont la complexité opérationnelle pourrait être rendue difficile par un paysage de certifications hétéroclite. Pour atteindre cet objectif, les EM et les acteurs privés devraient participer activement à l'élaboration de ces normes européennes et certifications, y compris en apportant leur soutien à la définition de profils de protection spécifiques pour chaque typologie de technologie.

À partir du moment où un schéma de certification a été inscrit dans *le Cybersecurity Act*, l'ANSSI s'est mise à travailler avec la BSI allemande[49] en vue d'un accord afin d'imposer leurs schémas de certification respectifs au niveau européen. L'Estonie, l'Espagne et l'Italie ont également participé activement aux débats. Pour le Cloud certifié au niveau substanciel (deuxième niveau), les exigences de la brique 5C de la BSI ont servi comme source d'inspiration. Pour le niveau élevé (troisième niveau), en revanche, c'est le référenciel de certification français SecNumCloud qui a servi de modèle ; celui-ci formule des exigences afin de limiter l'impact des lois d'extra-territorialité. Selon Franck Sadmi, Chef de division adjoint Produits et Services de sécurité à l'ANSSI, l'intérêt de la certification est de rationnaliser l'ensemble des schémas d'évaluation pour faciliter l'identification du niveau de confiance voulu par le fournisseur[50]. Il s'agit bien de confiance et non pas de sécurité car la certification est volontaire et son premier nveau est purement déclaratif. Toutefois, ce schéma a le mérite d'avoir posé les bases pour des certifications privées dont nous parlerons dans le Chapitre 3.

À la lumière des exemples cités, il apparaît que la cohérence des politiques européennes est entravée par des ressources financières limitées, un faible effectif (arrivé à saturation) dans les EM investisseurs et une division confuse des missions tant au niveau de l'EU que des EM. Sur l'axe vertical on gagne en cohérence grâce à l'européanisation des stratégies de cybersécurité à travers, entre autres, aux effets de la *Directive NIS* et au *RGPD* (conformité commune des politiques de cyber sécurité). Une contradiction de taille est pourtant à noter : d'une part, l'Europe est consciente des limites d'une approche nationale de la cybersécurité, par son caractère transnational et par l'hétérogénéité du niveau de maturité cyber des EM. De l'autre, *la Stratégie EU-CSS* promeut une organisation décentralisée où la gouvernance de la cybersécurité reste dans les EM avec tous les avantages et les inconvénients afférents (ressources, volonté politique, etc.), alors que l'UE se charge de construire des capacités communes et de faciliter la coordination et la communication entre les EM. La coordination accrue voulue par les institutions, inscrite dans nombre de documents n'a pas toujours apporté la preuve de pratiques coordonnées, ce qu'analysera encore plus en détail le chapitre suivant. Cela est aussi dû à un manque d'objectifs mesurables. Certes, le lien de cause à effet est presque impossible à déterminer dans la cybersécurité et donc l'efficacité des mesures (législatives ou autres) ne peut pas encore être pleinement évalué. De plus, même si cela était possible, le caractère récent de ces mesures rendrait leur évaluation peu pertinente aujourd'hui.

2.2. Une coopération transversale inégale

La coordination horizontale suppose l'élimination des contradictions en termes de procédures et politiques, entités et instruments mis en place par les institutions européennes, les États Membres (EM) et, enfin, les acteurs du secteur privé.

La *EU Cyber Security Strategy – An Open, Safe and Secure Cyberspace* (EU-CSS) de 2013 est le résultat des efforts communs de trois institutions et particulièrement représentative d'une volonté d'apporter davantage de cohérence dans les politiques liées à la cybersécurité.

L'expérience de la coordination au sein des institutions européennes

La coordination institutionnelle européenne est visible à travers l'augmentation du nombre de documents officiels faisant référence à la nécessité d'une coordination plus étroite et à travers la représentation des organes de l'UE, à savoir EC3, ENISA et CERT-EU : directives, règlements-cadre et livres blancs. La procédure législative ordinaire européenne[51], à l'origine des directives cyber, où les trois grandes institutions européennes se confrontent et coopèrent pour rejeter ou adopter un texte, en représente également la preuve.

En juillet 2018, la Commission Européenne et le Committee on Industry, Research and Energy[52] (ITRE), en charge de l'élaboration de *Cybersecurity Act*, ont permis, par un premier vote, de faire entrer le texte en première lecture de négociations interinstitutionnelles, entre la commission, le Parlement, et le Conseil Européen. Les résultats de ce premier vote en Commission ont été les suivants : 56 votes pour, 5 abstentions, et un vote contre. En mars 2019, le vote était soumis au Parlement Européen, dont les résultats ont continué en la faveur de l'adoption du règlement : 585 députés européens ont voté en faveur de la directive, 36 abstentions, et 44 votes contre. Enfin, un mois plus tard, en avril 2019, soumis au Conseil de l'UE, le règlement a définitivement été adopté en première lecture, avec 27 pays votant pour, et un vote abstentionniste de la part de la Croatie[53]. C'est ainsi que le règlement *Cybersecurity Act* a bien vu le jour. Cependant, il aura fallu deux années et trois soumissions au vote pour adopter ce règlement. La transparence de la procédure législative européenne permet d'observer, dès la réflexion quant à son élaboration, les voix divergentes entre les députés et les représentants des EM. Les procédures législatives montrent, à la fois, la complexité et les faiblesses de la diversité européenne. On pourrait se dire qu'une fois adoptée, le règlement est le fruit d'un processus démocratique respecté (c'est d'ailleurs le cas), mais on retiendra aussi que l'unanimité n'a pas eu lieu, que des pays, ou des représentants politiques des EM ne sont pas sur la même longueur d'onde en matière de sécurité de nos systèmes d'information. C'est pourtant un sujet pour lequel l'unanimité semble, en théorie, logique.

Dans ce cas, nous observons une coopération horizontale entre les principales institutions européennes qui fonctionnent, bien que cela prenne du temps (des années), des consultations, des procédures de vote, pour arriver à une adoption. Ensuite, il faut rajouter environ deux ans pour le déploiement - en fonction de l'urgence à laquelle le texte doit répondre -, de son contenu, des délais estimés, et surtout de la capacité à mesurer sa bonne application. Dans le cas du *Cybersecurity Act*, on peut dire que le travail est en cours. Le nouveau champ d'action de l'ENISA (qui a été à l'origine de la discorde[54]) est d'ores et déjà effectif puisque l'ENISA assume à ce jour ses nouvelles missions. En revanche, le déploiement de la certification européenne (dont l'ENISA est le moteur) est difficile à mesurer, aussi bien en ce qui concerne les entités volontaires, que l'efficacité et les résultats de cette certification.

Source : 2019 - Déclaration de la Commissaire européenne Mariya Gabriel sur l'entrée en vigueur de la loi européenne sur la cybersécurité.

Des outils encourageant la coopération entre États membres

Les EM restent opposés à l'idée de laisser les prérogatives de la cybersécurité entre les mains de l'UE et ce car la cybersécurité est avant tout une problématique locale, elle concerne avant tout le citoyen, le tissu économique, et les institutions d'un pays. Les différences considérables entre les EM du point de vue de leurs capacités technologiques et de différents degrés d'engagement ne les a pourtant pas empêché d'approuver à la majorité absolue la directive NIS, ni de considérer la menace comme un enjeu européen. Si la coordination institutionnelle s'avère plus facile à mettre en œuvre, rares sont les preuves de pratiques coordonnées.

Chaque année lors de la publication de *Digital Economy and Society Index*, la Commission Européenne et le Conseil de l'UE s'accordent à affirmer pourtant que le développement numérique de l'Europe est en retard par rapport au reste du monde. Bien que 80[55] % des entreprises de l'UE aient subi en 2016 au moins un incident lié à la cybersécurité, la prise de conscience des risques reste, selon ces institutions d'une faiblesse alarmante. La Cour des Comptes Européenne confirme qu'en 2019, dans l'UE, 69% des entreprises n'ont qu'une compréhension de base, voire aucune compréhension, de leur exposition aux cybermenaces[56], tandis que 60 % n'ont jamais évalué les pertes financières potentielles[57]. Par ailleurs, selon une étude mondiale de AON[58] de 2020, un tiers des organisations ne prend pas de mesure pour protéger les secrets d'affaires (évalués à 1 trillion de dollars de pertes annuellement) et moins de 10 % des opérations de fusion et d'acquisition font de la due diligence préventive en matière de cybersécurité. De plus, en 2021, 32% des organisations ont décidé de verser une rançon après attaque et le pourcentage ne cesse d'augmenter[59].

La coopération horizontale entre certaines autorités nationales peut prendre la forme d'une reconnaissance mutuelle de certifications, qui, par leur exigence, serait difficilement applicable à l'ensemble des EM. En effet, l'ANSSI et le BSI ont signé un accord de reconnaissance mutuelle des certificats de sécurité[60]. Il s'agit de certificats de sécurité pour les schémas CSPN (Certification de Sécurité de Premier Niveau) et BSZ (Beschleunigte Sicherheitszertifizierung). L'accord a vocation à couvrir l'ensemble des certificats émis par les deux schémas (CSPN et BSZ) mais certains certificats peuvent en être exclus s'ils sont, par exemple, soumis à une réglementation nationale spéciale. Cet accord pose les bases d'une coopération renforcée entre les organismes de certification de l'ANSSI et du BSI et posera la base d'une harmonisation européenne des schémas de certification telle qu'elle est inscrite dans *Cybersecurity Act* et sur lesquels nous reviendrons dans le Chapitre 3. La norme européenne *Fixed Time Cybersecurity Evaluation Methodology for ICT products* (FiTCEM - prEN 17640), en

cours d'élaboration, permettra d'étendre au niveau européen l'harmonisation des pratiques, notamment via la création d'un système européen de certification basé sur *le Cybersecurity Act*. La volonté du secteur privé de collaborer avec les institutions pour une gouvernance commune de la cybersécurité existe, mais les résultats ont jusqu'à présent été limités. D'une part, les attaques se multiplient à tous les niveaux et ciblent tous types d'organisations, y compris les entreprises de plus petite taille, hors du champ d'intervention des agences nationales et européennes, car considérées peu critiques. Néanmoins, ces entreprises représentent le maillon faible d'une chaîne que l'on souhaite forte puisqu'elles ne sont, en général, pas en capacité de répondre aux incidents, faute d'effectifs suffisants ou de compétences *in situ*.

Dans cette situation, la solution pour démultiplier les capacités d'intervention est le secteur privé. Celui-ci, par le biais des prestataires certifiés en réponse à incidents ou en audit, peut y contribuer et compléter l'action nationale. Les Directives européennes ont été pensées pour ça, car il faut avant tout certifier le secteur privé. L'Europe a déjà l'expérience de certification de produits, par le biais de la *Directive NIS*. À présent il s'agit de certifier des entreprises de service ; soit des entreprises qui vont de fait, s'introduire dans les systèmes d'information d'entreprises, et accéder au cœur de cible des cyberattaquants. La certification de prestataires privés est, par conséquent, cruciale, fort stratégique et répond à un double enjeu : de résilience et de confiance. La capacité du privé va s'avérer efficace dans deux situations. La première est pour pallier à la saturation des capacités de réponse en cas de crise de grande ampleur. La seconde vise à réguler davantage, en certifiant des entreprises non OIV ou OES.

Dans sa mission d'insuffler la coopération, l'UE a mis en place des mécanismes spécialement dédiés à la coordination interétatique pourvus d'une mission claire, à l'exemple de Horizontal Working Party on Cyber Issues (2004) et de Network and Information Systems Cooperation Group (NIS Coopération Group, 2014). Le premier est chargé de coordonner les travaux du Conseil sur les questions liées au cyberespace, principalement la politique et les activités législatives relatives au cyberespace. Sa mission est de lister les problématiques en matière cyber soulevées par les EM et de les porter à l'attention du *Committee of the Permanent Representatives of the Governments of the Member States to the European Union* (COREPER) et du Conseil de l'UE. Cela devrait assurer une cohérence entre des domaines très différents tels que la justice criminelle dans le cyberespace et la cyberdiplomatie. Le groupe coopère étroitement avec d'autres groupes concernés, ainsi qu'avec la Commission européenne, SEAE, Europol, Eurojust, l'Agence des droits fondamentaux de l'Union européenne, l'Agence européenne de défense et l'Agence de l'Union européenne pour la cybersécurité. Les principaux objectifs du groupe visent, entre autres :

- à assurer un cadre de travail horizontal permettant une harmonisation et une approche unifiée concernant les questions liées à la politique relative au cyberespace
- à définir et développer la coopération avec les instances préparatoires du Conseil et les autres acteurs concernés
- à assurer un partage d'informations sur les questions liées au cyberespace au niveau des pays de l'UE et des instances nationales

Le NIS Cooperation Group[61] a le mérite d'une portée tant verticale qu'horizontale. Verticalement, le groupe met autour de la table des échanges entre la Commission, les EM et l'ENISA. Horizontalement, il s'agit d'un mécanisme de coopération sur les thématiques de la sécurité de l'information dédié aux EM. Créé pour permettre d'harmoniser la mise en œuvre de la directive, il s'avère un carrefour de coopération très précieux en réunissant les autorités nationales référentes, l'ENISA et la CE. Ce groupe de coopération a su devenir un forum efficace en vue de l'identification des parties prenantes-clés au niveau de chaque EM ainsi que des sujets qui nécessitent des approfondissements pour une meilleure cohérence. Il fournit des orientations au réseau des CSIRT européens. Également créé par la *Directive NIS*, celui-ci réunit les CSIRT nationaux dont les États ont depuis 2018 l'obligation de se doter, et le CERT-EU, organe équivalent de l'Union européenne. Ces deux réseaux de coopération permettent de lier un espace de réflexion et d'élaboration de stratégies concertées avec le groupe de coopération d'une part, et un espace à la dimension plus opérationnelle avec le réseau des CSIRT/CERT-EU d'autre part.

Les profits privés au détriment de la sécurité

Au niveau des acteurs du secteur privé de la cybersécurité, des écarts sont aussi visibles.

Chaque année lors de la publication de *Digital Economy and Society Index*, la Commission Européenne et le Conseil de l'UE s'accordent à affirmer pourtant que le développement numérique de l'Europe est en retard par rapport au reste du monde. Bien que 80%[62] des entreprises de l'UE aient subi en 2016 au moins un incident lié à la cybersécurité, la prise de conscience des risques reste, selon ces institutions d'une faiblesse alarmante. La Cour des Comptes Européenne confirme qu'en 2019, dans l'UE, 69% des entreprises n'ont qu'une compréhension de base, voire aucune compréhension, de leur exposition aux cybermenaces[63], tandis que 60% n'ont jamais évalué les pertes financières potentielles[64]. Par ailleurs, selon une étude mondiale de AON[65] de 2020, un tiers des organisations ne prend pas de mesure pour protéger les secrets d'affaires (évalués à 1 trillion de dollars de pertes annuellement) et moins de 10 % des opérations de fusion et d'acquisition font de la due diligence préventive en matière de cybersécurité. De plus, en 2021, 32% des organisations ont décidé de verser une rançon après attaque et le pourcentage ne cesse d'augmenter[66].

Cela est d'autant plus impactant que les entreprises y jouent un rôle central. Ce sont les entreprises privées, les acteurs du terrain, qui portent à la connaissance des institutions certaines tendances observées depuis leur position en première ligne face aux attaquants. Pour cela, une coordination et un accord intra-sectoriel est d'autant plus souhaitable. Tout comme au niveau des EM, certains secteurs d'activité sont plus matures, avancés et favorables à la coopération (le secteur financier et bancaire) alors que d'autres secteurs craignent que l'échange d'information n'érode pas leurs avantages compétitifs (les télécommunications).

Pourtant, le secteur des télécommunications a l'opportunité d'insuffler la sécurité *by design*, au cœur même des normes internationales qui définissent les protocoles des communications. Pour la 5G, ces normes sont définies par des organismes internationaux de normalisation tels que l'International Telecommunication Union (ITU) et le 3rd Generation Partnership Project[67] (3GPP), le premier étant une organisation intergouvernementale, le deuxième, un consortium d'acteurs privés.

La 5G est destinée à traiter d'énormes volumes de données à grande vitesse ; elle est donc cruciale pour le développement de l'industrie 4.0 et de la défense. Cela marque un net changement. La future dépendance de nombreux services critiques (industries, santé, transports) à l'égard des réseaux 5G rendrait les conséquences d'une perturbation systémique et généralisée particulièrement grave. Les entreprises américaines et européennes détenaient les *Standard Essential Patent* (SEP) lors de la 3G et de la 4G, et les entreprises chinoises devaient payer d'importantes royalties aux entreprises occidentales. Cela est en train de changer. L'entreprise ou l'état qui contrôlera le plus de SEP sera probablement en tête dans la course au développement d'une nouvelle génération d'industries de pointe.

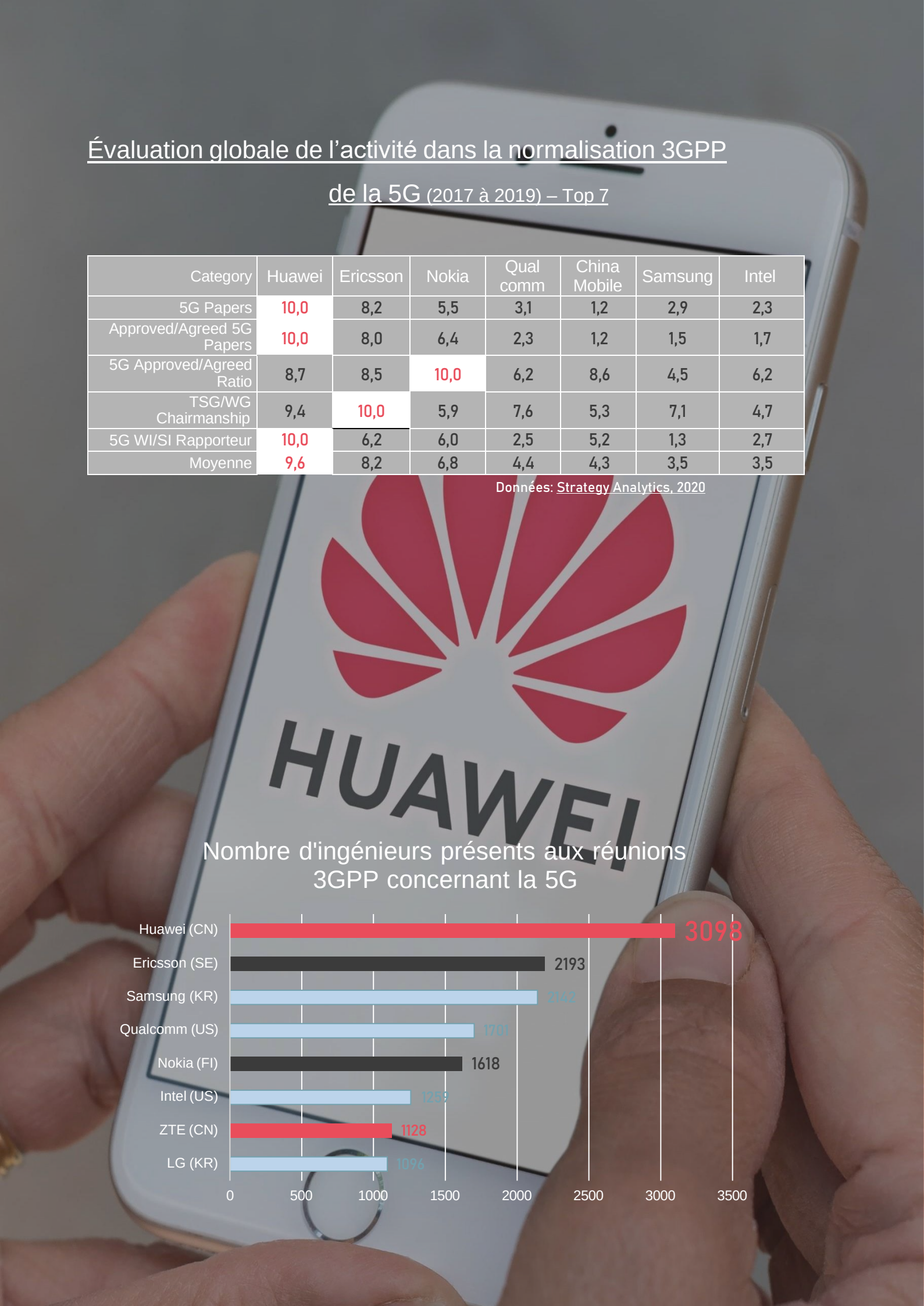
Du point de vue de la sécurité, plus il y aura de brevets intégrant la *security-by-design* et la *privacy-by-design*, plus l'environnement 5G sera sécurisé et utilisé en toute confiance. Par conséquent, garantir la sécurité des réseaux 5G est une question d'importance stratégique pour l'Union Européenne bien présente dans la *Stratégie EU-CSS*. En revanche cela ne semble pas être une priorité pour la Chine qui y voit un moyen d'aligner ces normes à ses objectifs géopolitiques. Comme développé précédemment, la Chine a fait preuve, par le passé, d'utilisation d'Internet et des nouvelles technologies pour des campagnes d'espionnage économique et des actions peu démocratiques de surveillance des populations. La souveraineté technologique voulue par la Chine pourrait passer par un isolement technologique de sa population, c'est déjà le cas pour le Cloud et certains réseaux sociaux. Le bannissement des technologies occidentales[68] est également en cours.

Dans ces circonstances, la participation massive des Chinois dans les groupes de travail de 3GPP et de l'ITU ferait poindre la menace d'une norme 5G peu sécurisée (les Chinois manquent d'expertise dans les

Évaluation globale de l'activité dans la normalisation 3GPP de la 5G (2017 à 2019) – Top 7

Category	Huawei	Ericsson	Nokia	Qual comm	China Mobile	Samsung	Intel
5G Papers	10,0	8,2	5,5	3,1	1,2	2,9	2,3
Approved/Agreed 5G Papers	10,0	8,0	6,4	2,3	1,2	1,5	1,7
5G Approved/Agreed Ratio	8,7	8,5	10,0	6,2	8,6	4,5	6,2
TSG/WG Chairmanship	9,4	10,0	5,9	7,6	5,3	7,1	4,7
5G WI/SI Rapporteur	10,0	6,2	6,0	2,5	5,2	1,3	2,7
Moyenne	9,6	8,2	6,8	4,4	4,3	3,5	3,5

Données: Strategy Analytics, 2020



Nombre d'ingénieurs présents aux réunions 3GPP concernant la 5G

télécommunications mobiles), soit contraire aux droits fondamentaux de la Démocratie. Bien que l'Europe fournisse plus de 44% des délégués, à travers principalement Nokia et Ericsson, ce sont les activités des délégués qui comptent le plus, le nombre comptant dans une moindre mesure. Aussi les États-Unis et l'Australie[69] n'ont pas tardé à décrier un leadership chinois[70]. En Europe, en 2020 déjà, Börje Ekholm, PDG d'Ericsson, confirmait le rôle de leadership de son entreprise dans l'élaboration de la 5G au sein du 3GPP[71] :

> *Depuis 1999, nous avons réalisé plus de 55 000 contributions au 3GPP dans son ensemble. Quel que soit votre point de vue, Ericsson est bien le leader en 3GPP et a influencé la technologie 5G plus que tout autre contributeur.*

Nokia, quant à lui, se félicitait en 2021 d'avoir dépassé le cap de 4000 familles de brevets indispensables à la 5G, fruit des 130 milliards d'euros d'investissements entre 2000 et 2021[72]. Suite à l'audit des contributions des acteurs par Strategy Analytics,[73] les conclusions sont plus mitigées[74] : si Huawei est en tête en termes de contributions globales aux normes 5G de bout en bout, Ericsson est en tête pour la présidence des groupes de spécification technique (TSG) et des groupes de travail (WG), et Nokia pour le ratio approuvé/accepté des documents de contribution 5G. Deux européens seulement font partie du top 13, voire même du top 3 en termes de leadership 3GPP : Ericsson et Nokia. Il est étonnant de noter une participation insuffisante des Américains et surtout l'absence du top 13[75] des 3 premières entreprises de télécom européennes, qui font aussi partie des 10 premières entreprises de télécom du monde : Deutsche Telekom (numéro 3 mondial), Telefónica (numéro 7 mondial) et Orange (numéro 8 mondial)[76] avec Vodafone qui n'est pas très loin. Par ailleurs, l'absence d'Orange interpelle d'autant plus que le groupe emploie plus de 1500 professionnels dans la recherche. Lorsque l'on sait que la 5G permettra la croissance en milliards d'euros qu'on lui attribue si, et seulement si, équipementiers, opérateurs et gouvernements travaillent ensemble, laisser la Suède et la Finlande représenter le monde démocratique serait une grave erreur de stratégie.

Serait-ce un problème de coût ?

La participation aux organismes de certification et normalisation est souvent une dépense non négligeable[77]. La facture monte donc très vite : depuis 1999, Ericsson aurait déboursé pas moins de 186 millions d'euros juste pour ses contributions à la 5G. De son côté, Huawei consacrerait 10 milliards de dollars[78] par an à la recherche et au développement des stations de base 5G, presque le double de Nokia, profitant de généreuses subventions offertes par l'Etat chinois au nom de sa stratégie *Made in China 2025* dont la 5G en est le pilier central.

Par ailleurs, le processus de normalisation prévoit qu'un organisme indépendant intergouvernemental fasse le contrepoids, valide les propositions techniques des acteurs privés et veille à ce que les systèmes de communication mobile bénéficient à tous. La stratégie "take-over"[79] de Pékin a été si bien ficelée qu'aujourd'hui, Pékin a réussi à placer deux des trois principales organisations internationales de normalisation – International Organization for Standardization (ISO) et International Électrotechnical Commission (IEC) - sous son influence. Jusqu'en septembre dernier l'ITU était dirigé par le chinois Houlin Zhao.

Si la coordination des Européens avec les États-Uniens laisse, à désirer, le manque de collaboration entre Européens est tout aussi évident. Une focalisation prioritaire sur le développement commercial et, éventuellement, un manque de moyens peuvent en être la cause (suite à un coût d'achat des fréquences 5G trop élevé, par exemple). Le silence des grands opérateurs occidentaux et l'absence des groupes de travail de Deutsche Telekom, Telefónica, Orange, mais aussi des fabricants de terminaux tels que Siemens ou des fournisseurs de service dans le Cloud tels qu'Atos, Dassault et Thalès, pour ne citer que les Français, dénote un manque d'adhésion à la stratégie européenne. Cependant, pour exploiter pleinement le vaste potentiel de rupture qu'offre la 5G, ces entreprises devraient bénéficier de l'appui de l'Europe pour leur participation au 3GPP, comme le font d'ailleurs les États-Uniens et les Chinois. Ces acteurs privés devraient plutôt collaborer plus étroitement entre eux, définir les domaines dans lesquels la 5G peut apporter une valeur ajoutée et concevoir la bonne feuille de route pour la mise en œuvre. En théorie, le leadership européen existe dans le secteur de la 5G ; c'est peut-être la seule technologie où celui-ci serait encore possible (nombre d'équipementiers, d'opérateurs et de brevets). Au titre de l'autonomie technologique, du leadership[80] et de la sécurité de l'espace cyber, l'UE se doit d'intervenir. Tout d'abord, en tant que membre de l'ITU. Et ensuite en tant que mécène de ses propres champions, en

subventionnant certaines dépenses et en facilitant la convergence des acteurs européens. Car, comme le dit le PDG d'Ericsson, cette norme est cruciale[81] :

> *One of the big things, with mobile technology-, well, it's the fastest-scaling technology the world has ever seen, we have more than 8 billion subscriptions globally today. That's been accommodated because we have a global standard. So, for us to protect that model of a global standard is really important, that's what gives us the connectivity we have today.*

À un autre niveau de normalisation, états-unien cette fois-ci, la recherche européenne a su faire la différence par une coopération réussie. Il s'agit de la normalisation des algorithmes post-quantiques (PQ). En 2016[82], le National Institute of Standards and Technology américain (NIST) lançait une compétition visant à certifier à l'horizon 2024 des algorithmes PQ différents[83]. Ces algorithmes seraient intégrés par la suite dans les futures clés digitales et autres solutions de chiffrement à clé publique (voir Annexe VII). Le but est de les rendre résistantes aux futurs ordinateurs quantiques. Les algorithmes PQ gouverneront l'Internet mondial dans une trentaine d'années[84] (au moins jusqu'au développement de l'informatique quantique à grande échelle), à moins qu'ils ne soient pas compromis avant. Aujourd'hui, 75% des certificats SSL utilisés actuellement sur le web sont pourvus par 8 autorités de certification, majoritairement américaines, dont le NIST. Pour un tel enjeu de sécurité mondiale, des chercheurs du monde entier se sont mobilisés. 69 candidatures seront jugées complètes, conformes et donc acceptées dans la compétition. La participation européenne est conséquente : 11 contributions contre 14 pour les États-Unis et 2 pour la Chine pour la première étape. En juillet 2022, après quelques éliminations et abandons, le NIST a retenu 4 algorithmes : un pour le chiffrement de la clé publique et 3 pour la signature digitale. Bien que les équipes soient internationales, elles sont majoritairement européennes. Le français Thalès est le porte-étendard de la solution Falcon (signature digitale). Cloudflare au Pays-Bas, se montre très présent dans la solution SPHINCS+ (signature digitale) aux côtés de l'allemand Genua GmbH.

Ces résultats montrent bien une coopération, certes, scientifique, mais redoutablement efficace tant entre chercheurs qu'entre chercheurs et entreprises privées. Toutefois, l'absence de processus similaire de la part de l'Europe surprend, d'autant plus que les États-Unis n'ont pas toujours été irréprochables vis-à-vis du chiffrement. Déjà en 2006 la NSA travaillait sous couvert pour faire approuver sa propre version d'un projet de norme de sécurité publié par the National Institut of Standards (NIST), selon les révélations de Snowden[85]. En avril 2014[86] le *National Institute of Standards and Technology* (NIST) des États-Unis a été contraint de retirer un algorithme cryptographique de sa liste de générateurs de nombres aléatoires après que la NSA l'eut délibérément affaibli pour le rendre plus facile à compromettre. Le chiffrement revêt donc une importance stratégique non seulement au niveau de la défense mais également de la sécurité des états. Peut-on conclure que, par absence d'une telle compétition au sein de l'UE, les mathématiciens européens n'ont eu d'autres moyens d'apporter le savoir qu'en participant et en soumettant leurs solutions au Gouvernement américain, avec tous les éventuels risques que cela pourrait impliquer à l'avenir ?

Le chiffrement post-quantique est un nouvel exemple où une technologie émergente crée des opportunités de leadership mondial. Moins encore que pour la 5G, les pays européens, à travers l'UE, semblent ne pas avoir saisi les impacts géopolitiques de ces technologies et devront, probablement, utiliser des solutions non européennes, comme c'est si souvent le cas aujourd'hui. Et l'épineuse question de la confiance dans le pays d'origine de la solution reste irrésolue. La question d'une obligation progressive[87] d'utilisation des certificats issus d'autorités européennes pour les sites web et incluant des algorithmes de sécurité post-quantiques non certifiés par le NIST pourrait être une solution. Cela serait possible à deux conditions : d'une part, que les EM acceptent la priorité d'œuvrer en faveur d'un internet de confiance, démocratique et transparent, à l'abri des regards et des oreilles autrui. D'autre part, il faudrait qu'ils s'accordent ensemble sur les solutions les plus fiables. En conclusion de ce chapitre, la vision européenne de la cybersécurité semble aujourd'hui définie, certainement améliorable. Elle est le résultat d'une coordination accrue à travers les institutions européennes et avec certains EM. En revanche, les exemples cités laissent penser à une diffusion peu homogène de cette vision à travers les EM et les acteurs privés. L'adoption semble peu appréciée et l'européanisation de la cybersécurité reste encore aujourd'hui problématique. Comment convaincre les réticents ? Sans doute par une communica-

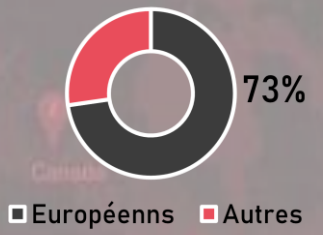
Nombre de soumissions NIST PQS

Europe 11 • États -Unis 15 • Chine 2

4 Finalistes

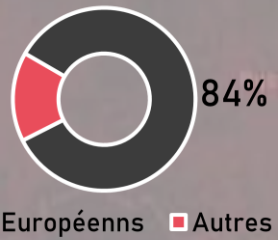
KRYSTAL- KYBER

% participation
(algorithme de chiffrement à clé publique)



SPHINCS+

% participation
(algorithme pour signature digitale)



FALCON

% participation
(algorithme pour signature digitale)

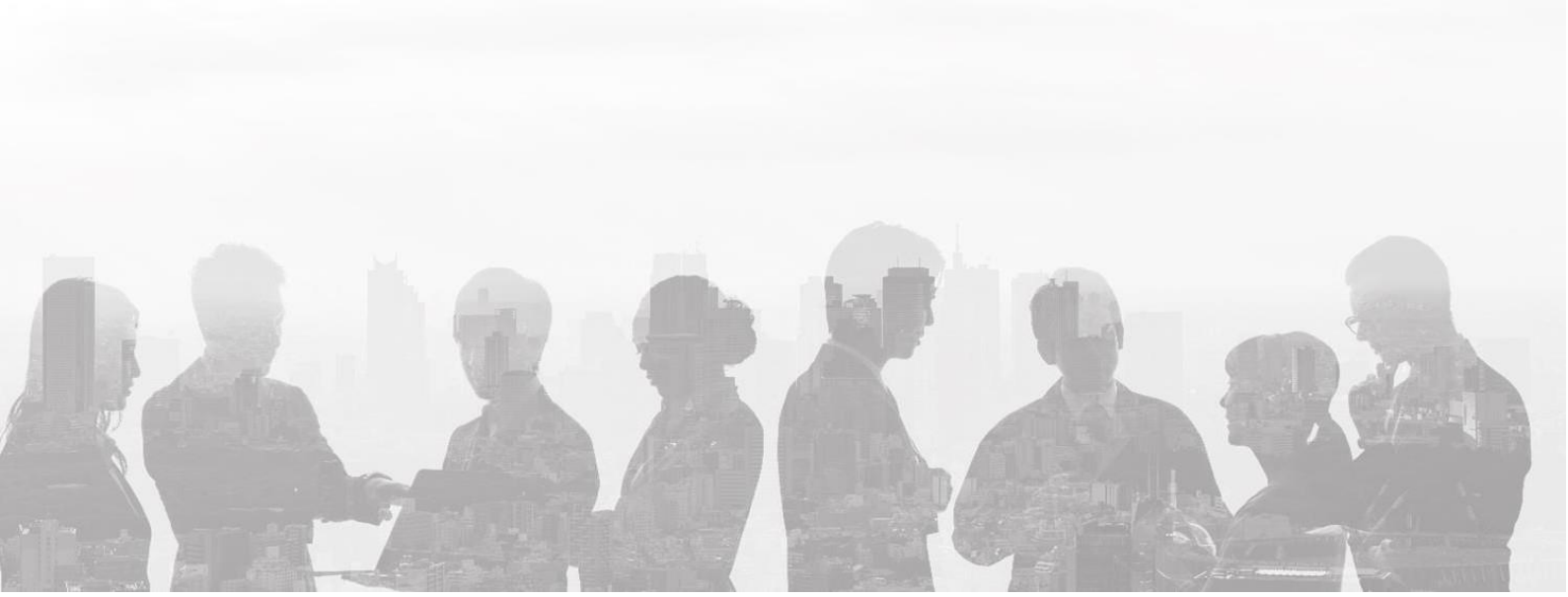
KRYSTAL- DILITHIUM

% partin
(algorithme pour signature digitale)

Données NIST 2022

NIST

tion centrée sur la diversité et l'inclusion. Trop souvent encore l'écart entre le niveau présent de maturité de certains acteurs et celui souhaité est trop important (dans un sens comme dans l'autre) et les recommandations d'ENISA peuvent ne pas suffire. Définir des objectifs chiffrés à atteindre devrait rendre la vision européenne plus concrète et plus facilement mesurable. Si l'Europe n'y est pas encore, cela ne veut pas dire que rien n'a été fait. Il faudra se donner les moyens de ses ambitions. Prioriser les financements et les centraliser facilitera la convergence vers les objectifs de la stratégie. L'adhésion des acteurs est en revanche la clé de voûte de la stratégie de cybersécurité de l'Europe puisque de cette adoption dépendra l'action commune, ou pas, et son alignement avec la vision définie par les institutions européennes. Le chapitre suivant va donc analyser de quelle façon la vision partagée devient une action commune, mitige les insuffisances et met au profit les atouts identifiés dans ce chapitre.



CHAPITRE TROIS

UNE COMPRÉHENSION COMMUNE DE LA CYBERSÉCURITÉ

3.1. Les limites de la coordination verticale

> *Les peuples d'Europe ont besoin d'une unité d'objectifs entre nos États membres et d'une unité d'action dans toutes nos politiques.*[1]

Pour faire face aux menaces, une approche partagée est indispensable, certes, mais insuffisante. Penser une solution communément ne suffira pas à atteindre les objectifs communs. Il faut agir ensemble. Cela nécessite des efforts holistiques de la part de toutes les parties prenantes, y compris des partenaires étrangers, de la société civile et du secteur privé.

Aujourd'hui, une certaine idée commence à faire son chemin en Europe : la conviction que la cybersécurité ne peut pas être assurée uniquement par les États mais qu'elle nécessite l'engagement de tous les acteurs. La compréhension commune des menaces cyber, ainsi qu'une unité commune d'action impliquent de redéfinir le concept de cybersécurité, afin que sa définition ne soit plus variable en fonction des différents acteurs. Dans la même mesure, il faut redéfinir les menaces et la réponse idéale à mettre en œuvre. Cela se reflète dans des stratégies et des opérations mises en place par les acteurs privés et publics qui gèrent quotidiennement la sécurité des systèmes et de l'information. Les efforts de l'Union Européenne dans ce domaine sont nombreux et visibles, comme nous l'avons vu dans le chapitre précédent. Cependant, leur efficacité semblerait variable car ces efforts, majoritairement réglementaires et financiers, se révèlent trop souvent insuffisants face à des États au monopole technologique qui jouent selon leurs propres règles et ne respectent que très peu les valeurs européennes d'un Internet libre au service de la démocratie et des droits fondamentaux. *La directive NIS*, la perception d'une augmentation de la cybercriminalité, la numérisation progressive des services et les attaques cyber subies par les États (Estonie, Pays-Bas [2]) ont accéléré ce qu'on pourrait appeler l'européanisation des approches nationales de cybersécurité. Néanmoins, la cybersécurité reste une prérogative presque exclusivement nationale. Cela s'oppose cependant aux mesures adoptées par les institutions européennes qui mettent en avant la nature trop complexe et transnationale de la menace cyber pour qu'elle soit laissée à la responsabilité seule des États Membres (EM). C'était d'ailleurs l'idée développée dans le premier chapitre. Cette dichotomie se reflète dans la façon dont les EM transposent, adoptent et suivent les lignes directrices formulées par la Commission Européenne (CE) et votées par chaque EM.

Adoption inégale des outils de coopération

Des dispositifs européens sont mis à la disposition des EM afin d'améliorer leur sécurité et de gagner en compétences. Depuis sa création en 2017, sous l'impulsion de la directive NIS, le réseau européen *CSIRTs European Network*, réunissant le CERT-EU et les CERT de chaque EM, a démontré sa capacité à fédérer les EM en amont puis en réaction à la menace cyber. Cela a été possible grâce à la solide confiance forgée entre les équipes de réponse aux incidents. De plus, ce réseau encourage les échanges techniques sur la menace et les incidents répertoriés. C'est une coopération réussie qui améliore le niveau de sécurité à travers l'UE. D'ailleurs, au-delà des EM, les institutions européennes ont aussi leur propre CERT, le CERT-EU. Le CSIRTs Network regroupe donc toutes ces cellules de réponse aux incidents, à la fois nationales et régionales. Il s'agit de l'un des objectifs majeurs du réseau qui reflète entièrement l'objectif d'harmonisation des compétences et de collaboration dans la cyberdéfense de la *Stratégie EU-CSS*. Ainsi, pendant l'attaque Wannacry[3] de 2017, ces mécanismes d'échanges multilatéraux ont permis de limiter les dégâts dans plusieurs pays, notamment en France.

Créé en 2020, le réseau *Crisis Liaison Organisation Network* (CyCLONe) rassemble l'ENISA, la Commission européenne et les responsables des autorités nationales compétentes en cas d'incident cyber. Ce réseau complète les structures de coopération de cybersécurité (CSIRTs European Network) en unissant les forces politiques et techniques pour répondre à la menace cyber. Il a aussi pour vocation de renforcer l'interaction et la confiance entre les responsables des autorités nationales compétentes en cas d'incident. Et enfin, il permet de faciliter d'éventuelles consultations sur les stratégies nationales de réponse aux incidents et l'établissement d'analyses conjointes sur les impacts anticipés ou constatés d'une crise cyber, au bénéfice des décideurs politiques nationaux ou européens.

Une fois le cadre européen de certification validé par la directive *Cybersecurity Act* en 2019, le temps de son déploiement est venu. Pour cela a été conçu *The National Cybersecurity Certification Authority* (NCCA), une certification européenne, avec l'appui de l'ENISA qui coordonne cette démarche. Au sein de chaque EM, des autorités nationales de certification sont donc désignées et mises en réseau au niveau européen.

La coopération, en cas d'attaque, semble donc bien structurée mais elle ne s'arrête pas là. Lors de la traduction en justice des coupables, une coopération transfrontalière s'impose aussi. Cela est parfois indispensable, car le problème d'attribution des responsabilités en cas d'attaque majeure dans un contexte de forte anonymisation et de chiffrement des attaques ne se pose pas uniquement sur le plan technique mais également sur le plan pénal. Les différences juridiques et procédurales entre les États peuvent faire obstacle aux enquêtes pénales et aux poursuites des coupables. À partir de 2001, *Budapest Convention on Cybercrime* est un instrument international qui fournit des lignes directrices contraignantes pour tout pays élaborant une législation en matière de lutte contre la cybercriminalité. Elle établit un cadre pour la coopération internationale contre la cybercriminalité entre les États parties. Actuellement, l'UE y est représentée par la Commission, le Conseil de l'Union européenne, Europol, l'ENISA et Eurojust.

Afin de trouver une solution au problème d'attribution des responsabilités, il sera nécessaire de formaliser davantage l'échange opérationnel d'informations, en mettant par exemple en place des procédures plus claires faisant intervenir Europol ou Eurojust, le réseau judiciaire européen en matière de cybercriminalité. D'ailleurs, Eurojust (*European Union Agency for Criminal Justice Cooperation)* est l'agence européenne chargée de renforcer la coopération judiciaire entre les EM par l'adoption, au niveau européen, de mesures structurelles destinées à promouvoir une coordination optimale des actions d'enquête et de poursuites qui ne concernent pas le cadre d'un seul territoire national, et ce dans le plein respect des libertés souveraines et des droits fondamentaux.

Sur le terrain, les recherches et stratégies opérationnelles sont définies par *The European Cybercrime Center* (EC3), en tant que branche d'Europol, qui opère notamment via le *Joint Cybercrime Action Taskforce* (J-CAT) d'Europol. Plusieurs opérations ont été élaborées et concrétisées à travers une coopération internationale avec des instances européennes et extra-européennes :

- Opération TALPA, Ukraine, octobre 2021[4]
- Opération FIFTH ELEMENT, Ukraine, octobre 2021[5]
- Opération GOLD DUST, Roumanie, novembre 2021[6]

L'EC3 remplit sa mission à travers plus de cent partenariats privés dans le domaine de la sécurité, de la communication, et dans le domaine financier. L'efficacité de l'EC3 émane des échanges des experts variés ainsi que d'une coopération opérationnelle. L'objectif commun de ces acteurs est bien de lutter contre la cybercriminalité.

Malgré les efforts déployés pour renforcer la cohérence entre les mesures, le cadre législatif de la cybersécurité reste incomplet selon la Cour des Comptes européenne, qui met en avant une fragmentation et des lacunes qui « *empêchent la réalisation des grands objectifs stratégiques et se traduisent par un manque d'efficience* »[7].

L'une de ces lacunes est l'absence d'une politique concernant *The Commun Vulnerabilities Disclosure* (CVD). Cela surprend d'autant plus que, dans un contexte post Wannacry et Petya[8], le Centre for European Policy Studies Task Force (CEPS) détaillait son urgente nécessité. Dans ce contexte, une politique nationale de CVD devrait permettre l'identification de vulnérabilités dans les produits (*zero day vulnerability*) de façon proactive. Une telle politique définit le cadre dans lequel les chercheurs en sécurité sont autorisés et encouragés à effectuer des recherches sur les produits et services numériques, en suivant un ensemble de règles. Ils sont ensuite encouragés à signaler aux autorités nationales ou au vendeur du produit toute vulnérabilité qu'ils découvrent. En outre, elle permet de gagner un temps précieux et d'instaurer une coopération entre les parties prenantes lors du développement de patchs, par exemple, et de repousser ainsi l'exploitation de ces failles.

L'attention des EM à ce sujet est encore très variable, allant de politiques déjà en place au 3ème trimestre 2021 (Pays-Bas, France, Lettonie, Belgique) à une absence totale d'intérêt pour neuf des EM (cf. carte ci-

contre). Bien que centrée sur une forte dominante procédurière, la politique CVD nécessite la définition de garde-fous législatifs qui protègent les chercheurs, ainsi que la mise en place de récompenses économiques pour soutenir ces recherches. En France c'est la *Loi pour une République numérique* de 2016 qui encadre et protège ces activités. En dépit des recommandations de la Commission, l'intérêt des EM envers les politiques CVD ne s'est que très peu intensifié entre 2017 et 2021 (cf. cartes ci-contre), alors que la découverte de vulnérabilités a augmenté de manière exponentielle. Cette découverte est d'ailleurs d'origine majoritairement états-unienne, britannique ou néerlandaise.

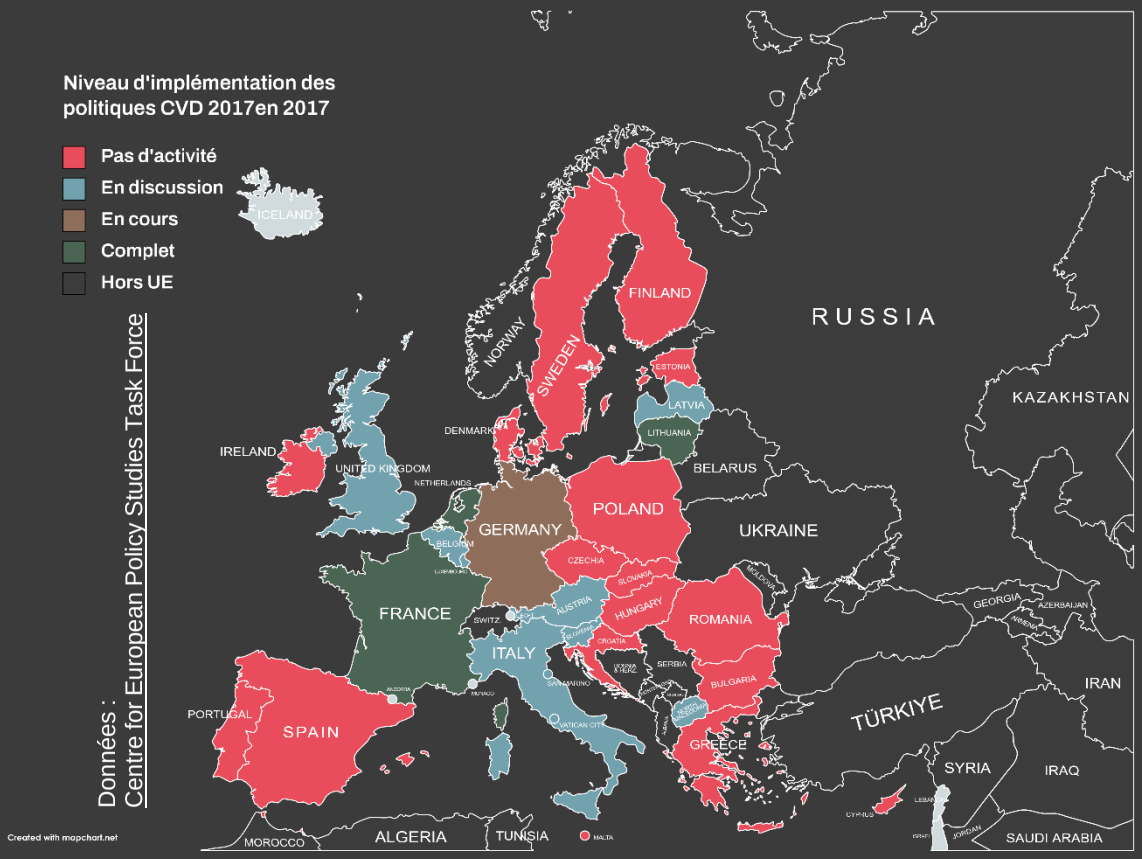
Pourtant, un déploiement généralisé des politiques CVD nationales est attendu avant que l'UE ne commence à travailler sur une homogénéisation de ces politiques ; le risque est que les EM adoptent des cadres de référence différents, ce qui rendra la tache de l'ENISA très difficile. Mais pour le moment l'implémentation de telles politiques relève du bon vouloir des EM.

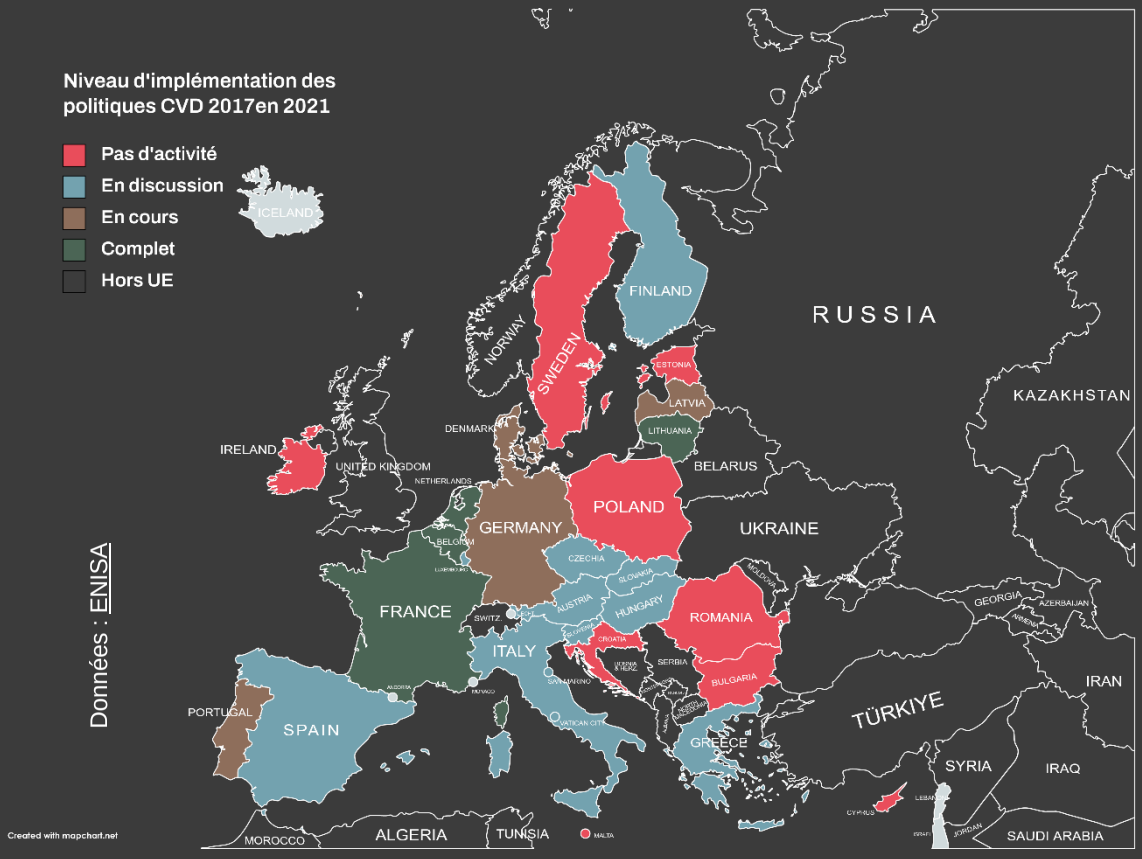
Des insuffisances législatives ont été également identifiées dans la *Directive NIS*. Les secteurs identifiés comme critiques par les deux versions de la directive sont les secteurs prioritaires de point de vue de la sécurité nationale mais pas du tout du point de vue de la criminalité. Les directives prévoient que les EM puissent aussi implémenter des mesures sur les secteurs non couverts, bien que cela soit discutable en termes d'entrave à la concurrence. Ainsi, le secteur de l'hébergement touristique, qui n'est pas couvert par ces deux directives, peut ouvrir la porte à d'autres crimes ou délits, comme la traite d'êtres humains, le trafic de drogue ou l'immigration clandestine. Trop souvent, les transpositions inégales des directives, pas seulement de sécurité, détériorent l'efficacité des mesures. C'est d'ailleurs ce que pointe Rayna Stamboliyska, experte en cyber et en affaires européennes[9] :

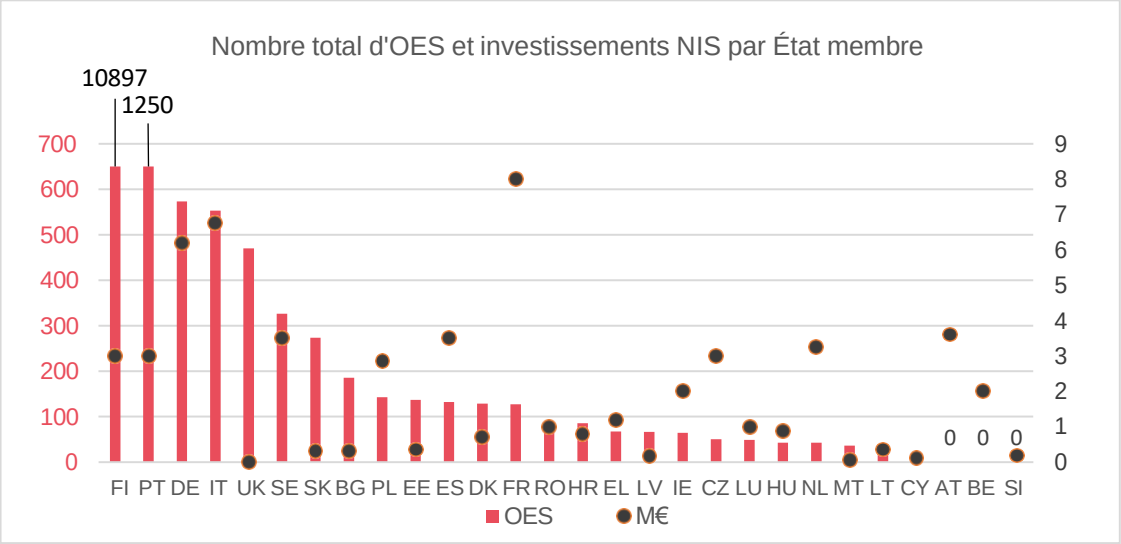
> *« La directive, comme toute directive européenne, indique des objectifs communs de cybersécurité à atteindre, mais laisse à chaque État le soin de la transposer en définissant sa propre stratégie et ses propres moyens. »*

Toujours sur le plan de la lutte contre la criminalité numérique, la *Directive NIS* ne traite pas directement de l'acquisition illicite de données par intrusion (par exemple le cyber espionnage). Il est donc difficile de l'invoquer pour entamer des poursuites judiciaires[10]. À cause de ressources insuffisantes, la *Directive NIS* a connu une transposition par les EM assez chaotique. Dans plusieurs d'entre eux, une agence centrale dispose d'un budget et d'effectifs importants (cf. carte ci-dessous), et d'une expertise qui a fait ses preuves en raison de nombreuses années de pratique de la cybersécurité : qu'il s'agisse de l'ANSSI en France, du *National Cyber Security Center* au Royaume-Uni, du *National Cyber Security Center* (NCSC) irlandais ou de la BSI allemande. D'autres EM présentent en revanche un profil beaucoup plus éclaté : l'Italie a ainsi fait le choix d'une structure polycentrique, avec plusieurs ministères désignés comme autorités nationales au sens de la directive, et un système de coordination de l'action de ces ministères par un comité technique de liaison : mais aucune agence nationale unique n'est chargée du champ de la cybersécurité.

Le bilan de l'identification des OES par les EM, pilier de la *Directive NIS*, est mitigé : *six* États ont été notifiés d'une mise en demeure pour leur retard et cinq EM n'ont envoyé que des données partielles sur l'identification des OES[11]. De plus, ce qui pourrait affaiblir la future coopération est la confrontation des données rendue complexe par des interprétations nationales des méthodes et des seuils retenus pour la qualification des OES. Les écarts en nombre d'OES identifiés sont très conséquents[12] : 0 en Slovénie, Autriche et Belgique, 10897 en Finlande, 127 en France, 573 en Allemagne.


Niveau d'implémentation des politiques CVD 2017en 2017
Pas d'activité
En discussion
En cours
Complet
Hors UE
Données : Centre for European Policy Studies Task Force
Created with mapchart.net
ICELAND
IRELAND
UNITED KINGDOM
NETHERLANDS
DENMARK
NORWAY
SWEDEN
FINLAND
RUSSIA
ESTONIA
LATVIA
LITHUANIA
BELARUS
KAZAKHSTAN
POLAND
GERMANY
BELGIUM
CZECHIA
SLOVAKIA
UKRAINE
FRANCE
SWITZ.
AUSTRIA
HUNGARY
ROMANIA
MOLDOVA
GEORGIA
AZERBAIJAN
ARMENIA
ITALY
SLOVENIA
CROATIA
SERBIA
BULGARIA
IRAN
PORTUGAL
SPAIN
GREECE
TÜRKIYE
SYRIA
IRAQ
MOROCCO
ALGERIA
TUNISIA
MALTA
SAUDI ARABIA


Niveau d'implémentation des politiques CVD 2017en 2021
Pas d'activité
En discussion
En cours
Complet
Hors UE
Données : ENISA
Created with mapchart.net
ICELAND
IRELAND
UNITED KINGDOM
NETHERLANDS
DENMARK
NORWAY
SWEDEN
FINLAND
RUSSIA
ESTONIA
LATVIA
LITHUANIA
BELARUS
KAZAKHSTAN
POLAND
GERMANY
BELGIUM
CZECHIA
SLOVAKIA
UKRAINE
FRANCE
SWITZ.
AUSTRIA
HUNGARY
ROMANIA
MOLDOVA
GEORGIA
AZERBAIJAN
ARMENIA
ITALY
SLOVENIA
CROATIA
SERBIA
BULGARIA
IRAN
PORTUGAL
SPAIN
GREECE
TÜRKIYE
SYRIA
IRAQ
MOROCCO
ALGERIA
TUNISIA
MALTA
SAUDI ARABIA



NIS

Implémentation et investissements hétérogènes

Données CE 2019 et ENISA 2021

Il est donc urgent de remédier aux lacunes du droit européen et à sa transposition nationale inégale, puisque de ces failles naissent des espaces hors-loi qui sont presque immédiatement investis par les criminels. La résilience de tout le système est en jeu et dépend de la résilience de l'acteur le plus faible.

Conséquences des contraintes législatives

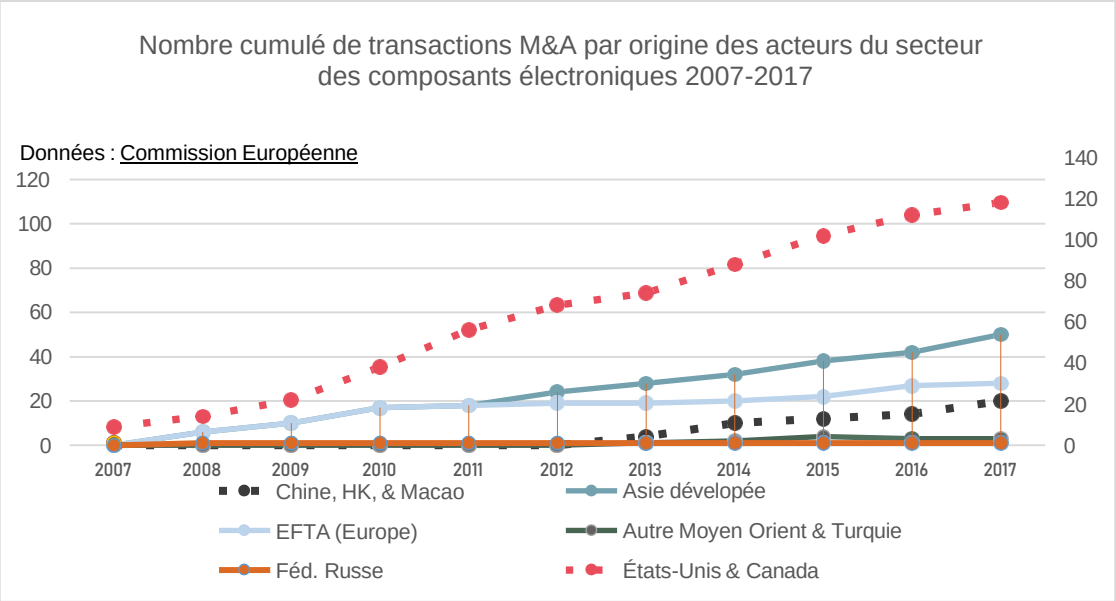
Il arrive parfois que la cohérence ne soit plus une priorité lors de la transposition des exigences formulées par Bruxelles lors des opérations des EM sur le terrain. Les Investissements Directs Étrangers (IDE) en sont un exemple.

Grâce à un marché facile d'accès, l'UE reste un importateur net de produits et services non seulement liés à Internet ou au digital, mais aussi à la cybersécurité, ce qui augmente le risque de dépendance technologique et de vulnérabilité aux équipementiers ou prestataires étrangers. Cette situation fragilise en particulier la sécurité des infrastructures critiques de l'UE, qui s'appuie sur des chaînes d'approvisionnement mondiales complexes. Lorsqu'il ne s'agit pas d'importation, la présence d'intérêts étrangers perdure à travers l'acquisition de parts de marché d'entreprises stratégiques. La part des actifs étrangers dans l'économie européenne a été évaluée à 35%[13] par *The First Annual Report on the screening of foreign direct investments into the Union* de la Commission Européenne et concerne des secteurs économiques européens clé tels que les équipements électroniques, l'IA et le conseil IT. En 2016, la CE évalue la part des actifs et des entreprises non-européennes à plus de 50% dans le secteur des industries de l'informatique et de l'électronique, en deuxième position après les minerais métalliques[14]. Les Etats-Unis et le Canada en fournissent la plus grande partie. Par exemple ; la part de ces pays dans la fabrication d'ordinateurs et de composants électroniques dépasse 50%[15].

Sur la période 2014-2017, les fusions et acquisitions (M&A) sont en nette augmentation non seulement aux Etats-Unis (un peu moins de 120 M&A en 2017), mais aussi en Chine (20 M&A en 2017)[16]. Le rapport confirme, entre autres, une nette augmentation des investissements non seulement états-uniens mais aussi chinois

Le filtrage des investissements directs étrangers (IDE) relève de la responsabilité des États membres bien que, depuis 2020, soit entré en vigueur un cadre européen pour les mécanismes de filtrage des IDE entériné par le *Règlement (UE) 2019/452* du Parlement européen et du Conseil. Le règlement vise une homogénéisation des législations nationales, ainsi que davantage de coopération et de transparence selon la déclaration de la Commission Européenne[17] :

> *Le règlement de l'UE sur les IDE encourage la coopération, le partage d'informations et un niveau minimum de transparence concernant le contrôle des IDE entre la Commission européenne et les États membres.*



Ce cadre, adopté par la majorité des pays européens, n'impose pas d'obligation de filtrage ni de conditions précises ou de déclaration des filtrages effectués. Cependant il met en place des mécanismes de coopération interétatiques, tels que le partage d'informations et des préoccupations lorsque les EM perçoivent un risque pour la sécurité ou l'ordre public d'un autre EM ou en rapport avec un projet de l'Union (Horizon). C'est un exemple concret de collaboration qui, pour aboutir, nécessite la participation et le consensus de minimum deux EM. Ce règlement visant les IDE peut paraître quelques peu dépourvu d'ambition face au redoutable interventionnisme de la Commission et sa politique anti-trust ; on le considère redoutable car on lui reproche notamment d'empêcher la création de champions européens capables de s'opposer à des géants états-uniens ou chinois. Ce fut par exemple le cas lors de la fusion Siemens-Alstom qui aurait pu faire barrage au chinois CRRC. Face à ce choix, le caractère volontaire du cadre des IDE, adopté également au niveau national par certains pays tels que l'Allemagne et la Finlande, est signe d'une contradiction : on régule davantage les entreprises européennes que les investisseurs étrangers.

L'inaction des autorités auprès du secteur privé

En France et dans d'autres états, le secteur privé et les institutions nationales se placent sur une relation hiérarchique très verticale. L'ANSSI, par exemple, a comme priorité la sécurité des infrastructures critiques, alors que la gouvernance du développement industriel de la cybersécurité relève de la Direction Générale des Entreprises. L'absence par le passé du Président français et du Premier ministre au FIC témoigne de cet éclatement de l'approche de la cybersécurité alors que la coopération de tous les acteurs est essentielle. Le secteur privé est en premier ligne pour gérer au quotidien la sécurité des systèmes de l'information. Ces conseils sont d'autant plus pertinents qu'ils sont les fruits d'expériences passées. C'est d'ailleurs ce qui légitime les fortes ambitions pour la 5G formulées par Neelie Kroes, l'ex-vice-présidente de la Commission Européenne en charge de la société numérique, dès 2013[18] :

> *OK, nous avons raté la 4G alors que nous étions le leader de la 3G, maintenant prenons le contrôle de la 5G.*

Cela paraissait réalisable grâce à l'acquisition d'Alcatel-Lucent par Nokia en 2015. L'entité combinée, appelée Nokia Corporation, aurait dû devenir le deuxième plus grand fabricant d'équipements mobiles au monde, avec une part de marché estimée à 35%, juste derrière le suédois Ericsson, dont la part était estimée à 40%[19]. Bien que loin de sa position de leader mondial des années 2000, Nokia acquérait des avantages géographiques stratégiques et technologiques (*small cells*, *Voice-over LTE*) qui le positionnaient comme un acteur fort dans le domaine des équipements de télécommunications en Europe, en Chine, ainsi que sur le marché très rentable des États-Unis[20].

L'Europe et la France approuvent donc la naissance d'un potentiel fleuron européen des télécommunications. Et pourtant, en 2019, Nokia passe de 20% parts de marché à peine 15%, derrière Huawei et Ericsson [21]. La gestion difficile de l'acquisition d'Alcatel[22] a entraîné des mauvais choix stratégiques[23] qui ont fait piétiner Nokia au départ de la course à la 5G. Finalement, la fusion-acquisition a entraîné la construction d'une gigantesque structure de 98 000 employés, découpée en une multitude d'unités peu performantes. Et pourtant, certains risques avaient été pris en compte, dont la difficulté d'intégrer de telles entreprises à forte intensité de R&D, comme cela s'était vu dans le passé, avec Nokia-Siemens ou Alcatel-Lucent ; nous y reviendrons dans le Chapitre 4.

Comme pour la 4G, la coopération et la coordination sont la clé d'une mise en œuvre réussie de la 5G. Au moment de l'"invasion" de Huawei, Nokia accuse des années de retard. Lorsqu'il a fallu fédérer des intérêts nationaux afin d'obtenir des financements de la part de l'Europe, Nokia n'a pas convaincu, et l'Europe n'a pas saisi l'importance stratégique d'un tel soutien, comme le remarquait Alain Juillet, haut fonctionnaire français[24] :

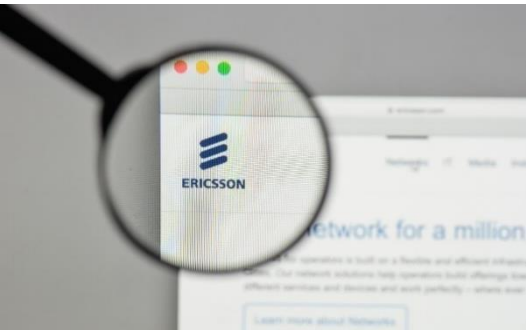
> *Le problème c'est que, pour que [Nokia] puisse gagner du temps par rapport au Chinois, il faut qu'elle investisse beaucoup. Or elle n'a pas les moyens pour investir. Donc il faudrait que ce soit l'Europe qui investisse, qu'elle l'aide. L'Europe ne le fera pas, parce que l'Europe est tiraillée entre toutes les tendances. Résultat : l'Europe ne bougera pas.*

Mais alors que l'Europe, avec Nokia, n'avait jamais été aussi proche du leadership technologique mondial… elle a tout de même refusé d'apporter son soutien à Nokia. Cela confirme les propos d'Alain Juillet.

Les causes du retard de Nokia sont en partie des failles dans la coordination et la coopération européenne, ainsi qu'entre les EM : manque de cohérence entre les propos et les actions de l'Europe, signe d'une faible compréhension commune des priorités technologiques et de sécurité européenne ; manque d'implication et de conformité de la France dans la *Stratégie EU-CSS*… Ni Europe ni EM ne se sont engagés aux côtés de Nokia, alors qu'aux Etats-Unis et en Chine les gouvernements ont accompagné de très près la naissance de leurs champions mondiaux respectifs.

Afin de devenir plus compétitive et rattraper son retard, Nokia change de PDG en août 2020 (le deuxième en 5 ans), se sépare de presque 10% de sa masse salariale (10 000 employés dont plus de 1200 français) et avec ces économies booste sa R&D[25] et ses ventes de 5% au premier trimestre 2022[26]. Pekka Lundmark, le nouveau PDG, fait en revanche ce qu'il dit : la bataille pour la 5G doit être gagnée, coûte que coûte. Il sait que la réussite de la 5G est cruciale pour l'avenir de Nokia. Il devrait également savoir que la capacité de l'Europe et des États-Unis à profiter de la prochaine vague d'innovation est également en jeu. Aujourd'hui, le déploiement de la 5G est toujours problématique, et les instances européennes de contrôle s'inquiètent d'ailleurs du retard de certains Etats dans le déploiement des solutions commerciales. Selon l'Observatoire 5G de juillet 2022, douze pays sont en retard et un seul, la Finlande, a atteint les objectifs fixés par l'EU[27]. L'Europe semble avoir oublié les priorités stratégiques qu'elle a elle-même formulées : autonomie stratégique, leadership technologique, résilience des infrastructures. Aussi, l'allocation des fréquences est une étape clé dans le déploiement de la 5G. Par le passé, l'Europe a envisagé de règlementer l'allocation mais finalement cela a été laissé à la discrétion de chaque EM.

Pourtant, dès 2019, les équipementiers européens attirent l'attention des chefs d'états et des institutions européennes sur les effets néfastes d'une éventuelle inaction vis-à-vis de ce sujet. En l'absence d'une mise à disposition coordonnée et de prix raisonnables des fréquences,



prévient Börje Ekholm, PDG d'Ericsson [28] , 2ème équipementier mondial, le déploiement de l'infrastructure numérique risque d'être parcellaire. Le PDG de Nokia, Pekka Lundmark, à son tour, réitère la critique en 2021[29] :

> *The infrastructure is absolutely necessary and very much the wireless mobile 5G infrastructure. Every single country in Europe makes their own frequency allocation decisions which makes the whole system inefficient. There was intention already a long time ago to that Europe would have a coordinated approach to 5G frequencies. Finland is the only country in Europe will implemented that decision. So, we have a lot to improve in order to compete with Asia and the United States.*

L'uniformisation des fréquences allouées auraient pu faciliter la tâche des opérateurs et fournisseurs de terminaux. Cependant, la situation de 2021 fait état d'un déploiement hétérogène de cette technologie (cf. carte ci-contre)[30]. Quant aux coûts des licences, la vision des États et des équipementiers ne converge guère. Selon Ekholm, l'attribution des licences devrait plutôt se concentrer sur le résultat qui permet de construire l'infrastructure le plus rapidement possible afin de créer le plus d'avantages[31] :

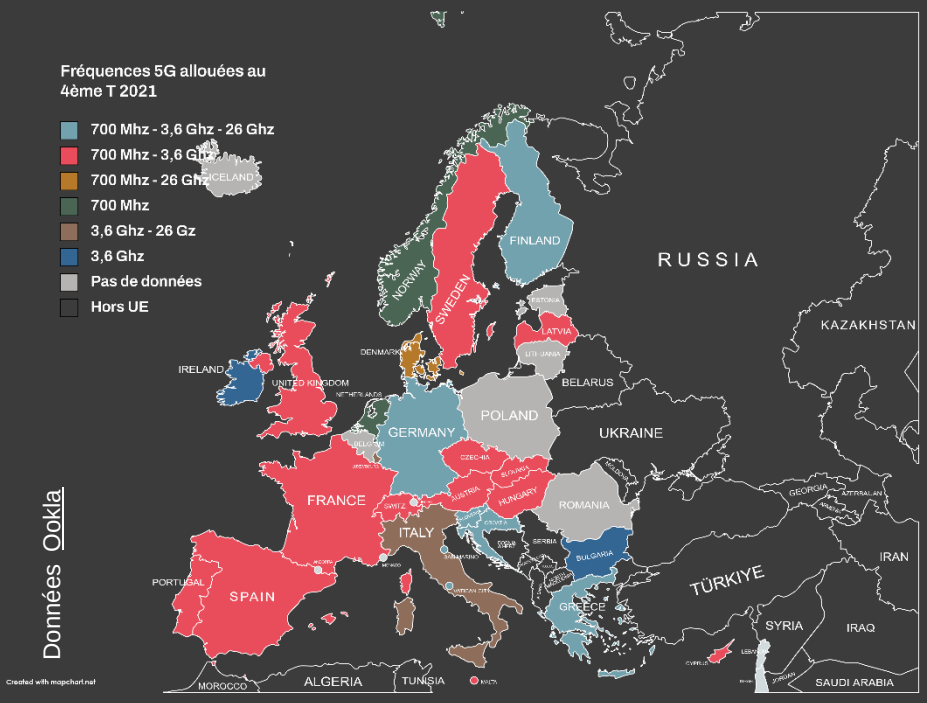
> *Today a spectrum auction is deemed a success if it raises the maximum amount of money for the tax income of the government. […] But the reality is that we need to factor in all the other benefits you would get from rapidly building out the telecom infrastructure.*

Or les enchères d'attribution des fréquences ont apporté à certains Etats Membres plus que ce qu'ils espéraient. Ce fut le cas de la France, où la vente des licences a apporté à l'État 2,17 milliards d'euros[32]. Des prix aussi élevés pourraient se révéler pénalisants pour les plus petits opérateurs, Bouygues Telecom et Free, aux capacités financières moins importantes qu'Orange ou SFR. Pour certains, ces frais sont alourdis par des coûts de remplacement du matériel chinois faisant suite à de mauvais choix stratégiques, pris en l'absence de lignes claires de l'ANSSI ou du gouvernement. Les fortes ambitions de l'Arcep, désireuse d'améliorer le rang de la France dans le classement européen des réseaux mobiles (dernière du classement en 2015), a établi l'état d'urgence auprès des équipementiers. C'est ainsi que deux d'entre eux ont choisi un équipementier chinois (SFR et Bouygues). En 2021, deux ans après la loi "anti-Huawei" du député Eric Bothorel, l'ANSSI exige le démantèlement des antennes Huawei 4G/5G des grandes villes d'ici 2028, une opération chiffrée à plus de 2 milliards d'euros[33]. Le contexte est donc tendu et peu propice à une coopération en faveur d'une mutualisation des réseaux dont Orange est majoritairement propriétaire, à un déploiement dans les temps et d'une qualité de service à la hauteur des investissements et des besoins des utilisateurs.

Des réactions négatives ont été exprimées en 2019 par certains opérateurs allemands également, se plaignant d'un système d'enchères injuste et des prix des licences qui ont fini par apporter à l'état fédéral 6,55 milliards d'euros [34] , montant similaire à celui récolté en Italie en 2018. Comme en France, les opérateurs outre Rhin s'inquiètent de leur capacité à construire les réseaux, selon les affirmations de Dirk Wössner, membre du conseil d'administration de Deutsche Telekom[35] :

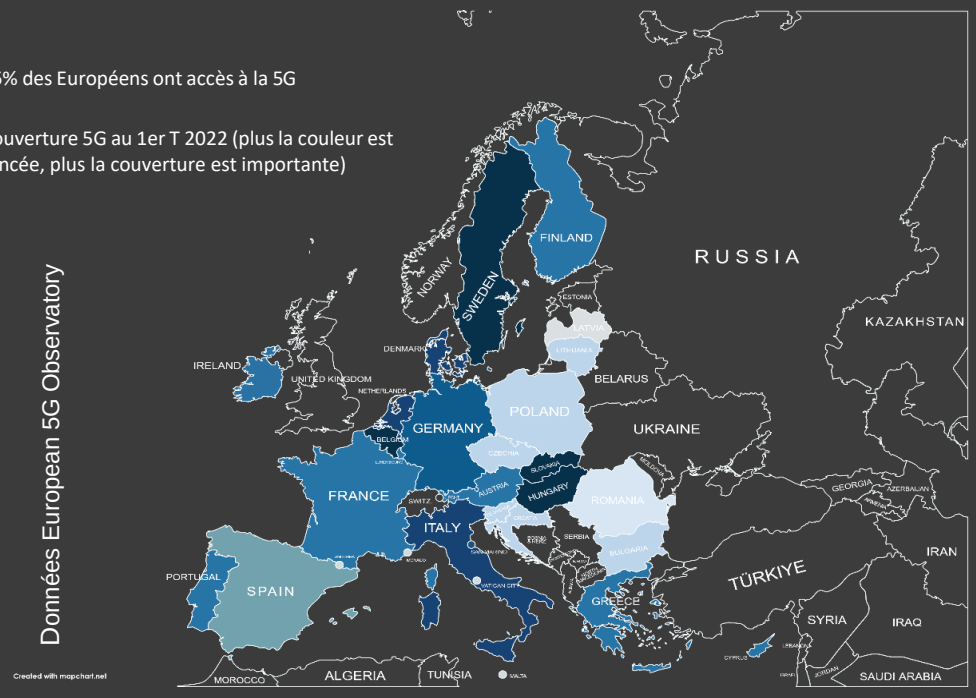
> *Le prix aurait pu être beaucoup plus bas. Encore une fois, le spectre en Allemagne est beaucoup plus cher que dans d'autres pays. Les opérateurs de réseau n'ont plus les fonds nécessaires pour développer leurs réseaux. On aurait pu construire environ 50 000 nouveaux sites mobiles et mettre fin à de nombreuses zones blanches.*

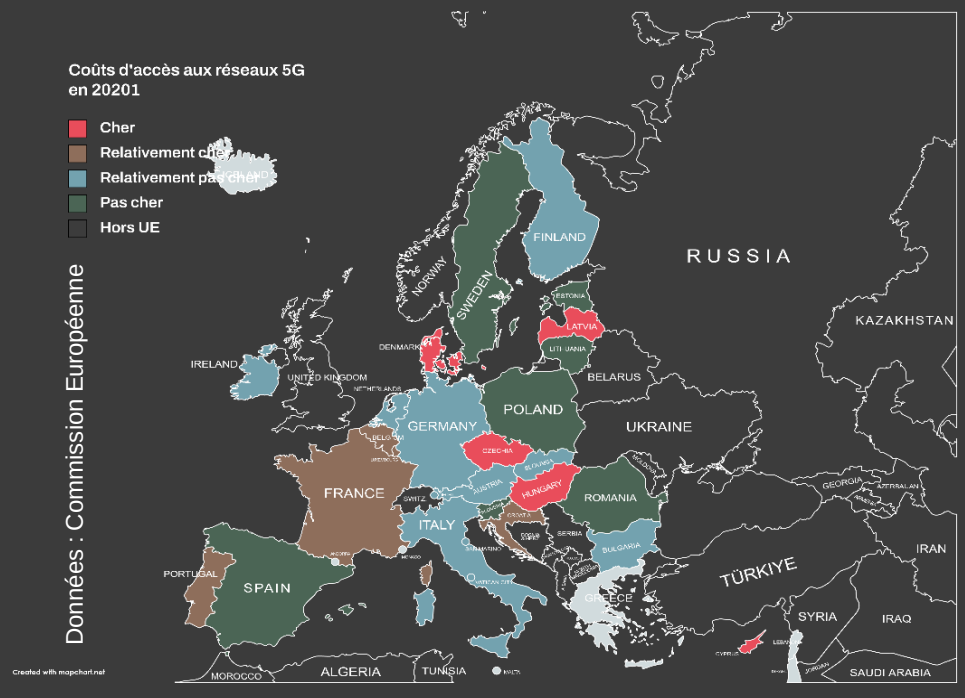
Ekholm (ci-contre) met également en garde contre une durée trop courte des licences d'utilisation des fréquences, car l'approche actuelle en Europe entraîne une incertitude en matière d'investissement pour les opérateurs dans la dernière partie de la période d'attribution des licences.



66% des Européens ont accès à la 5G

Couverture 5G au 1er T 2022 (plus la couleur est foncée, plus la couverture est importante)





Au cours des dernières années de la période de validité d'une licence, les opérateurs ne sont plus incités à investir dans l'exploitation des nouvelles technologies lorsqu'il y a une incertitude quant à l'avenir de la licence et de l'utilisation des fréquences. La réglementation et les politiques devraient renforcer les capacités des opérateurs mobiles à générer des capitaux pour investir dans de nouvelles technologies.

Or, la priorité donnée aux prix les plus bas à court terme est une réalité aujourd'hui qui n'augure pas le meilleur service, selon Ekholm[36] :

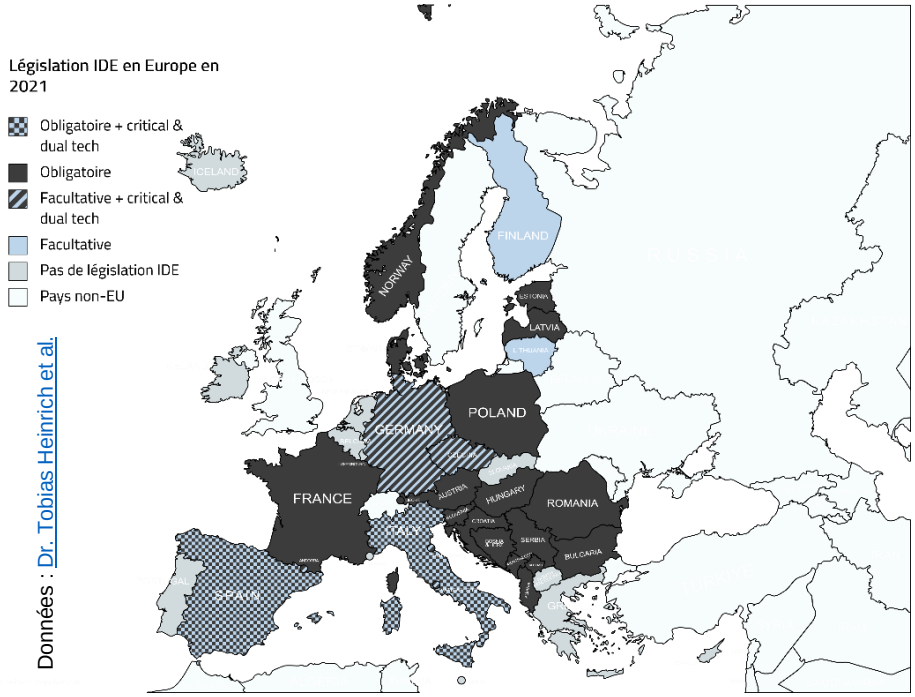
> *Many European consumers spend more in coffee shops per-week than on mobile broadband per-month. It's short-term gain, but long-term pain.*

Par leur diversité et leur grand nombre, les plus de 200 opérateurs européens [37] fragmentent considérablement le marché et freinent les investissements à long terme. Et enfin, Ekholm rappelle l'importance vitale de la sécurité. La sécurité des réseaux 5G sera complexe et dépendra de tous les acteurs des télécoms : états, équipementiers, opérateurs et utilisateurs. Finalement, le CEO d'Ericsson déplore l'adoption du même état d'esprit qui, dans un passé récent, a retardé l'Europe lors de l'arrivée de la 4G au profit d'acteurs globaux[38] :

> *The US and China see 5G as a critical national infrastructure and the backbone of digitalizing society. […] It was no coincidence that big 4G winners such as Alibaba, Netflix, and Tencent – emerged from the U.S. and China, and not Europe.*

Peu de ces conseils ont été suivis par les Etats et le déploiement de la 5G est non seulement déficitaire mais aussi peu performant. Seuls trois pays de l'UE ont des vitesses de téléchargement 5G supérieures à 300 Mbps alors que les Emirats Arabes ne sont pas loin de 600 Mbps ; la majorité des pays membres de l'UE étaient en-deçà de 200 Mbps[39]. Insuffler la dimension critique et stratégique de la 5G dans les institutions européennes et dans les décideurs de chaque EM est désormais indispensable.

Le lancement presque forcé de la 5G grand public en Europe dans un contexte de faiblesse concurrentielle du marché européen (déboires de Nokia, fragmentation du marché, absence de fleuron technologique) peut se comprendre par la crainte de priver l'économie européenne des avantages de la 5G. Aujourd'hui, avec le recul, certains pensent que c'était une erreur stratégique. La 5G en tant que réseau privé d'entreprise n'a pas attendu l'Europe pour se développer. Ce qui est moins compréhensible



en revanche est le manque d'intervention des institutions européennes et de des EM qui semblent décider seuls de leur politique industrielle.Lorsque des législations nationales sont en vigueur afin de protéger

les exportations de technologies critiques, la liste des d'activité concernées varie fortement. A part la 5G, qui figure dans la législation de 14 pays parmi les 21 qui ont une législation, les technologies critiques et les *dual-use technologies* surprennent par leur rareté, et concernent seulement 5 pays sur 21[40].

En 2021, en pleine offensive américaine contre l'équipementier Huawei, celui-ci lançait officiellement la construction de sa première usine en dehors des frontières, en France. Quelques mois plus tard, l'équipementier chinois annonçait le projet de construction d'un centre ferroviaire intelligent nourri par la 5G, en collaboration avec le britannique Vodafone et le centre de logistique hongrois East-West Intermodal. Si le projet arrive à terme, il s'agira de la plus grande plateforme ferroviaire multimodale intelligente d'Europe, ainsi que du premier port ferroviaire d'Europe à utiliser un réseau privé 5G. Le politologue hongrois Botond Feledy met en avant le contexte particulier des pays est-européen, parfois moins regardants sur l'origine des investisseurs :

> *D'une part, [Huawei] a été très chaleureusement accueilli par le gouvernement [hongrois]. D'autre part, il est clair qu'au moment de leur arrivée sur le marché hongrois, ils ont attaqué avec des prix très bas. Les Européens de l'Est sont toujours désireux d'accueillir plus facilement n'importe quel type d'investisseur, qu'il s'agisse d'une centrale nucléaire russe ou d'un centre logistique chinois, car ils manquent d'investissements et ont besoin d'investissements directs étrangers.*

Il faut reconnaître que le marché européen réunissant 500 millions de potentiels utilisateurs et quelques 23 millions d'entreprises[41] : c'est donc une grande opportunité pour Huawei, alors banni du marché états-unien. Ainsi, l'Europe représente le deuxième marché pour les fournisseurs d'Internet et services associés après l'Asie, alors que les Amériques sont en quatrième position. Les affaires doivent prospérer même si cela devait contredire la *Stratégie de cybersécurité*.

À l'interventionnisme des institutions européennes les gouvernements opposent une tendance à protéger leurs propres champions nationaux et à tenir les rivaux européens à l'écart des secteurs stratégiques. La France est un bon exemple, comme nous l'avons vu avec les mesures protectionnistes imposées à Nokia qui n'ont fait que retarder le retour des profits après l'acquisition d'Alcatel-Lucent.

Au niveau des EM, la stratégie de Bruxelles passe souvent derrière l'intérêt national, que cela concerne la politique, l'économie ou la sécurité et les exemples de la France et de la Hongrie sont concluants. Entre intérêts nationaux et nécessité d'acquérir une autonomie stratégique, le curseur varie trop souvent en défaveur de la cause européenne commune et de l'autonomie stratégique. Soumettre les fusions et acquisitions d'entreprises européennes au vote du Conseil pourrait-il déplacer le curseur dans le sens opposé ? Cela semble difficile selon Thomas Vinje, expert en fusions et acquisitions[42].

Entre 2011 et 2016, les GAFAM ont fait l'acquisition de 53 entreprises de technologies européennes[43]. Entre 2001 et 2012 la France a ainsi vendu de multiples applications de e-commerce (PriceMinister, Pixmania, iBazar) ou de réseaux sociaux (auFéminin, Meetic) a des géants technologiques tels que eBay et Rakuten. L'états-unien Nuance, développeur de l'IA derrière Siri et propriété de Microsoft depuis 2021, a aussi racheté discrètement en 2013 le français VirtuOz qui conçoit des assistants virtuels, il l'a ensuite rebaptisé Nina Web.

Une acquisition fait mémoire a été l'achat de l'estonien Skype [44] par Microsoft. Rappelons que la Commission Européenne a donné son accord en 2011 pour ce rachat à hauteur de 6,6 milliards d'euros. Skype était une fierté européenne assez unique en son genre à une époque où Siri, Alexa et autres assistants vocaux étaient au stade de projet. En 2013, Cisco accuse la Commission d'avoir donné feu vert à la création d'un monopôle de plus de 80% de parts de marché. Saisi par Cisco et l'italien Messagenet, le Tribunal de l'UE reconnaît les 80-90% parts de marché détenues par Microsoft mais ne considère pas lui conférer « *un pouvoir de marché permettant à Microsoft de nuire de façon significative à la concurrence effective sur le marché intérieur.* » [45]

C'était sans le savoir que l'acquisition ne visait pas l'exploitation de ce monopôle mais plutôt l'élimination d'un concurrent. La suite des évènements le confirmera. Depuis le rachat en 2011, laissée sans mises à jour pour combler ses vulnérabilités, la solution a été largement devancée par les groupes Meta et Alphabet.

Quel équilibre entre régulation et innovation ?

Les entreprises privées savent qu'un environnement plein d'incertitudes peut limiter la consommation, les investissements et la recherche. À regarder la multitude de textes européens en vigueur ou à venir voués à réguler le secteur de la sécurité de l'information (*RGPD, Cybersecurity Act,* les directives *NIS, Chips Act, Data Governance Act, Digital Operational Resilience Act, Cyberresilience Act, Artificial Intelligence Act, Digital Services Act, Digital Markets Act*), la question se pose quant à la conscience réelle à cet égard de la part des institutions européennes et nationales. Car ces textes ne sont pas les seuls ; s'y ajoutent d'autres obligations réglementaires telles que celles prévues dans la *Competition toolbox* (des règles sur les ententes et les abus de position dominante, le contrôle des concentrations, les aides d'État, les entreprises et les services publics) et des obligations financières (PCI DSS). L'objectif principal de ces règles est de permettre le bon fonctionnement du marché intérieur de l'UE, moteur essentiel du bien-être des citoyens, des entreprises et de la société dans son ensemble.

Toutefois, les lois et les réglementations en lien avec la compétitivité impactent fortement les économies européennes, car elles peuvent entraîner des externalités négatives inattendues pour les entreprises et les citoyens, notamment en termes de compétitivité à l'étranger, d'innovation et de coûts réglementaires. Par exemple, une approche réglementaire parallèle (qui s'étale sur plusieurs textes) peut générer en plus des obstacles à l'innovation, et une perte de confiance dans le processus réglementaire, en particulier pour les projets et les investissements à haut risque à charge du secteur privé. C'est l'exemple des textes régulant les télécommunications dans le secteur numérique, pas toujours cohérents en termes de protection des consommateurs. L'évolution rapide des technologies et du marché rendent obsolètes les règles de protection des consommateurs car le temps politique est toujours plus long que celui de la technologie. De plus, la législation européenne a généré une distinction arbitraire entre les services des opérateurs et les autres services numériques, au détriment de la protection des consommateurs, de la concurrence loyale et des outils d'application des autorités publiques. Si les opérateurs sont soumis à des obligations spécifiques et strictes lorsqu'ils fournissent leurs services aux clients finaux, en revanche, les fournisseurs de services Internet offrant des services similaires (les places de marché en ligne) ne sont pas soumis aux mêmes règles. La protection des consommateurs qui repose sur un si grand nombre de cadres différents[46] devient complexe à comprendre non seulement pour les consommateurs mais aussi pour les opérateurs.

De plus, la réglementation sectorielle a un impact sur la capacité des opérateurs de télécommunications à concurrencer les *Over-the-Top telco* (OTT), car elle entrave ou retarde l'innovation en raison de procédures de mise en conformité longues et complexes - y compris la négociation avec les régulateurs, voire leur approbation préalable. Ainsi, les opérateurs jouissent d'une moindre flexibilité pour introduire de nouveaux modèles commerciaux en raison de restrictions toujours plus nombreuses. Et cela entraîne des coûts de mise en conformité plus élevés. Tout cela a finalement un impact considérable sur l'innovation, les coûts et les délais de mise sur le marché des nouveaux services. De nombreux services de télécommunications qui auraient pu être lancés en l'absence de réglementation ont été avortés, ou n'ont été lancés qu'avec un retard considérable : cela a eu une incidence sur la compétitivité de l'entreprise concernée (par exemple, les entreprises de télécommunications tels que Nokia ou Ericsson n'ont pas pu réagir rapidement aux offres de leurs concurrents, dans ce cas Huawei). Aujourd'hui, et depuis 2016, la 5G est en cours de déploiement. Son déploiement nécessite des investissements importants dans les réseaux fixes et mobiles et les différents services qu'elle permettra sont aujourd'hui encore inconnus. Il est donc essentiel de veiller à ce que le cadre réglementaire devienne plus favorable aux investissements dans sa définition et son interprétation.

En ce qui concerne la 5G, la réglementation sectorielle a rendu la tâche plus difficile [47] pour les équipementiers et les opérateurs qui, pourtant, n'ont pas cessé d'innover dans de nouveaux réseaux et services : virtualisation des futures infrastructures 5G, réseaux privés, Open RAN. Dans ces cas, le soutien réglementaire est arrivé en retard, ou manque toujours. Et pourtant il était impératif de permettre

aux opérateurs de déployer ces nouveaux réseaux le plus efficacement possible en accordant des ressources spectrales pertinentes sur la base de licences individuelles, en temps utile et dans des conditions raisonnables, ainsi qu'en facilitant l'utilisation des micro-cellules. Il s'agit également de veiller à ce que l'évolution de ces réseaux ne soit pas entravée par une interprétation trop restrictive du règlement sur l'Internet ouvert. Tout cela rappelle les mises en garde des PDG de Nokia et d'Ericsson.

Une précaution excessive peut également entraver la compétitivité des acteurs privés. Une réglementation trop axée sur la prévention des risques peut créer des obstacles aux solutions innovantes, même à un stade précoce. La protection des données personnelles illustre parfaitement cette situation. Idéalement, il ne doit pas y avoir de contradiction entre la protection de la vie privée des clients et le développement de nouveaux produits et services. Dans ce contexte, toutes les questions relatives à la vie privée doivent être soigneusement évaluées lors du lancement de nouveaux produits et services centrés sur les données. Le *RGPD* aurait dû fournir un cadre de confiance permettant à l'UE de réaliser son marché unique numérique, en assurant un équilibre entre la protection des droits des citoyens en matière de données, et une plus grande innovation dans ce domaine. Concrètement, il aurait dû assurer une harmonisation des lois fragmentées censée protéger les entreprises et réduire les coûts de mise en conformité.

Le *RGPD* comprend de nombreuses exceptions et exemptions pour les États membres, ce qui leur laisse une grande marge de manœuvre. Cela a mené à différentes approches en matière de protection des données entre les EM, par exemple vis-à-vis du traitement des données sensibles, (données de santé notamment). Compte tenu du droit des EM à décider des questions de santé publique dans leur propre juridiction, la fragmentation et le manque d'harmonisation en ce qui concerne le traitement des données relatives à la santé sont vouées à se poursuivre.

Par ailleurs, certains termes non définis permettent une interprétation différente car très vagues : "retard excessif", "probabilité d'un risque (élevé) pour les droits et libertés" et "effort disproportionné" seront interprétés par les tribunaux à leur façon. Le niveau “raisonnable” de protection des données personnelles offre aux autorités une grande latitude d’interprétation lors de la formulation des sanctions. Le règlement écrit en 2016 adopte l’approche du traitement des données de cette époque et n’est pas adapté à l'ère du Big Data, de l'analytique, du chiffrement homomorphe ou de la blockchain qui ont connu un développement conséquent depuis. Cela entraînera des coûts de mise en conformité plus élevés et pourrait même conduire les entreprises à décider qu'il ne vaut tout simplement pas la peine de faire leur développement de produits de R&D en Europe : seulement 7% des entreprises allemandes interrogées en 2017 ne voient pas d’inconvénient au *RGPD*[48].

Le *RGPD* devient une contrainte pour les géants d’Internet dont le modèle économique est fondé sur la commercialisation des données en échange de la gratuité de certains services (Google, YouTube, Meta, etc.). La possibilité de refuser la collecte de certaines informations, telles que les adresses IP, peut rendre l’enquête sur les actes de malveillance plus difficile. Pour les partisans d’un Internet libre et ouvert, le *RGPD* peut donc paraître une menace redoutable. Pour les entreprises soucieuses de rester en conformité avec la loi, il leur faut mobiliser des ressource financières et humaines – compétences et connaissances, charge administrative, coûts - qui réduisent d’autant les ressources de production ou les investissements dans l’innovation. Certaines PME, par ailleurs, n’ont pas les ressources financières pour assurer leur conformité. Cela est d’autant plus vrai du point de vue de la sécurité de l’information car nombre d’entreprises manquent également de ressources pour protéger leur activité.

La Commission européenne[49] a estimé que le coût des obligations de mise en conformité réglementaire pour les entreprises de l’UE se situe entre 4% et 6% du PIB et que 15% de ce de ce chiffre est constitué de "paperasserie" évitable (qui désigne spécifiquement les charges de conformité inutiles).

Dans le sillage de la démocratisation rapide des technologies émergentes - IA, IoT, 5G, - les responsables de la réglementation sont confrontés à un défi majeur : comment protéger au mieux les citoyens, garantir des marchés équitables et faire appliquer les réglementations, tout en permettant à ces nouvelles technologies et entreprises de prospérer ? Cela devient encore plus complexe car ils doivent le faire tout en travaillant

dans les cadres existants, en essayant d'encourager l'innovation et en assurant une conformité avec d'autres réglementations mondiales. C'est l'exemple de la réglementation sur l'IA que l'Europe ne va pas tarder à publier et qui, selon Dionys Gragouian, Directeur AI Governance & Sustainability, chez DataRobot, va poser une série d'obstacles[50] :

> *The EU strikes again with a new set of regulations that take aim at the use of artificial intelligence (AI) to address the variety of risks associated with the societal adoption of AI. Like its sibling the General Data Protection Regulation (GDPR), the Artificial Intelligence Act (AIA) actually has teeth, with fines rising to €30 millions, or 6% of global revenue.*

Dans l'absolu, cela ne représente pas en soi un obstacle direct à l'innovation. Mais l'analyse du *Center Data Innovation*[51] considère que les impacts seront considérables[52] :

> *If adopted, the AIA will be the world's most restrictive regulation of artificial intelligence (AI) tools. It will not only limit AI development and use in Europe but also impose significant costs on EU businesses and consumers.*

Selon la même source, l'*AIA* coûtera à l'économie européenne 31 milliards d'euros au cours des cinq prochaines années et réduira les investissements dans l'IA de près de 20 %. Une entreprise dont le chiffre d'affaires est de 10 millions d'euros verrait ses bénéfices réduits de 40%[53]. Face à l'ambition de l'Europe qui souhaite que 75% des entreprises européennes utilisent l'IA d'ici la fin de la décennie, les nombreuses restrictions imposées par le règlement démontrent une absence de coordination et d'anticipation. L'écart d'investissements par rapport à la Chine et aux États-Unis en matière de développement et d'adoption de l'IA va se creuser davantage. A titre d'exemple, sur les 30 milliards d'euros de capital-risque privé investis dans des entreprises d'IA en 2019, moins de 10 % sont allés à l'Europe[54].

Plus la liste des restrictions s'allonge, plus la facture de mise en conformité et donc, de la solution, s'allongera et les fonds disponibles pour l'innovation et le développement des marchés diminueront. L'idée que la réglementation soit source de croissance est un tabou politique en Europe que peu osent remettre en question publiquement.

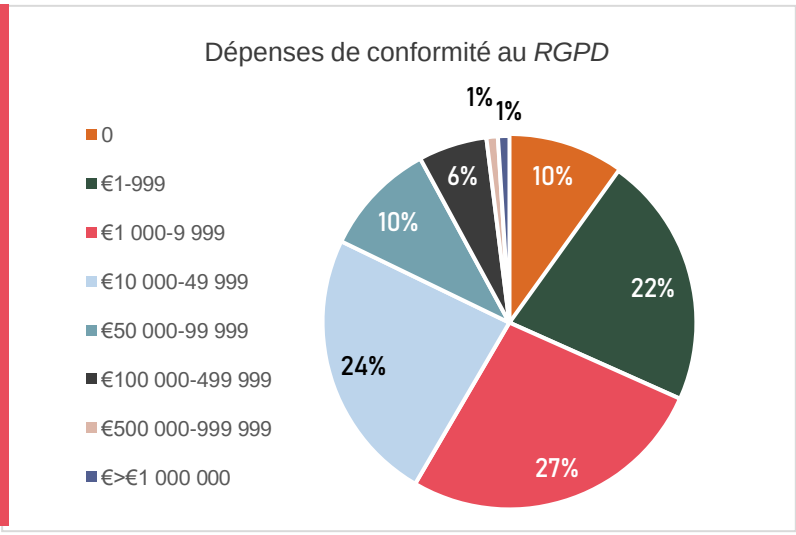
Le *RGPD* fournit un point de référence par rapport auquel les coûts de la mise en œuvre de l'*AIA*. 42% des PMI interrogées ont dépensé plus de 10 000€ pour mettre en œuvre le *RGPD*, plus de la moitié des PME déclarent avoir dépensé entre 1 000 et 50 000€ pour la mise en conformité avec le *RGPD*. Plus l'entreprise est grande, plus les frais augmentent, et pas toujours de manière linéaire cumulant des milliards de dollars[55]. On peut s'attendre à ce que l'*AIA* entraîne des coûts similaires, car tout comme l'*AIA*, le *RGPD* est un cadre horizontal qui peut toucher potentiellement plus d'un tiers des organisations européennes (éducation, infrastructures critiques, gouvernement, santé, défense, nouvelles technologies et télécommunications, énergie). L'IA n'est pas une industrie distincte ou une niche étroite de l'économie. Il s'agit d'une technologie qui touche tous les secteurs de l'économie et alimente en particulier l'économie numérique à croissance rapide. De plus, l'*AIA* impose aux entreprises un ensemble d'exigences plus détaillées. Ainsi, il est probable que les coûts

42%

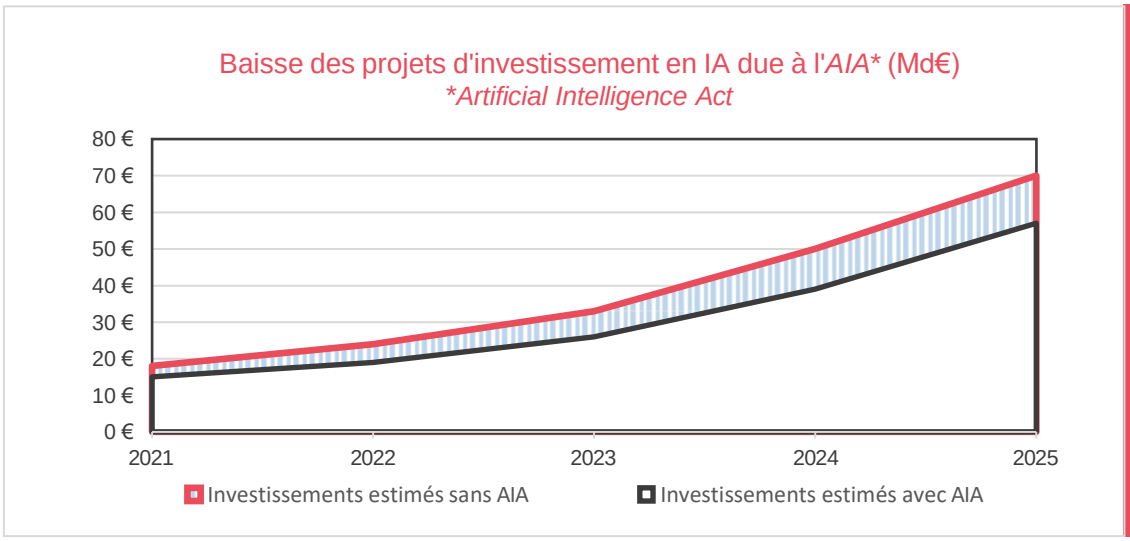
des PME ont dépensé plus de 10 000 €.

716 PME (<500 employés) interrogées en France, Irlande, Espagne et Grande-Bretagne.

Source : GDPR Survey 2019



de mise en œuvre du *RGPD* constituent une estimation inférieure des coûts de mise en œuvre pour les entreprises. Si les anticipations du *Center for Data Innovation* sont correctes, l'*AIA* va accroître le fossé entre l'Europe, les États-Unis et la Chine et risque ainsi d'encore réduire la vitesse de croissance de la productivité, et d'aggraver le retard en matière de compétitivité numérique dans les années à venir. Il n'est pas à exclure que des PME voudront éviter le marché régulé européen et s'installeront hors de l'Europe.



31Md€

d'ici 2025 seront perdus en Europe au titre de l'AIA

Données : Center for Data Innovation

Une approche conventionnelle de la sécurité au détriment du développement industriel

Les entreprises ont souvent une meilleure connaissance des pratiques malveillantes, puisqu'elles sont la cible principale des attaques cyber, mais aussi parce qu'elles achètent elles-mêmes des produits de cybersécurité. Dans certains pays, des infrastructures d'importance vitale se trouvent sous la gouvernance d'entreprises privées. Bien que les partenariats publique-privé[56] (PPP) soient nombreux dans le secteur de la cybersécurité, la coopération effective est variable. Il est difficile de s'assurer de la bonne intention du cyber-partenaire (les organismes publics sont parfois politisés). Toutefois, privé et public ne suivent pas les mêmes objectifs et peuvent adopter des perspectives différentes. C'est le cas en France pour la cybersécurité : l'ANSSI gouverne la sécurité des systèmes critiques, et cela concerne majoritairement des structures publiques. Les enjeux de la politique industrielle sont assurés par la Direction Générale des Entreprises et les deux mondes ne semblent pas communiquer. Aux trois dernières éditions du Forum International de la Cybersécurité (FIC)[57], aucun haut représentant de l'État, président ou ministre n'en a fait la visite. Guy-Philippe Goldstein soulignait cette approche française qui pénalise le développement industriel, à l'inverse de celle israélienne, ou états-unienne redoutablement efficaces :

> *En France on va militariser le sujet, on développe des solutions en interne, et comme c'est militaire, on ne peut pas l'exporter (c'est normal). Puis, à côté, on a des coopérations peu renforcées avec certains états proches.*

La première préoccupation du secteur privé est d'ordre économique, tandis que celle du secteur public est la sécurité civile. Cela rendrait donc difficile une définition claire des objectifs d'un tel partenariat. Pour cause, un accent considérable a été mis sur l'harmonisation des capacités et des infrastructures des États membres, et sur la garantie d'un niveau minimum d'exigences parmi les acteurs du secteur privé pour permettre la coopération d'un point de vue technique (*Directive NIS*).

Le partage d'informations sur la menace y figure en premier lieu, aussi bien que la transmission de bonnes pratiques. La confiance est essentielle à tous les niveaux afin de créer un environnement propice à l'échange d'informations sensibles par-delà les frontières.

Pour réussi à développer un tel partenariat, il faut s'assurer que l'échange d'informations est non seulement pertinent, et qu'il permet également d'obtenir une vision d'ensemble. Pour ce faire, il importe de parvenir à une conception commune fondée sur des outils reconnus. Si les échanges sur la cybersécurité entre grands groupes et États sont limités dans le temps et l'information communiquée

réduite au plus stricte nécessaire, cela ne relève pas de la solution la plus efficiente. A cet usage, certains canaux existent déjà sur la toile : le CTI (Cyber Threat Intelligence) peut se retrouver en open source comme à travers le programme STIX (Structured Threat Information eXpression). Ces protocoles privés reconnus et homologués par l'UE démontrent bien la nécessité de coopérer pour la cyber résilience. En prenant exemple sur cette initiative de partage de connaissance, les EM peuvent utiliser l'*European Union eXchange Cyber Threat Intelligence*, EUXCTI. Il s'agirait d'un outil délivrant une habilitation au pays membres et aux fleurons de l'UE leur permettant de communiquer en toute sécurité sur l'analyse de l'insécurité cyber mondiale, européenne et nationale. Cela leur permettrait de renforcer la défense de l'espace cyber européen. Chaque membre doit renouveler son habilitation une fois par an et les sanctions lourdes de conséquences sont censées faire respecter le pacte européen.

3.2. Une coopération linéaire européenne qui peine à trouver sa ligne directrice

Un manque d'alignement entre les institutions européennes

L'Union Européenne, à travers ses institutions, organismes et agences (EUIBA), s'emploie depuis plus de vingt ans à créer un cadre et des règles pour la cybersécurité en Europe, ce que nous avons vu dans le chapitre précédent. En raison des informations sensibles qu'elles traitent, les institutions, mais aussi organes et agences de l'UE, sont des cibles de choix pour les criminels, en particulier pour les groupes capables de commettre des attaques furtives très sophistiquées à des fins de cyber espionnage.

Pour toutes ces raisons, la confiance dans le pays d'origine du matériel informatique utilisé devrait être sans faille. Ainsi, avec beaucoup d'efforts et dans un élan d'européisme qui pousserait les institutions européennes à donner l'exemple et à n'utiliser que du hardware et du software d'origine européenne serait extrêmement bénéfique.

Si le choix de Microsoft pour équiper tous les bureaux des institutions peut éventuellement s'expliquer par la solution informatique globale offerte historiquement par l'entreprise américaine (hardware, software, Cloud), l'audit des contrats liant les EUIBA à Microsoft effectué par le *European Data Protection Supervisor* (EDPS) en 2019 met en lumière au moins 4 points critiques[58] de non-conformité au *RGPD* :

- le contrat permet à Microsoft d'agir non seulement en tant que data processor mais aussi en tant que *data controller* et de modifier à sa guise le traitement des données
- opacité sur l'identité des sous-traitants de Microsoft
- impossibilité de localiser les données et donc de garantir leur sécurité
- laxisme quant aux exigences contractuelles formulées vis-à-vis de Microsoft

> *« Les résultats préliminaires révèlent de sérieuses préoccupations quant à la conformité des clauses contractuelles pertinentes avec les règles de protection des données et au rôle de Microsoft en tant que sous-traitant pour les institutions de l'UE utilisant ses produits et services EDP »*

Plusieurs EM ont audité les contrats les liant à Microsoft, à l'instar des Pays-Bas, et y ont identifié les mêmes préoccupations. C'est d'ailleurs l'accord obtenu entre l'autorité judiciaire des Pays-Bas et Microsoft qui a servi de modèle aux institutions européennes dans leur volonté de mettre à jour les contrats. Toutefois, une certaine confiance naïve surprend dans un environnement si critique que celui des institutions européennes, ce qui a poussé EDPS à envisager la rédaction de contrats uniques, que les institutions européennes et les EM pourraient utiliser vis-à-vis des géants technologiques.

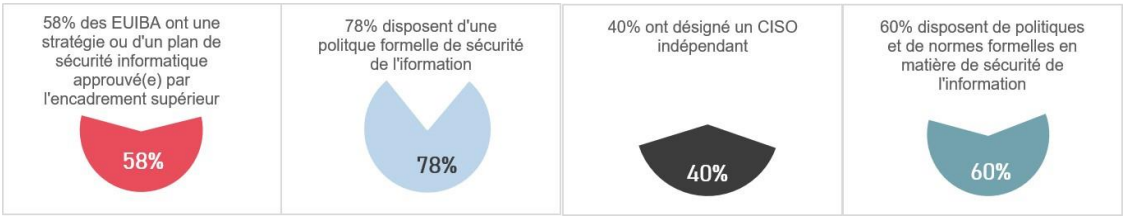
En termes de sécurité de l'information et des infrastructures, et bien que jouissant d'une indépendance institutionnelle et d'une autonomie administrative, l'interconnexion entre les EUIBA représente un risque de sécurité pour tout l'écosystème.

Chaque institution de l'UE dispose de ses propres règles de gouvernance relatives à la sécurité de l'information. De plus, un accord interinstitutionnel prévoit que la Commission prête assistance aux autres institutions et aux agences en ce qui concerne la sécurité de l'information. Les institutions et organes de l'UE ont enfin admis la nécessité de développer leurs capacités de cyberdéfense et leurs approches de la gestion des risques de manière cohérente. Le rapport de 2022 de la Cour des Comptes Européennes [59] visant à évaluer le niveau de maturité cyber des EUIAB met en avant une inégalité inquiétante : application insuffisante des bonnes pratiques en matière de cybersécurité, absence de certains contrôles essentiels, budgets clairement insuffisants alloués par plusieurs EUIBA, absence d'une véritable gouvernance et stratégie en matière de cybersécurité, de validation par l'encadrement supérieur, politiques de sécurité pas toujours formalisées et évaluations des risques trop partielles, insuffisance d'audits indépendants.

1300 systèmes informatiques et 50 000 appareils étaient utilisés en 2019 par la Commission Européenne à elle toute seule[60]. Il s'agit d'une énorme surface d'attaque.

Gouvernance en matière de sécurité informatique des institutions UE

Données : Cour des Comptes Européenne, 2022



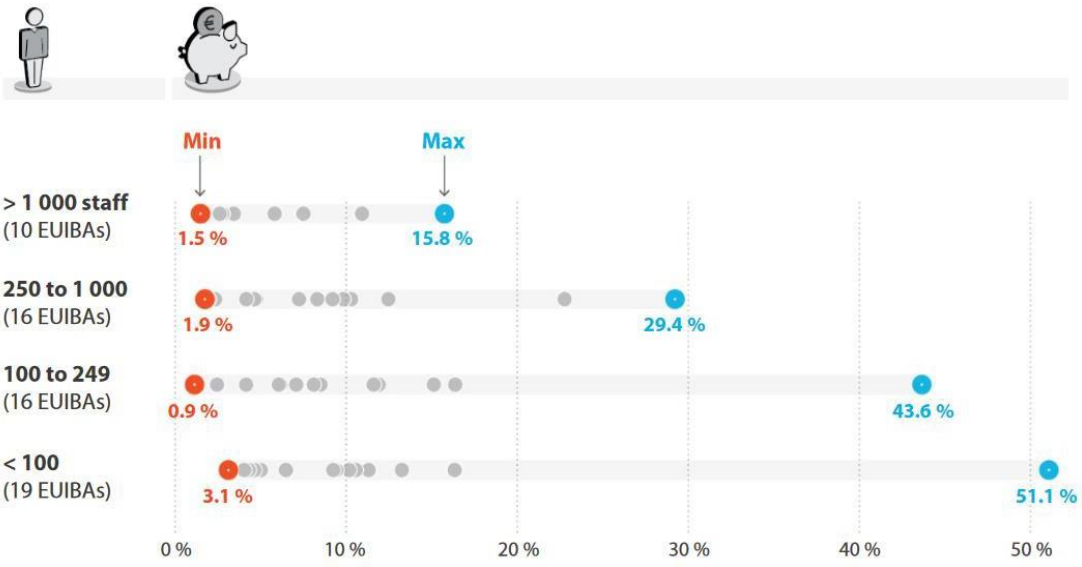
Du côté humain, les formations à la cybersécurité ne sont pas toujours systématiques - un peu plus de la moitié des EUIBA seulement offrent une formation continue en cybersécurité à leurs informaticiens et à leurs experts en sécurité informatique. Peu d'EUIBA imposent une formation en cybersécurité aux managers en charge des systèmes informatiques contenant des informations sensibles. Le recours aux exercices d'entraînement reste insuffisant.

Dépenses de cybersécurité en pourcentage des dépenses informatiques totales (répartition des EIBA sur la base des effectifs)

de 0,9 à 51,1%

dépenses pour la cybersécurité en pourcentage des dépenses IT

Source : Cour des Comptes Européenne, 2022



Bien que des structures de coopération et d'échange d'informations dans le domaine de la cybersécurité aient bien été mis en place, les EUIBA n'exploitent pas pleinement les synergies potentielles. On relève ainsi une absence d'échanges systématiques des informations relatives à leurs projets, à leurs évaluations de la sécurité et à leurs contrats de service en lien avec la cybersécurité. Par ailleurs, les outils de communication de base tels que les solutions de courrier électronique crypté ou de visioconférence ne sont pas totalement interopérables. Selon le même rapport, plus de la moitié des organisations a des failles dans la gestion des informations sensibles, la protection des terminaux mobiles ou la gestion des données au repos[61].

Au niveau de la réponse aux incidents, le CERT-EU et l'ENISA sont les deux principales entités chargées d'intervenir en cas d'incident. Toutefois, le rapport conclut qu'en raison de leurs ressources limitées et des priorités accordées à d'autres domaines, elles ne sont pas en mesure de fournir toute l'assistance qui serait nécessaire, vu le volume d'incidents. Ces incapacités d'assistance concernent notamment les EUIBA qui en sont à un stade moins avancé. Bien que le CERT-EU soit très apprécié dans les EUIBA, son efficacité est compromise par une charge de travail croissante, un financement et des effectifs instables (Annexe VIII), et une coopération insuffisante de la part de certains EUIBA, qui ne partagent pas toujours

en temps utile les informations sur les vulnérabilités et sur les incidents de cybersécurité importants qui les ont touchés, et qui sont susceptibles d'avoir une incidence sur les autres organisations.

Les insuffisances identifiées par le rapport de la Cour des Comptes ressemblent beaucoup aux problématiques rencontrées dans les EM. Une coopération et une coordination renforcées devraient permettre de solutionner plus de problèmes dont : le manque d'homogénéisation des pratiques de gouvernance et des stratégies cyber, l'interopérabilité pas toujours réelle entre les systèmes, les financements insuffisants ainsi que la formation humaine parcellaire.

Un élan de coopération militaire

Au même titre, l'Europe de la Défense est freinée par les volontés souverainistes de chaque membre. La cyberdéfense européenne se développe en parallèle d'une souveraineté immuable de chaque État Membre. Des difficultés similaires à celles existantes entre les institutions européennes semblent perturber les échanges entre certains EM, parfois de manière plus sérieuse. Le secret d'Etat et les informations sensibles empêchent le partage d'information. La définition même d'"information sensible " varie d'un pays à l'autre. Bien que la coopération fasse partie de l'ADN des agences de cybersécurité, comme l'affirme Anne Tricaud de l'ANSSI, le partage est toujours lié à un intérêt précis :

> *On partage parce qu'on a intérêt de partager et parce qu'on a protégé la manière dont on partage. Mais on ne partage pas pour partager*.

Ce partage est motivé par la gestion des risques préalable et non pas par la confiance réciproque. Ce partage individualiste et conditionnel n'est plus une coopération mais une négociation. De surcroît, la sécurité nationale est encore trop souvent invoquée comme raison de non-partage de l'information. Le Responsable Cybersécurité du National Health System écossais que nous avons interviewé confirme que le partage de *threat intell* « as wide as possible, with no secrets » est vital lorsqu'il s'agit de se défendre. Pour cela la communauté mondiale cyber utilise le Traffic Light Protocol [62] afin de catégoriser l'information de manière à ce que chacun sache ce qu'il peut faire avec l'information reçue.

Si les EM partagent la même compréhension des menaces et les mêmes préoccupations, grâce aux responsabilités vis-à-vis des infrastructures qui leur ont été imposées par les directives, les réponses à incident restent encore inégales à cause des niveaux de maturité défensive différents. Il n'est pas rare que des équipes cyber interviennent en signe de solidarité en cas de grosse attaque. Ça a été le cas suite à de puissantes attaques en août 2022 [63] (probablement d'origine russe) auxquelles des systèmes critiques de la République de Monténégro, membre de l'OTAN[64], candidat à l'adhésion UE soutenant les sanctions contre la Russie, a dû faire face. L'ANSSI, la Slovénie ainsi que l'OTAN sont intervenues lors de la détection, de l'analyse et de la remédiation technique à ces attaques. Le projet initial visait la création d'un centre régional de développement capacitaire cyber, porté par la France et la Slovénie[65].

Comment s'assurer de la réelle volonté de nos partenaires européens vis-à-vis de la France, par exemple ? En effet, la crise ukrainienne démontre que l'Europe de la Défense sera bientôt admise dans un service de réanimation. Alors que des projets étaient en discussion depuis plusieurs années avec la France, l'Allemagne a préféré les fournisseurs états-uniens pour les avions de chasse F35 achetés en mars 2022. De plus, l'Allemagne a dévoilé au salon EUROSATORY de juin 2022 le dernier char de RHEINMETALL, le FK51 "panther" après avoir fait miroiter un projet commun de char pour remplacer le Leclerc français et le Leopard 2 allemand. Dans ce domaine très spécifique de la Défense, il s'agit bien d'une opération de guerre économique : on a là un partenariat dupé par une entreprise nationale qui a ralenti la conception d'un projet à la base fondé sur un partage à 50% entre deux pays, puis une mise en vente d'un produit élaboré, conçu, testé, qui se veut exportable en dehors de l'Europe. Lors de projets aussi coûteux, emblématiques et stratégiques et en absence de confiance dans nos partenaires européens, il semblerait plus intelligent de rester méfiants sur la collaboration dans la cyberdéfense

Toutefois, par la nature intrinsèque de la cybersécurité qui ne s'arrête pas aux frontières physiques, les EM sont enclins à collaborer en cybersécurité. La création d'équipes d'intervention rapide en cas

Crédit photo : PESCO

d'incident informatique et l'initiative d'assistance mutuelle dans le domaine de la cybersécurité[66] sont deux projets favorisant un meilleur échange d'informations qui s'inscrivent dans le cadre du *Permanent Structured Cooperation* (PESCO). Il s'agit d'un succès qui a le mérite de rassembler des acteurs tant sur la dimension verticale qu'horizontale. La principale différence entre PESCO et les autres formes de coopération est la nature juridiquement contraignante des engagements pris par les 25 États membres qui se réunissent et travaillent à une soixantaine de projets communs. Malte (non alignée) et le Danemark (membre de l'OTAN) sont les deux pays qui ne participent pas au PESCO.

Le *Cyber and Information Domain Coordination Centre* (CIDCC)

Le CIDCC aspire à fonctionner comme un pôle de compétences pour connecter les capacités, compiler des données et les analyses, et contribuer à une efficacité accrue des entités de l'UE dans les domaines du cyber et de l'information. Il se concentrera clairement sur la défense, et le domaine de l'armée, mais cherchera également à interagir avec toutes les institutions, les organismes et les agences. Il est envisagé d'établir le CIDCC en tant que partie intégrante de la structure du Conseil de l'UE dans l'intérêt commun de tous les EM.

Le mécanisme de *Cyber Rapid Response Team*[67]

L'une des solutions envisagées au niveau européen pour mettre en œuvre une solidarité entre les EM sur les questions de cybersécurité. Le projet a été initié en 2020 et compte pour l'instant six pays actifs au sein de la structure : la Lituanie, la Croatie, la Pologne, l'Estonie, la Roumanie et les Pays-Bas. D'autres membres de l'UE, parmi lesquels la France, participent également au projet en tant qu'observateurs. L'objectif de cette structure est de permettre de former des équipes de réponse à incident composées d'experts provenant de plusieurs EM pour assister un pays membre de l'Union européenne ou un pays allié afin de faire face à une crise cyber.

À travers les projets dédiés à la cyberdéfense[68], trois grandes missions ont été identifiées : connecter, composer, et contribuer.

- ✓ Connecter : le CIDCC est en charge d'établir un lien entre les parties prenantes concernées de l'UE pour renforcer l'échange d'informations et améliorer la coordination des activités relatives à l'opérationnalisation des CID.
- ✓ Composer : le CIDCC doit collecter, fusionner et scruter les données et informations pour accroître la connaissance de la situation et pour fournir une analyse globale ainsi que des recommandations personnalisées.
- ✓ Contribuer : le CIDCC devra orchestrer les effets souhaités au sein du CID et fournira un soutien et des conseils quant à la planification et la conduite des opérations de l'UE et de ses missions.

PESCO permet donc aux EM de collaborer afin de développer des solutions à usage militaire et de se défendre réciproquement en cas de grande crise. C'est un mécanisme qui a le mérite de poser les bases d'une défense militaire autonome. En dehors du contexte militaire, le partage d'information se résume à une négociation et nombre d'informations sur les menaces pourraient ne pas être divulguées, puisque le secret d'état y contribue. Aux Etats-Unis, ce sont les entreprises et les chercheurs privés qui font circuler une grande quantité de renseignements sur la menace. Lier la bataille pour le leadership de l'information à la compétitivité et à la renommée semble être une stratégie gagnante. Qu'en est-il du secteur privé européen ?

Un problème de confiance nuisible à la coopération dans le secteur privé

La vision de l'Union articulée dans la *Stratégie EU-CSS* intitulée « *Un cyberespace ouvert, sûr et sécurisé* » repose sur cinq priorités qui, en fin de compte, rapprochent les enjeux de sécurité et de développement économique. La stratégie dessine un lien fort entre le renforcement de la cybersécurité et le développement de ressources industrielles et technologiques propres à ce secteur.

Toutefois, sur le terrain, certains acteurs du secteur privé font preuve d'une priorisation exacerbée de la dimension économique parfois aux dépens de la sécurité, voire même en totale opposition avec les cinq objectifs formulés dans la *Stratégie de cybersécurité européenne*.

Face à l'écrasante compétition états-unienne, à la montée en puissance des Chinois et aux obstacles réglementaires européens, les entreprises européennes ont varié les initiatives, allant de la mutualisation à des tentatives de coopération.

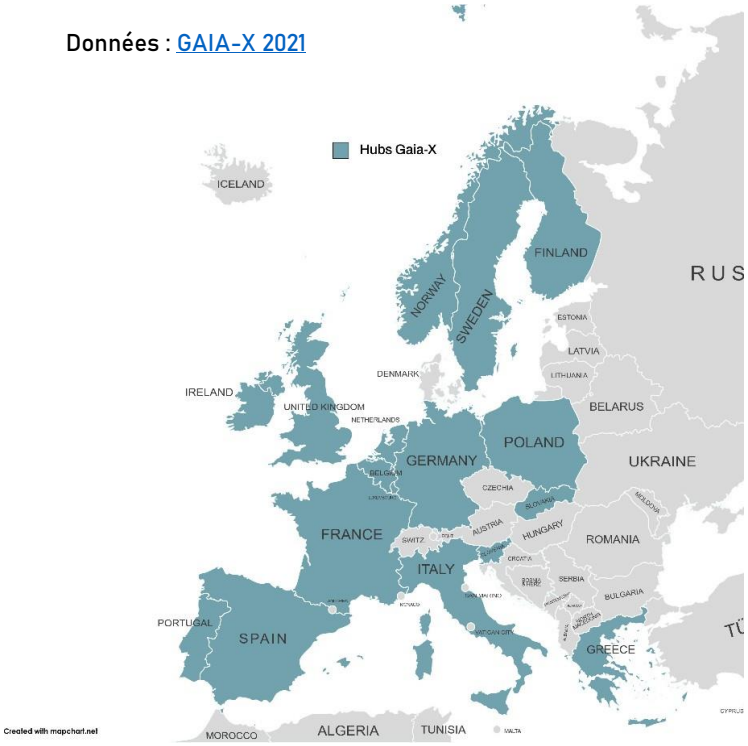
Pour les services dans le Cloud, la dépendance états-unienne est écrasante car plus de 70% des capacités du Cloud mondial se trouvent entre les mains des GAFAM. Dans ces conditions, le rêve d'une solution 100% européenne renaît avec le projet collaboratif Gaia-X.

La coopération franco-allemande lancée, pas sans peine, en 2020 dans le cadre du projet Gaia-X vise à donner vie à une infrastructure fédérée de données qui mettent davantage l'accent sur la sécurité, la transparence et la protection des données. Celles-ci sont partagées ouvertement, les utilisateurs conservant le contrôle de leurs données. Son ambition est de devenir la place de marché européenne permettant de mettre en relation fournisseurs de capacités de stockage et entreprises européennes : le partage de données se ferait en toute transparence et la réversibilité permettrait de déplacer aisément les données d'un fournisseur à l'autre.

Bien que née d'une coopération bilatérale, Gaia-X réunit en 2021 plus de 340 organisations et entreprises européennes, dont 40% des PME[69], issues du monde politique, économique, industriel et scientifique. 16 pays ont d'ores-et-déjà défini des hubs sur leur territoire (cf. carte).

Néanmoins, des inquiétudes voient le jour lorsque Gaia-X décide d'ouvrir la porte aux grandes entreprises technologiques étrangères, alors que son but était de façonner un projet européen : Microsoft et Amazon participent désormais aux groupes de travail et sont des membres à part entière grâce à leurs filiales en Europe. OVH, qui en fait aussi partie, a annoncé devenir un intégrateur du Cloud Google. Son directeur par intérim est le français Hubert Tardieu d'Atos, partenaire stratégique de Google également. Dans cette lignée, la longue liste des sponsors du *GAIA-X Summit 2021* incluait Huawei, Alibaba, Microsoft et AWS.

Données : GAIA-X 2021



Sans surprise, de plus en plus de voix s'élèvent contre l'orientation prise par l'association GAIA-X et les premiers départs n'ont pas tardé. Hosteur a quitté l'association fin 2021. Le fournisseur français de cloud computing Scaleway s'est également retiré du projet, citant l'influence étrangère comme l'une des raisons de son départ. Pour son PDG français Yann Lechelle[70], Gaia-X est en dehors de son orbite :

> *On ne peut plus rien attendre de GAIA-X qui a adopté une approche très conservatrice du cloud de confiance. D'un point de vue structurel et fonctionnel, il n'y a pas d'innovation et lorsque l'harmonisation se fait à partir de dénominateurs communs, on est dans un tropisme d'acteurs dominants qui rejettent toute différence. […] On n'a pas besoin des étasuniens dans les comités techniques, mais ils sont finalement indirectement ou directement aux manettes, donc il n'y a plus de souveraineté. […] Les américains ont quant à eux les capacités humaines, légales et de lobbying pour faire ralentir tout le monde si cela les arrang*

La désillusion est de taille car un problème de communication s'est posé dès le départ. Gaia-X n'a jamais été conçue comme une alternative aux offres des fournisseurs de cloud états-uniens. Cependant, beaucoup l'ont compris de cette manière. Gaia-X se proposait de trouver des solutions d'interopérabilité, un ensemble de règles et de normes communes pour un usage des données des organisations européennes, en accord avec le cadre législatif propre à l'Europe. Le but global n'était que de faciliter la circulation des données partout dans l'espace géographique européen. Gaia-X serait plutôt un Amazon Marketplace des data qu'un AWS. De surcroît, sur la liste des membres publiée le 29 mars 2021, figurent Alibaba Cloud Singapore, Palentir, Microsoft NV, Google Ireland, AWS Europe Core, Huawei technologies Düsseldorf, IBM Belgium, Oracle[71]. Après toutes les affaires d'écoute et d'espionnage de l'Est et de l'Ouest, aligner tous ces noms en tant que membres d'un projet européen défie toutes les lois de la confiance et marque le retour à la case de départ.

Le contrat de confiance est rompu et il semblerait que l'histoire ne fasse que se répéter. Dix ans avant Gaia-X, le gouvernement français avait lancé le projet Andromède pour faciliter la création d'un cloud souverain. Les trois entreprises françaises impliquées, parmi lesquelles les membres du premier jour de Gaia-X, Atos, Thalès et Orange, ont ignoré les fournisseurs de cloud français qui avaient démontré leur capacité à fournir des solutions IaaS, multi-datacenters et de haute disponibilité (par exemple NiftyName) utilisant un logiciel de virtualisation open-source français (Qemu). Elles ont préféré utiliser 150 millions d'euros de fonds publics pour soutenir une technologie états-unienne émergente appelée OpenStack. Disposant de suffisamment d'argent pour surpasser les efforts marketing des PME européennes, les intégrateurs d'OpenStack ont également utilisé ces fonds pour débaucher des ingénieurs clés d'autres entreprises françaises de Cloud telles que Gandi.net, ce qui a conduit à des allégations selon lesquelles l'argent public a été dépensé pour nuire aux entreprises françaises et européennes. L'effritement de la confiance a ainsi fait échouer Andromède.

La mutualisation des ressources : un début de coopération

Conscientes de l'importance de la confiance à avoir dans le pays d'où provient le matériel informatique, 70 organisations[72] ont formé la *European Cyber Security Organisation* (ECSO) afin de booster le développement industriel de la cybersécurité en Europe. L'organisation a défini et publié un schéma de certification privée pour la cybersécurité, *CYBERSECURITY MADE IN EUROPE* qui certifie aujourd'hui 90 entreprises à travers l'Europe[73]. Elles doivent remplir les conditions suivantes :

- siège social situé en Europe. Si l'entreprise fait partie d'un groupe, le siège social du groupe doit être enregistré en Europe

- absence de propriété ou de contrôle majeur en dehors de l'Europe
- lieu principal d'activité en Europe : plus de la moitié de leurs activités de R&D en cybersécurité et/ou de leur personnel doivent être en Europe
- solutions sécurisées respectant les exigences des *Indispensable baseline security requirements for the secure ICT products and services* de l'ENISA.

A travers son groupe de travail 4, *Support to SMEs, coordination with countries and regions*, l'ECSO se propose de faciliter la coopération entre les autorités régionales européennes et les décideurs politiques européens. L'échange de bonnes pratiques et l'amélioration de la compétitivité des start-ups et des PME locales en matière de cybersécurité vise à stimuler un réseau paneuropéen commercial. Cela implique le développement des compétences en marketing des start-ups et PME locales de cybersécurité, et doit en résulter une meilleure compétitivité de ces entreprises au niveau européen. En 2020, l'ECSO a également proposé à la Commission Européenne et aux principaux investisseurs dans la cyber européenne la création d'une plate-forme unique dédiée à ces investissements. 49 signataires originaires de 18 pays membres y ont déjà adhéré. La plate-forme devrait mettre à la disposition de l'écosystème cyber européen 1 milliard d'euros d'investissements pour les cinq années à venir[74].

La coopération dans le secteur privé passe également par la mutualisation des investissements, dans le but de faire émerger des solutions innovantes. C'est le cas de la start-up Clear qui propose en 2019 une solution de blockchain d'essai pour le règlement des accords de réduction de l'itinérance, suite à un investissement de 13 millions de dollars [75] de la part de l'espagnol Telefónica et de l'allemand Deutsche Telekom. L'opérateur britannique Vodafone a également adhéré au projet. Les trois opérateurs des télécommunications appellent d'autres fournisseurs à rejoindre le réseau des utilisateurs de la solution Clear, dans l'espoir que le règlement automatisé de l'itinérance stimulera de nouveaux partenariats commerciaux pour soutenir les nouveaux services nécessaires aux technologies telles que la 5G, l'informatique de pointe et l'IoT.

Un autre projet de mutualisation des ressources a été mis en place en octobre 2021 par quatre opérateurs de l'industrie des télécommunications à travers leurs structures dédiées à l'innovation : les start-ups de Singtel (Singtel Innov8), Orange (Orange Fab), Deutsche Telecom (hub:raum) et Telefónica (Telefónica Open Future)[76]. Le partenariat vise à catalyser la croissance des start-ups éligibles et à les lancer au-delà de leurs marchés domestiques respectifs en leur permettant de tirer parti des ressources et du réseau des quatre opérateurs de télécommunications majeurs. Des passerelles entre les écosystèmes de start-ups à travers l'Asie du Sud-Est, l'Afrique, l'Europe, l'Amérique Latine et le Moyen-Orient pourraient être ainsi créés. À terme, ces passerelles visent à aider les opérateurs de télécommunications à améliorer l'expérience digitale des entreprises dans le monde entier.

Les mutualisations sont nombreuses dans le domaine des services Cloud, mais ce n'est pas forcément le cas en ligne avec la *Stratégie de cybersécurité*, à l'exemple des récents projets Bleu, réunissant Orange, Capgemini et Azure, les collaborations Thalès-Google, Nokia-Azure, Deutsche Telekom-Google, Telefónica-Oracle, Ericsson-Google, etc. De telles coopérations risquent davantage de transformer les principaux acteurs européens en des simples distributeurs de logiciels et d'applications états-uniennes que d'offrir une liberté de choix à l'abri d'intérêts étrangers. À l'avenir, *« on peut très bien imaginer que les données publiques seront hébergées en France, remarque un hébergeur, dans une ferme de données construite par l'américain Equinix, sur des serveurs Intel, utilisant les technologies cloud de Microsoft, l'IA de Google, les algorithmes de Google, les logiciels de chiffrement développés conjointement par Thalès et Google. Le label "cloud de confiance" servira de faux-nez aux GAFAM et sans doute à la NSA. »*[77] Sans parler de la sécurité du code source qu'il sera impossible d'auditer.

Ces quelques exemples montrent bien que la coopération est une priorité pour quelques acteurs privés. Ce sont surtout les entreprises de technologies qui s'y impliquent fortement, conscientes de l'impossibilité d'agir individuellement. La mutualisation des connaissances et des savoir-faire est plus courante entre les entreprises du même pays, et rarement sur la même verticale. Lorsque la tâche devient gigantesque, il semble impossible aujourd'hui de se passer des géants états-uniens, notamment par rapport aux besoins liés aux services du Cloud.

OBSTACLES ET INCOHÉRENCES

CHAPITRE QUATRE

4.1. Les obstacles à la coopération

En termes de coordination, l'attitude, le comportement et le résultat liés à la formulation conjointe des objectifs communs de la stratégie de cybersécurité de la part des acteurs européens sont globalement unitaires (cf. Indice de souveraineté à la fin du chapitre 1). Les menaces cyber ne sont plus un mystère pour personne. L'engagement des EM en faveur d'une plus grande autonomie stratégique est globalement suffisant. Le travail de coordination réalisé par l'ENISA, bien qu'imparfait, porte néanmoins ses fruits. Ce sont les capacités qui non seulement varient d'un état à l'autre, mais la moyenne européenne est mauvaise (3/10 selon l'indice d'EUFR)[1]. La coopération, elle, fait référence à l'attitude, au comportement et au résultat de la mise en œuvre de ces objectifs tels qu'ils ont été convenus. Ici aucun acteur n'est champion dans la poursuite d'intérêts mutuels et de bénéfices communs. Si les alliances existent, quand l'un des acteurs ne fait défaut (les EM pour la 5G), c'est le manque de confiance qui fragilise la coopération (Gaia-X). Ni la concurrence ni la compétition ne sont compatibles avec la coopération. Or dans les nouvelles technologies la concurrence est âpre car les enjeux économiques sont gigantesques, sans parler des enjeux de défense militaire et de stabilité géopolitique. Si la concurrence est un des obstacles à la coopération, il n'est pas le seul.

Dans ce dernier chapitre, nous allons donc nous pencher sur quelques facteurs qui font obstacle à la coopération européenne en matière de cybersécurité.

Une Europe orpheline de son récit

Un projet de coopération et de collaboration nécessite un récit fort et clair pour être mené à bien. Les États-Uniens, les Chinois, les Russes, les Israéliens, toutes les grandes cyber puissances ont développé un récit qui porte leur projet de civilisation au sens large, incluant leur projet numérique.

Le récit états-unien : Longtemps autoproclamés gendarmes du monde, les États-Unis se présentent au monde comme les défenseurs de la liberté et de l'innovation sans frontières. Dans ce cadre, la donnée est nécessaire pour nourrir les agences de renseignement états-uniennes, mais aussi une source de business pour les entreprises, largement exploitée aussi à des fins de guerre économique.

Le récit chinois : Contre l'impérialisme états-unien, la Chine veut redevenir l'empire qu'elle a été par le passé, avec la volonté de dominer l'économie mondiale, et ainsi garantir un niveau de vie digne à ses citoyens. Compte tenu de sa population, le défi est colossal. Pour cela, la surveillance par la donnée numérique est un outil essentiel. Internet est contrôlé à des fins sécuritaires, et exploité à des fins d'espionnage économique principalement.

Le récit russe : La Russie œuvre pour le retour de l'empire soviétique, notamment par la reconquête des ex-pays membres de l'URSS. Le récit russe pointe du doigt les faiblesses des démocraties européennes et occidentales trop laxistes, trop permissives. La Russie entretient une volonté d'interférer au sein même de ces démocraties, notamment par le biais d'une guerre de l'information, et de cyberattaques destructrices.

Le récit israélien : "Hasbara" – est un terme utilisé par l'état d'Israël, qui signifie littéralement "explication" en hébreu. Il s'agit de penser et d'expliquer le monde, pour décrire les efforts déployés par les politiques gouvernementales et promouvoir l'État d'Israël. Enfin, le terme "cyber" n'a pas de traduction en hébreu, mais phonétiquement, on pourra le prononcer "*CBR*" ou [*CéBéaR*], qui veut dire "penser le monde, modeler le monde". Ça ne s'invente pas.

En Europe, le récit est jeune, né après la Seconde Guerre mondiale : l'économie (le marché), et un libéralisme "européanisé" (réglementé) apporteront croissance et prospérité, pour les entreprises et les citoyens européens, et maintiendra ainsi la paix sur le continent. Fort est de constater qu'aujourd'hui, ce récit ne tient plus. La guerre est réapparue sur le continent européen, et les inégalités économiques sont toujours source de fortes tensions sociétales. Il semble donc indispensable pour l'Europe de construire un nouveau récit.

Depuis cinq à dix ans, nous observons les premières lignes de ce nouveau récit, mais sa construction (accélérée par la pandémie de Covid19) est encore hésitante. De plus, ce récit est fréquemment déconstruit par des États membres qui, de défenseurs sont devenus avec la pandémie des opposants. Les bénéfices d'une zone de libre-échange ne sont plus suffisants, trop fragiles, et inégalement exploités. Les dépendances multilatérales en matière de commerce, d'énergie, de défense, et de technologie font vaciller le récit européen. Si l'approche par le libre marché a fonctionné pour de nombreux États membres, dont l'Allemagne, les Pays-Bas, et les pays de l'Est, cette même approche a montré ses limites et ses risques depuis le début du conflit en Ukraine.

Des attitudes trop différentes face à la menace

Certains États membres (EM) ignorent tout simplement les risques auxquels leurs systèmes d'information sont exposés. Comme illustré précédemment, la perception du cyber risque est très variable au sein des EM, tout comme leur niveau de numérisation. Ignorer le risque, ne pas connaître sa surface d'attaque ne permettent pas une gestion des risques efficace. C'est ce que constate en France Ali Jaghdam, enseignant-chercheur à EM Léonard de Vinci qui parle d'une certaine naïveté[2] :

> *Les risques cyber font encore plus peur aux assureurs qu'aux assurés.*

C'est une raison de plus pour approcher la menace cyber de la manière la plus objective possible, par une analyse des risques. Toujours en France, la gestion des risques reste un sujet mal aimé : on sait qu'on en a besoin mais on n'aime pas en parler. Ainsi, selon une enquête menée au sein du Club des Experts de la Sécurité de l'Information et du Numérique (CESIN) en 2017, si l'implication des RSSI dans la gouvernance d'une assurance cyber est très forte (83,7%), celle des Risk Managers (62,8%) n'est pas au même niveau, alors que cela devrait être le cas [3] ; sans parler de l'implication des dirigeants qui sont moins de 1 sur 2 à s'y intéresser.

Certes, les directives européennes et autres règlements comportent de nombreuses préconisations, mais leur efficacité est, comme nous l'avons vu, questionnable. L'approche de la menace doit se faire de la manière la plus objective possible, par une analyse des risques. Selon la même enquête, 58,8% des interrogés reconnaissent des difficultés à modéliser et à quantifier les risques en interne. La France, et probablement d'autres pays européens, pêchent par une culture des risques insuffisante. Les deux méthodologies les plus utilisées au monde sont états-unienne (PMI Institute) et britannique (Prince2). Et pourtant des méthodologies dédiées aux risques cyber existent, à l'exemple de l'ISO 27005 et EBios Risk Manager. L'ISO 27005 est pénalisée par sa faible diffusion car elle est payante ce qui fait qu'elle est très peu utilisée en Europe. La méthodologie de l'ANSSI EBios Risk Manager actualisée en 2018 reste aussi d'application restreinte car conçue pour les OIV et les organisations de l'état.

Pour toute une série d'arguments, EBios RM pourrait en faire partie, la France se dit confiante dans sa stratégie de cybersécurité. Pourtant, combien d'entreprises ont une politique de sécurité des SI en place ? Exceptés les OIV, et OES, combien de ces politiques suivent une méthodologie standardisée ? Selon quelle méthode ? Combien d'entre elles ont réalisé un audit externe des risques cyber ? Combien d'organisations ont une politique de sauvegarde adaptée et testée ? Combien ont un plan de reprise d'activité, qui est testé au moins une fois par an ? Combien d'entreprises testent, dans un environnement protégé, les mises à jour avant leur déploiement dans leurs SI de production ?

En réalité, les acteurs privés, opérateurs ou entreprises, sont très peu incités à renforcer la sécurité au-delà du strict nécessaire. Comme le disait le PDG d'Ericsson, à partir du moment où l'efficacité de la connectivité se mesure en dollars-par-gigabyte, quel citoyen penserait à la sécurité le moment du choix venu ? La réalité est que personne ne pense payer plus cher pour la sécurité de tel ou tel réseau de télécom ou équipement. La sécurité, de nos jours n'est pas assez encouragée, selon le Directeur technique du *National Cyber Security Center*[4] britannique :

> *No-one currently buys telecoms services based on how secure they are, so a company wouldn't get rewarded if they invested more than their competitors in making a more secure service. That leads to a weird situation where you don't get rewarded for doing the right thing, which makes it hard to do, long term.*

Cela mène à des niveaux de maturité hétérogène, qui se reflètent, à leur tour, lors de la conception des actes législatifs. Les schémas de certification des produits et services de cybersécurité prévu dans *Cybersecurity Act*, à part le fait qu'il est volontaire, comprend le premier niveau qui n'engage l'entreprise à aucune analyse des risques ni audit. Tant que la sécurité sera déclarative ou considérée comme une dépense optionnelle, des lacunes continueront à apparaître à mesure que le cyberespace évolue et les technologies se complexifient. Désormais il faut aller plus loin et aligner tous les acteurs sur la dimension critique et stratégique des nouvelles technologies.

Une Europe structurellement incompatible avec le développement industriel

La 5G est la technologie qui, par un concours de circonstances, a accumulé des défaillances et des manquements généralisés. Nous rappelons qu'à l'époque de la 3G l'Europe était le leader mondial. Aujourd'hui l'Europe est en retard sur tous les critères : part de marchés (Ericsson et Nokia se placent derrière Huawei), couverture des territoires (66% de la population en 2021)[5], offres commerciales (2 pays européens toujours sans offre commerciales en mars 2021[6]), et performance (la majorité des pays offrent des vitesses en deçà de 200 Mbps).

Dans le domaine des solutions de cybersécurité, la Cour des Comptes européenne évalue comme insuffisante l'efficacité des entreprises européennes face aux concurrents états-uniens et israéliens[7] :

> *Globalement, les entreprises de l'UE spécialisées en cybersécurité affichent des performances inférieures à celles de leurs homologues internationaux : elles sont moins nombreuses et le montant moyen des fonds qu'elles lèvent est nettement plus faible. Il est donc indispensable de garantir un ciblage et un financement efficaces des jeunes entreprises pour atteindre les objectifs de la politique numérique de l'UE.*

Des insuffisances structurelles au sein de l'UE ont été mises en avant, notamment lors du déploiement de la 5G. Plusieurs articles et interviews soulignent la frustration grandissante des industriels et des cadres technologiques européens à un moment où les politiciens tirent la sonnette d'alarme sur le déclin technologique et la dépendance croissante à l'égard des entreprises étrangères. Le PDG d'Ericsson Ericsson affirme que, pour l'instant, le soutien aux entreprises locales reste faible dans son pays d'origine, la Suède, et dans toute l'Union européenne, ce qui renforce la confiance de ses rivaux. Quant aux investissements, c'est plus facile hors-Europe que dans son propre pays[8] :

> *We get more support in other geographies than we get in Europe. We have almost the weakest market share in Sweden … Our competitors think that, if you can win in Sweden, you can market that to every other operator globally by saying : Look, we can even win in Sweden.*

Certes, l'UE s'est mise à travailler à la rédaction de boucliers commerciaux, d'outils de concurrence et de politiques de marchés publics - y compris sur des restrictions potentielles vis-à-vis des entreprises et des investissements chinois. Mais les temps européens sont trop longs par rapport à la vitesse à laquelle les nouvelles technologies avancent et les marchés évoluent. Pour la 5G, exemple édifiant des insuffisances structurelles de l'UE et des EM, la position de la CE vis-à-vis de Huawei a été arrêtée quatre ans après le moment où elle était attendue. Le 10 novembre dernier, Margrethe Vestager, vice-présidente de la Commission en charge du numérique, pointait l'Allemagne[9] :

> *We are urging member states who have not yet imposed restrictions on high-risk suppliers to do that without delay, as a matter of urgency.*

Pendant ce temps, les EM sont passées par toutes les nuances d'acceptation du matériel chinois. Trois pays pourtant n'ont toujours pas pris des mesures de limitation de Huawei, les intérêts nationaux prévalant sur les intérêts européens. : la Hongrie, l'Allemagne et le Portugal.

Ces intérêts nationaux peuvent également interférer avec le processus de création et d'application des directives par lesquels l'UE légifère. La rédaction et surtout la transposition d'une directive européenne n'est pas simple, pour différentes raisons.

Tout d'abord, l'exercice peut se heurter *de facto* à la mauvaise volonté des EM. Cela étant dit, on peut, en effet, se demander si le vote à la majorité qualifiée n'entraine pas certains effets "pervers" au moment de la transposition, liés aux réticences particulières des États qui n'ont pas voté en faveur de la directive européenne concernée. Une prise de décision à l'unanimité où chaque État membre doit donner son accord à l'adoption du texte ne faciliterait-elle pas, dans une certaine mesure, l'opération de transposition ? Rien ne le garantit en réalité. L'avantage ou le désavantage que représente l'une ou l'autre de ces procédures décisionnelles au stade de l'adoption de la directive aurait-elle un rôle inverse au stade de la transposition ? Cela doit être nuancé. En effet, même si elle peut paraître simplificatrice, l'adoption à l'unanimité peut être un frein, dans la mesure où les acteurs intervenant au moment des négociations et de l'adoption, d'une part, et au moment de la transposition, d'autre part, ne sont pas nécessairement les mêmes. En effet, le temps politique est un temps long, et les gouvernements changent régulièrement dans les régimes démocratiques. Mécaniquement, il faudrait peut-être des années et beaucoup de progrès technologique, politique et social pour qu'une mesure soit adoptée à l'unanimité.

Au-delà de la résistances politique, "l'insertion" des directives dans les droits nationaux peut s'avérer juridiquement ou techniquement complexe. Les raisons de ces difficultés sont nombreuses. Elles peuvent être liées au contenu de la directive elle-même, ou au contenu du droit national, mais aussi au rapport entre les deux. Selon que les directives se montrent plus ou moins précises quant au résultat à atteindre et, donc, plus ou moins généreuses dans la marge de manœuvre qu'elles laissent aux EM, elles sont plus ou moins difficiles à transposer. Plus grande sera leur flexibilité, plus grande sera la faculté d'adaptation laissée aux États, plus facile devrait logiquement être leur transposition. Par ailleurs, la transposition d'une directive nécessite souvent une interprétation des règles et des formulations qu'elle consacre. Cette interprétation peut se révéler problématique. Cela nécessite également une harmonisation avec les législations locales afin d'assurer une cohérence législative dans chaque pays membre.

De manière schématique et quelque peu caricaturale, l'exercice de transposition sera d'autant plus difficile que le secteur de la sécurité fait déjà l'objet d'une réglementation étoffée en droit interne ou de principes bien ancrés dans le droit national. Cela est encore plus complexe, car les règles nationales préexistantes peuvent être différentes des normes figurant dans la directive à transposer, puis tout ce travail est rendu long par le nombre considérable de textes nationaux à modifier, etc.

Comme déjà évoquées, les positions de chaque État souverain viennent trop souvent ralentir la machine européenne, par une volonté protectionniste ou des stratégies économiques nationalistes. En imposant aux EM une autonomie numérique européenne, l'Europe en sortirait renforcée. Cette souveraineté implique une volonté d'autonomie stratégique sur le champ matériel informatique, dans la technologie Cloud, en s'appuyant sur le cadre politique et juridique européen (NIS, NIS II, *RGPD*, etc.). Les volontés sont déjà présentes mais ne sont pas suivies, ou partiellement, par tous les EM. Pour cela, les États doivent s'inscrire dans le temps long, le temps 3 de la méthodologie militaire[10]. Se référer à la méthode militaire n'est pas anodin, en effet, d'autres puissances cyber construisent leur stratégie de cybersécurité en s'appuyant sur l'expertise et les méthodes militaires. Dans les faits, ce modèle militaro-centré collaboratif s'avère très efficace (modèles états-unien et israélien). Il faut définir les adversaires et concurrents malgré les partenariats, et les échanges économiques extra européens. Il ne faut pas craindre de définir le champ d'action, le terrain de bataille dans lequel l'Europe doit faire face. Le combat est d'autant plus vicieux que l'ennemi peut être un partenaire commercial ou un allié politique et économique dans un autre domaine, sous un enjeu différent. Cependant, ces mêmes États raisonnent froidement pour manœuvrer au mieux, malgré le brouillard de la guerre.[11]

Les gouvernements doivent avoir l'honnêteté intellectuelle de dépasser leur mandat et leurs frontières pour suivre la *Stratégie européenne de cybersécurité* afin d'édifier le système cyber autonome européen en parallèle des autres politiques. La souveraineté des États en serait d'autant plus consolidée, résiliente

et immuable face aux nombreux acteurs sur ce champ de bataille planétaire. La fragmentation de la cybersécurité entre plusieurs services de l'état qui ne communiquent pas a montré ses conséquences. La France en ce sens est à l'image de l'Europe : en avance sur certains points de sécurité mais en retard du point de vue industriel. Des pays comme la France ou la Suède n'ont pas joué leur rôle lorsqu'il fallait soutenir Nokia et Ericsson pour des raisons protectionnistes. Si chaque EM se replie sur ses frontières, ses enjeux nationaux, l'Europe des 27 ne sera plus qu'un terrain de jeu pour les grandes puissances qui diffuseraient leur influence non pas par la force ou le *softpower,* mais par le *political warfare*, en utilisant des techniques qui permettent de modéliser les adversaires et autres compétiteurs[12].

Le potentiel de renseignement sur la menace est considérable à travers l'Europe. Aussi, le partage d'informations entre les EM afin de mieux se défendre ne doit pas être une option. Refuser le partage et transformer la coopération en négociation au motif d'une souveraineté technologique nationale, qui en réalité n'existe plus depuis bien longtemps, présente le risque de transférer les informations, les données, vers un état tiers "sans le savoir", après que ce dernier aurait mis en place une politique de guerre du média social.

La diversité culturelle

Inutile de le rappeler, la diversité de l'UE est très souvent reconnue comme son point faible. Bien que partageant un espace géographique commun, le continent européen, les pays européens sont imprégnés d'une histoire, de valeurs et de cultures parfois totalement opposées qui les a souvent placés dans des camps qui s'affrontent : les gagnants et les perdants des deux Guerres Mondiales, les démocraties de l'Ouest et les états communistes à l'Est, des monarchies, des républiques et des états fédéraux, des politiques libérales ou, au contraire, nationalistes, avec des partenariats avec des puissances étrangères, souvent rivales économiques et systémiques, telles que les États-Unis et la Chine. Parler d'une seule voix est, en conséquence, une tâche presque impossible, même lorsqu'il s'agit du marché unique. Des malentendus, des incompréhensions, voire des discordes arrivent tous les jours.

La diversité linguistique de l'Union n'est pas non plus étrangère aux difficultés d'interprétation des directives au moment de leur transposition. Outre certaines erreurs qui se glissent parfois dans les traductions des directives publiées au Journal Officiel des Communautés Européennes (JOCE), il arrive que certaines versions linguistiques ne concordent pas. On comprend les problèmes que peuvent rencontrer des États comme la Belgique par exemple, susceptibles de se trouver confrontés à la transposition d'une directive dont les versions linguistiques francophone, néerlandophone et germanophone ne correspondraient pas. Par ailleurs, certains mots existant en anglais, langue de rédaction des textes officiels de l'UE, n'existent pas dans toutes les langues européennes. Par exemple, le français ne fait pas la distinction entre les anglais "confidence" and "trust". Par ailleurs, le vocabulaire propre à l'informatique et à la cybersécurité, étant d'origine anglaise, n'a pas toujours de correspondant dans les langues européennes. Les services du Cloud, en roumain, sont des "*servicii de Cloud*". Cela en devient presque risqué lorsque des pays souhaitant trouver un équivalent dans leur langue et des faux amis se fraient dans les traductions : le français "impact" pour l'anglais "impact", ou le français "fréquence" pour l'anglais "*probability*", notamment dans la gestion du risque. En 2022, seulement 12 des 27 EM ont une probabilité élevée d'atteindre les objectifs de l'UE à l'horizon 2025[13].

La multiplicité des langues au sein de l'UE fait que le niveau d'anglais est très variable (cf. carte ci-contre) dû à l'existence de plus de 27 langues source à partir desquelles l'anglais est appris. Plusieurs pays du

Dans les *Recommandations de la Commission** du 26 mars 2019 visant la cybersécurité des réseaux 5G, le conditionnel "*Member States should* " apparaît 47 fois en 8 pages. La rédaction de documents de la Commission en première intention en anglais, langue officielle d'aucun état membre après le Brexit, est une aberration car le verbe modal *should*** peut transmettre toute une palette de nuances :

- dire ou demander ce qui est correct ou ce qui est le mieux à faire [...]
- montrer quand quelque chose est probable ou attendu [...]
- faire référence à un événement possible dans le futur.

La valeur de *should* n'est donc pas d'obligation, de devoir, mais de recommandation des bonnes pratiques.

*CE. *Recommendations of 26.3.2019 - Cybersecurity of 5G networks*. . 26 mars 2019.

** *Cambridge Dictionary - Should*

Nord de l'Europe ont une très bonne maîtrise de l'anglais (les néerlandais sont les premiers dans le monde), alors que la France et l'Espagne ont une maîtrise moyenne[14]. Le rapport établit des corrélations directes entre le niveau de maîtrise de l'anglais l'économie et l'innovation[15].

Le niveau de maîtrise de l'anglais, la langue la plus utilisée lors des échanges entre les différents acteurs de la cybersécurité, peut représenter un risque. Lorsque le FIC est organisé en anglais, on ne s'étonnera pas du faible niveau de participation d'entreprises étrangères. En règle générale, les compétences linguistiques sont à l'image de la diversité européenne : très inégales. Les différences dans la culture, l'expression et la langue des membres d'une alliance sont très souvent source de risques, comme le confirme Général de division Philippe Delbos[16] :

« Très souvent les choses se heurtent au fit qu'on ne se comprend pas. Et on ne sait pas qu'on ne se comprend pas. C'est ça le problème. Souvent on pense que la nation partenaire bloque, alors qu'elle ne bloque pas sur l'objectif. Elle bloque sur la compréhension, sur l'idée qu'on a, qu'on se fait sur ce que veut l'autre.
[…] Ce n'est pas parce qu'on connait la langue qu'on comprend la pensée de nos partenaires. »

Accepter humblement que *« Je ne saurais jamais tout de l'autre et donc je sais que je ne sais pas »*[17], comme disait le Général, est le premier pas vers une intelligence interculturelle. La difficulté est d'autant plus sournoise qu'on ne se rend pas compte qu'on parle une langue mais on pense dans une autre.

Sur le plan opérationnel, aux risques liés au fait de parler chacun son anglais, s'ajoute des risques liés à la culture d'entreprise. L'acquisition de l'entreprise américano-française Alcatel-Lucent par Nokia a été perturbée par de tels risques : culture de travail, interprétations des objectifs, biais culturels, etc. Les Français n'hésitent pas d'ailleurs d'exprimer dans la presse leur désaccord. Un syndicaliste français chez Nokia parle d'un *« choc culturel »* depuis l'arrivée des Finlandais à la tête de l'ex-Alcatel[18] :

« Ils sont très durs, la culture Alcatel c'était celle d'inventeurs, mais eux, ce sont des donneurs d'ordre qui n'écoutent pas les gens. Résultat, il y a beaucoup de burn-out, de gens arrêtés, la greffe n'a pas du tout pris et ils ne comprennent pas la mentalité française. Même les jeunes ingénieurs qui rentrent ici ne restent pas longtemps, un an ou deux, ils font leurs armes et puis s'en vont. »

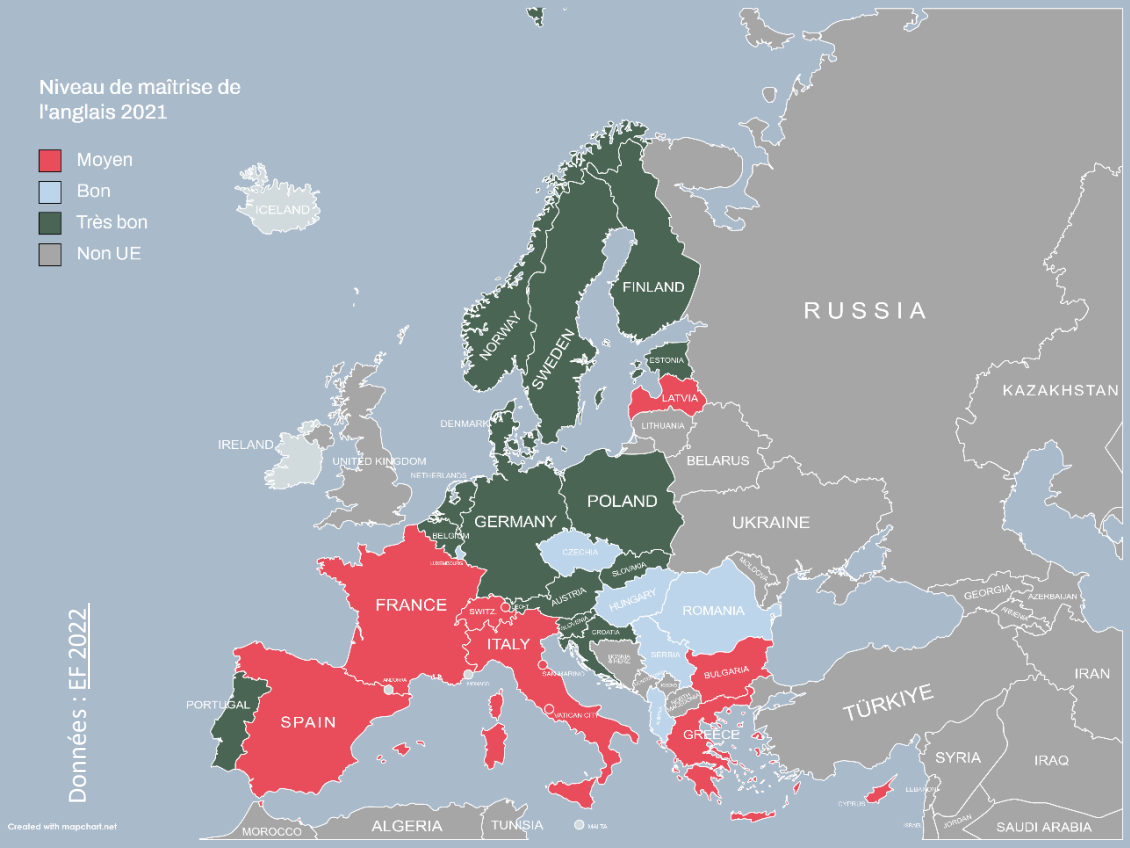
Nos entretiens[19] sur les différences et les ressemblances perçues vis-à-vis de professionnels français par des professionnels étrangers montrent un écart de perception importante entre le savoir-être et le savoir-faire des Européens, sans vouloir pour autant généraliser. Une professionnelle finlandaise nous confirmait un grand écart entre les deux cultures :

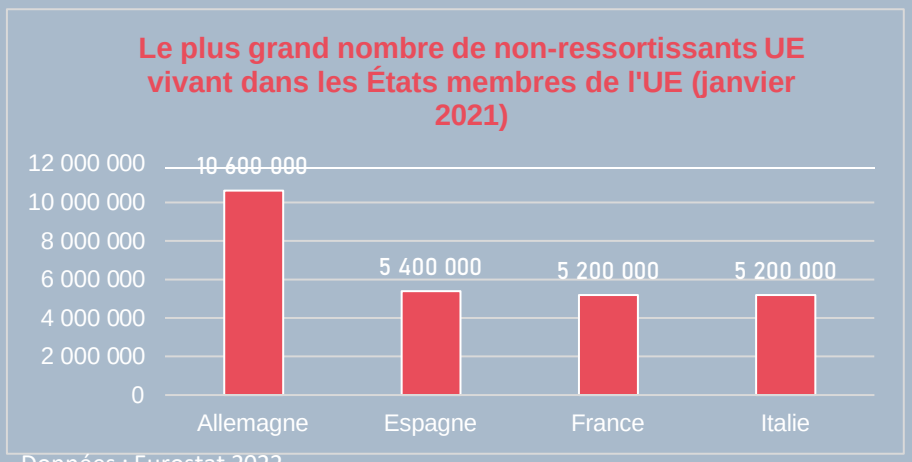
« Les Français sont très motivés par leurs vacances. Je ne pense pas que les Français aient le sens de l'humour. Ils sont trop sérieux. Les Français sont très narcissiques, individualistes. Ils ne pensent qu'à eux. Ils ne travaillent pas vraiment pour la communauté, pour le bien de tous. Je dirais aussi égocentriques. »

Les professionnels IT roumains apprécient le calme et l'organisation des Français, tout comme leur capacité à profiter de leur temps libre et des vacances qui sont généralement respectées. Le rapport au temps impacte également le travail en équipe. Déjà l'écrivaine française Germaine de Staël disait en parlant des Allemands[20] :

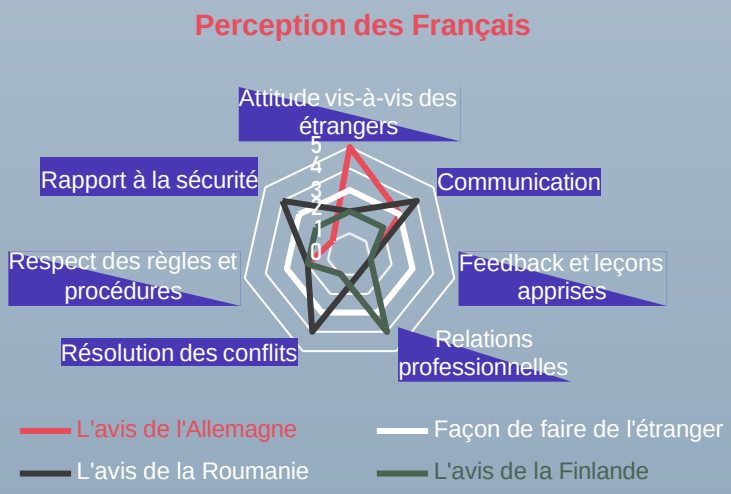
« Le talent des Allemands est de bien remplir leur temps, mais le talent des Français est d'oublier le temps. »

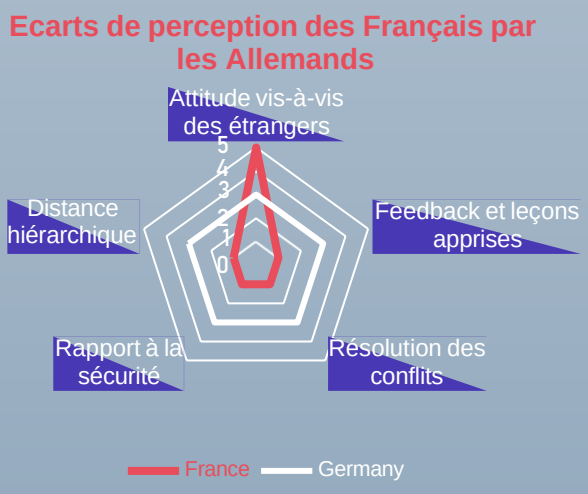
Effectivement, la façon de travailler entre Français et Allemands peut parfois être aux extrêmes. Sur 12 critères évalués, le professionnel allemand interrogé fait état de 7 critères où les Allemands seraient aux antipodes des Français (cf. ci-contre).





Données : Eurostat 2022





Est-ce que les Français auraient un passé centré sur une culture nationale unique ? La nation française s'est construite au détriment des langues et cultures régionales, en imposant une langue et une culture communes, au service d'une nation unie. L'édification d'une conscience nationale, garante de l'homogénéité de la nation, s'est faite au détriment de la diversité. L'école a été l'un des principaux instruments de cette unification ; les programmes et les manuels français restent muets sur des méthodes à exploiter la différence interculturelle des élèves[21]. Ailleurs, dans des pays plurilingues, la Belgique, la Suisse, la diversité, linguistique, culturelle, est la normalité. Au niveau de l'Union Européenne, une double interculturalité est à l'œuvre : d'un côté est visible une diversité interne (culturelle, linguistique, institutionnelle et politique) s'élargissant avec les récentes adhésions.

De l'autre, une diversité externe, issue de l'accueil de populations non-européennes influence directement la sensibilité interculturelle. En Europe, 70,3% des étrangers sont accueillis dans 4 pays[22] (cf. ci-contre). L'UE est confrontée à une interculturalité croissante et la gestion de la diversité culturelle diffère d'un pays à l'autre. La création d'une culture transeuropéenne est un objectif de l'UE et la pédagogie multiculturelle est mise en avant par des projets soutenus par exemple par l'Office Franco-Allemand pour la Jeunesse. À l'échelle du continent, ces initiatives sont anecdotiques car il est difficile de conjuguer diversité et unité, et d'infuser une identité qui soit perçue à la fois comme hybride et unique. Benjamin Boula[23] identifie des obstacles à ce projet :

- l'Europe se définit plutôt par l'exclusion que par l'inclusion au nom de l'égalité des chances,
- les systèmes éducatifs nationaux font résistance aux identités multiculturelles
- si elle devait soutenir un modèle européen éducatif, l'Europe partirait d'exemples déjà existants, nationaux, au lieu de concevoir un modèle unique en fonction des valeurs européennes et pas étatiques parce que cela risque de bouleverser le statu quo existant entre les États.

À travers ses méthodologies de structuration de la pensée, l'éducation participe considérablement à la construction d'un état d'esprit particulier. Entre une pensée généraliste, globale, et une pensée pratique, spécifique, l'éventail de nuances est visible même à l'échelle de l'entreprise. Entre une approche individualiste et une approche collective, l'Europe penche plutôt vers l'individualisme, avec de nombreuses variations cependant. Cela est visible au niveau des échanges avec les institutions européennes. La Cour des Comptes Européenne souligne un manque d'efficacité global des acteurs de la cybersécurité. Le principal défi consiste à faire naître le réflexe de rendre compte et de s'évaluer selon des critères standardisés de façon rigoureuse, en passant par l'adoption d'une culture de la performance. Dès son arrivée au NCSC en 2016 en tant que Directeur Technique, Ian Levy a exigé une gouvernance de la cybersécurité fondée sur des indicateurs mesurables et une approche scientifique et transparente[24]. Encore aujourd'hui, à l'ère de la donnée, certaines cultures peinent à rendre compte de manière factuelle et transparente. La maîtrise de l'anglais en est une cause[25], mais certainement pas la seule.

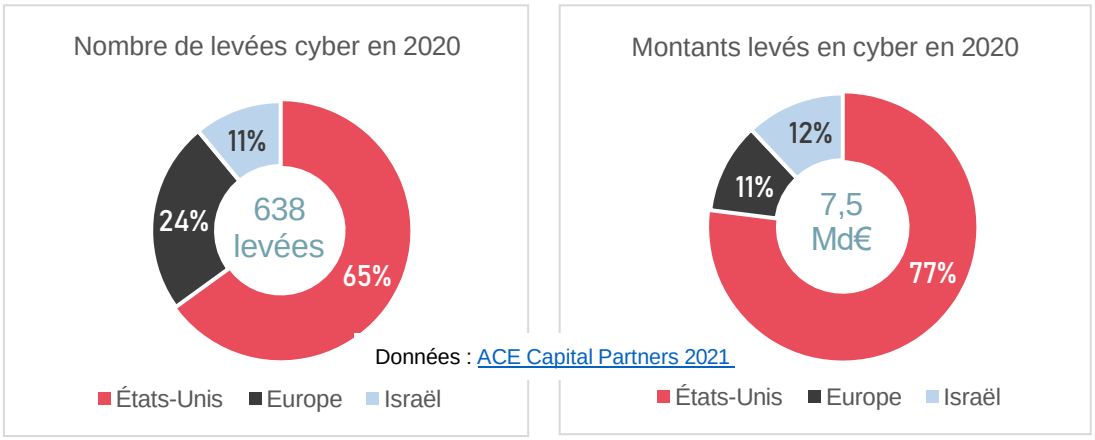
La concurrence, l'ennemi de la coopération

La question centrale de la compétition concerne la prévalence des objectifs privés par rapport aux objectifs communs entre les concurrents la poursuite d'intérêts mutuels et de bénéfices communs dans des alliances. Or la politique économique et industrielle européenne encourage la logique de concurrence de marché, Avec des objectifs privés prioritaires focalisés sur les profits, les entreprises privées ne collaborent que rarement., comme nous l'avons vu avec les partisans de l'Open RAN. Lorsque les grands opérateurs télécom coopèrent afin d'éviter l'interdiction de Huawei, les équipementiers européens sont les premiers à devoir en gérer les conséquences, avant même de parler de quelconque gestion des risques.

Du point de vue européen, la logique de concurrence au sein d'un marché réglementé offre à toutes les entreprises la chance de réussir. Plutôt que de faire converger des "champions" pour n'en faire qu'un, l'Europe assume pencher pour une multitude d'acteurs de taille plus modeste afin d'offrir une pluralité de choix aux consommateurs. L'UE a d'ailleurs, à travers le *Digital Markets Act*, renforcé cette position, notamment vis-à-vis des GAFAM. Il est donc légitime, au regard de cette situation, de s'interroger sur la volonté de faire naitre des "licornes européennes" dans la cybersécurité. Nous allons observer les résultats du baromètre de l'investissement européen en cybersécurité publié par *Ace Capital Partner*[26].

La capacité d'attirer les investisseurs dans l'industrie cyber européenne est flagrant et tout aussi inquiétant.

En 2020, les États-Unis poursuivent largement leur domination en nombre et en montant total des fonds levés en cybersécurité. Ils représentent à eux-seuls 65% des 638 opérations enregistrées et 77% des 7,5 milliards de dollars levés. Environ deux fois plus d'opérations ont été réalisées en Europe par rapport à Israël, en revanche, le montant total levé est comparable dans les deux régions avec un chiffre proche du milliard d'euros (respectivement 926 millions d'euros en Israël soit 12% et 811 millions d'euros en Europe soit 11%). Pour rappel, l'Europe, c'est plus de 746 millions d'individus ; Israël, c'est plus de 9M d'individus, soit un pays 83 fois moins peuplé qui lève autant de capitaux que l'ensemble des pays européens. De surcroît, par rapport à 2019, le montant des levées de fond a progressé de 2 milliards de dollars en moyenne pour les États-Unis et l'Israël, alors qu'il a diminué en Europe, on enregistre une baisse des investissements de plus d'un milliard d'euros[27]. Aujourd'hui, fort est de constater que l'Europe n'a pas réussi à se doter de géants du numérique, capables de rivaliser avec les géants états-uniens ou chinois.



Données : ACE Capital Partners 2021

La logique de libre concurrence au sein de l'Union Européenne ne permet pas de faire émerger un géant du numérique capable de se confronter aux entreprises états-uniennes. Il en résulte une difficulté certaine à faire naitre des licornes, comme le font par ailleurs très bien les Israéliens. En conséquence, en 2020, huit nouvelles sociétés de cybersécurité ont atteint le niveau de licorne, dont 6 états-uniennes, deux israéliennes et une seule européenne. Le protectionnisme stratégique est difficilement envisageable car il se ferait au détriment d'accords multilatéraux dans d'autres domaines pour compenser. Des opportunités auraient pourtant pu être saisies, notamment avec le 5G, et les

2020

8 licornes États-Unis

2 licornes Israël

1 licorne Irlande

Source : ACE Capital Partners, 2021.

équipementiers européens Nokia, ou Ericsson, ou le projet Cloud Gaia-X. Comme dit précédemment, celui-ci n'a pas su répondre pas suffisamment aux enjeux de confiance du *Cloud computing* pour espérer confédérer les professionnels européens.

En matière de cybersécurité, l'Europe a choisi de développer un tissu industriel de confiance, en s'appuyant sur des outils de certification de services et de produits, incluant la concurrence internationale, sans logique protectionniste. C'est un parti pris qui n'est pas compatible avec la coopération et qui se montre défaillant face aux enjeux stratégiques d'aujourd'hui. C'est aussi un investissement humain et financier, se faisant forcément au détriment d'autres alternatives. Il semble cependant assez clair que l'investissement européen n'est pas du tout à la hauteur de l'enjeu, ce manque d'investissement se faisant bien ressentir à travers le manque d'innovations technologiques. Plus la concurrence est rude, moins il peut y avoir de coopération. Les États-Uniens et les Israéliens l'ont bien compris : des investissements massifs dans l'industrie et la R&D font d'eux les leaders du secteur cyber. Dans ce contexte, il est très difficile d'imaginer comment l'Europe pourrait rattraper son retard dans l'industrie et l'innovation numérique.

La confiance, le liant de la cybersécurité

Vis-à-vis des systèmes d'information, la confiance serait la certitude que les données des utilisateurs soient traitées et utilisées selon leurs souhaits. Cela paraît simple, mais en réalité la confiance est une notion abstraite, subjective, et surtout multidimensionnelle.

Tout d'abord, il y a la confiance entre les acteurs européens de la cybersécurité. En dépit des progrès réalisés ces dernières années, les niveaux de confiance restent insuffisants selon *The Directorate-General for Communications Networks, Content and Technology*[28], tant au niveau de l'UE qu'au sein de certains États membres. L'un des objectifs de la *Stratégie de cybersécurité* EU-CSS, et des structures de coopération instituées par la *Directive NIS*, est de renforcer la confiance entre les parties prenantes, comme présenté dans le deuxième chapitre. Dans l'évaluation de la stratégie, les services de la Commission reconnaissent que les bases d'une coopération stratégique et opérationnelle au niveau de l'UE ont été jetées. Malgré cela, ils estiment que la coordination est, d'une manière générale, insuffisante[29] :

> *Il faudra améliorer la coordination et la coopération en matière de communication stratégique entre l'ensemble des institutions de l'UE, les États membres et les partenaires et organisations internationales.*

Multiplier les mécanismes de coopération découple également les échanges entre les représentants de l'UE, les autorités nationales et le secteur privé : plus de 24 groupes de travail et instances préparatoires traitent de thèmes liés au cyberespace. En l'absence d'une confiance absolue, l'efficacité n'est pas toujours en rendez-vous.

Ensuite il y a la confiance dans le fournisseur du matériel ou des services numériques par lesquels transitent les données des Européens : états, entreprises et citoyens. Par le passé, les États-Unis ont exploité, voire créé des vulnérabilités dans des solutions ; en théorie, d'autres pouvaient (ou peuvent) le faire aussi car les mêmes terminaux, protocoles et connexions sont utilisés à travers le monde afin d'assurer l'interopérabilité des réseaux. Par conséquent, l'évaluation de la sécurité d'un système d'information sera partielle si celle-ci se propose d'évaluer uniquement le niveau de sécurité intrinsèque à la technologie (qualité du code source, déploiement, configuration). La confiance dans le pays d'origine de la technologie y joue un rôle tout aussi essentiel. Celle-ci est à évaluer de manière très sérieuse.

C'est justement ce qui a manqué en Europe lors du déploiement de la 5G et qui pénalise, encore aujourd'hui, certains opérateurs (Bouygues et SFR en France). La 5G transportera une grande partie des données mondiales d'ici une dizaine d'années. Le compromis quant à sa sécurité n'était pas envisageable, comme l'explique Danielle Cave d'Australian Strategic Policy Institute[30] :

> *If you are bringing a company into your 5G network which is a critical piece of national infrastructure and other national infrastructure is going to sit on top of that 5G network, you need to be able to trust that company and they need to be very transparent. The problem with Huawei is we don't*

have that. […] When it comes to 5G network, you need to worry about security more than cost. And if the equipment is really cheap, that doesn't matter if you can't assure security.

Robert Hannigan, ancien Directeur de la communication du Gouvernement britannique le confirme également[31] :

The challenge for those who simply want to ban [Huawei], is what's the alternative.
The challenge for those who think they can manage it; the challenge is are you kidding yourselves?

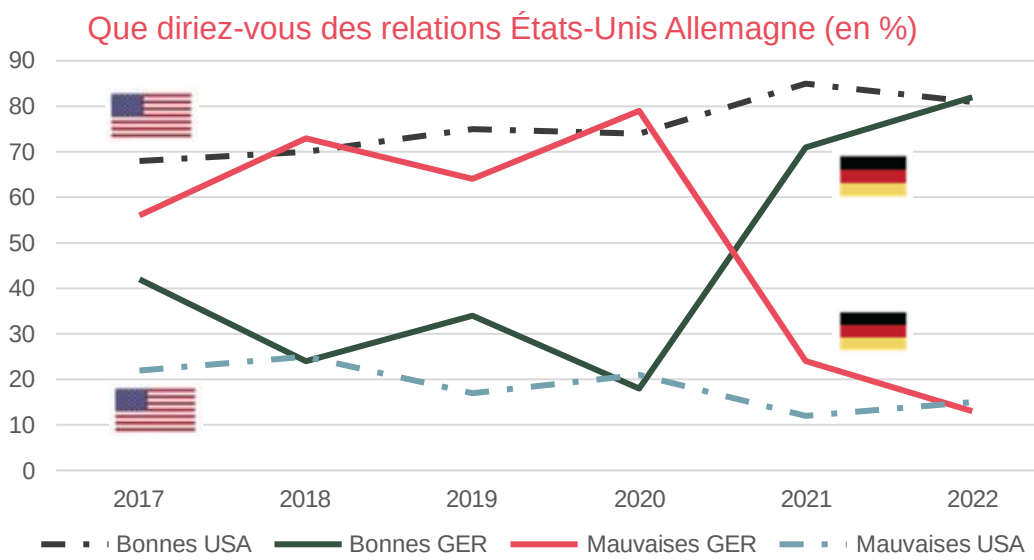
Anne Tricaud de l'ANSSI, partage le même avis :

On peut décortiquer le matériel, on peut aller très loin dans l'analyse. On va découvrir des failles, très bien. Mais la backdoor, il faut être réaliste.

La cohérence entre ce que l'Europe dit et ce que l'Europe fait, reflète la difficulté d'arbitrage entre intérêts économiques et souveraineté technologique. Plusieurs faits récents interpellent et polluent la communication de l'UE : l'occasion loupée de reprendre le leadership de la 5G en soutenant Nokia ou Ericsson, idéalement les deux, la réouverture des négociations sur le transfert des données personnelles aux États-Unis, les nombreux échanges "confidentiels" de plusieurs hauts représentants des institutions européennes et le contrat d'Europol avec Palentir[32] qui court depuis 2016. Cela est d'autant plus grave que la Présidente de la Commission, Ursula von der Leyen, faisait de la transparence une priorité de son mandat[33] :

If Europeans are to have faith in our Union, its institutions should be open and beyond reproach on ethics, transparency and integrity.

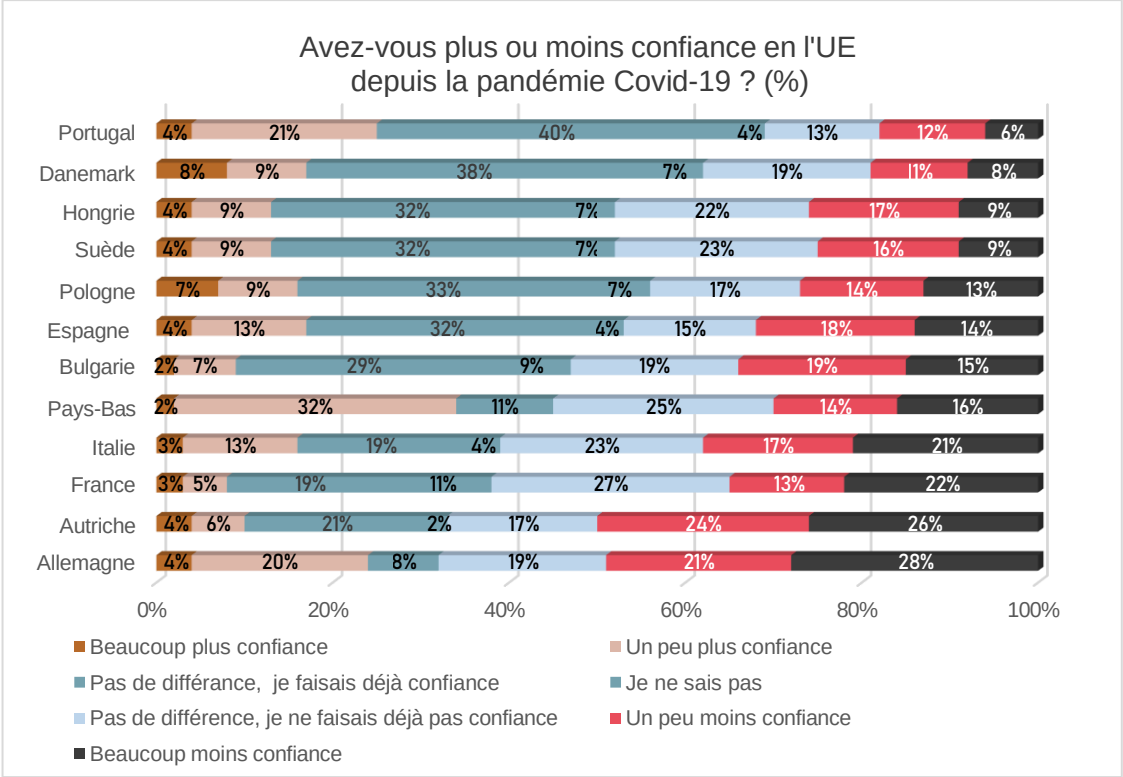
La vérité est que la pandémie a érodé la confiance des Européens dans les institutions européennes, avec des pays comme la France, l'Allemagne et l'Italie où le manque de confiance est majoritaire[34]. Quant à la confiance des utilisateurs dans les administrations nationales et celles des partenaires, celle-ci est plus volatile que jamais. Ainsi, en 2019 les Allemands avaient plus confiance dans les relations de leur pays avec la Chine qu'avec les États-Unis[35], se prononçant en faveur des Chinois contre 23,1% seulement en faveur du pays gouverné par Trump. Trois ans plus tard, plus de 80% des Allemands évaluent les mêmes relations de positives[36].



Données : Pew Research Centre 2002

Note : Les personnes qui n'ont pas répondu ne sont pas indiquées. Avant 2022, les enquêtes aux Etats-Unis étaient menées par téléphone.
par téléphone. Les résultats allemands sont tous issus d'enquêtes téléphoniques.
Source : Sondage du Pew Research Center réalisé aux États-Unis du 1er au 14 août 2022. Q6.
Allemagne: résultats du sondage Körber-Stiftung réalisé du 2 au 11 août 2022.

La question de la confiance des Européens dans l'Europe doit également être posée. La pandémie et le conflit en Ukraine viennent d'ébranler les convictions des citoyens européens et leur confiance. La France et l'Allemagne, les deux pays vers lesquels les regards des EM se tournent, fers de lance de la technologie mais aussi de la diplomatie européenne, sont pourtant partie des États les plus réticents à avoir confiants dans les institutions EU. Ensemble à l'Autriche, 62% d'interrogés affirment ne pas avoir confiance dans l'UE.



62%

des Français et des Allemands n'ont pas, ou ont moins, confiance dans l'UE.

Données : ECFR

De surcroît, le manque de confiance semble se généraliser et est de plus en plus visible dans le rapport des Européens avec leurs propres gouvernants également. Selon les récentes prévisions de Forbes, seulement un Européen sur 5 aura confiance dans son gouvernement d'ici fin 2023[37].

Au sein des acteurs privés, industriels, opérateurs, équipementiers, la confiance est fortement perturbée par la concurrence. Alors que la sécurité est la raison la plus citée d'un virage vers la 5G, les offres et les réseaux sont voués à un morcellement néfaste aux opérateurs, chargés d'interconnecter des configurations d'origines variées. Bien que convaincues des mérites de la 5G, les industriels doutent de la volonté et de la capacité des opérateurs de télécommunications de répondre aux exigences de leur secteur en matière de sécurité, de disponibilité du réseau et qualité de service. Un dirigeant, responsable de l'infrastructure télécom d'un grand groupe industriel allemand déclare[6] :

« Les opérateurs télécoms ne savent pas comment exploiter une infrastructure critique. Ils traitent les pannes de réseau avec une approche statistique. Un changement culturel majeur est nécessaire. »

Bien que l'anticipation de la 5G soit forte parmi certaines industries, les fonctionnalités prendront du temps à émerger. Alors que certaines entreprises veulent adopter la 5G dans les deux ans, les opérateurs télécoms estiment qu'il faudra au moins cinq ans pour l'adoption à grande échelle de fonctions telles que la qualité de service garantie ou le découpage du réseau. Entre opérateurs et industriels la communication ne passe pas, chacun ne voyant que son propre intérêt. Les réactions de méfiance quant à l'efficacité des opérateurs télécom en sont la preuve. L'engouement, principalement en Allemagne, pour les licences privées 5G trahit ce manque de confiance car le besoin de s'assurer une plus grande autonomie et sécurité est plus important que les coûts. De plus, cela n'est pas limité à l'Allemagne. Selon un sondage de Capgemini de 2019[38], un tiers des entreprises européennes seraient intéressées par une licence privée, bien qu'il existe des obstacles réglementaires.

Comme présenté précédemment, le projet pour un cloud européen Gaia-X a été considérablement perturbé par le manque de confiance et de transparence. La présence des GAFAM et des Chinois n'a pas été acceptée par tous les membres, comme l'affirme le PDG de Scaleway[39] :

> *The big players, they do what they do. First, they knock on the door, then they take a step in the door ... Very quickly it became clear that these guys were dominant in the technical groups.*


FROM POLITICO PRO

Inside Gaia-X: How chaos and infighting are killing Europe's grand cloud project

The initiative, meant to boost Europe's cloud services, is failing to fix the problems it was intended to solve.

Entre les jeux des coulisses des Français, la dominance technique des États-uniens et le manque de clarté des objectifs, le projet est en retard par rapport à l'urgence critique de l'Europe de grader le contrôle sur la donnée européenne. En absence d'un objectif clair, la coopération s'est transformée en chaos, chaque entreprise soutenant son propre objectif.

Toutefois, si les lois devaient être insérées dans des normes techniques, comme le veut la Chine, cela pourrait offrir un objectif commun au nom duquel équipementiers, opérateurs et industriels pourraient coopérer. Cela pourrait permettre une certaine autonomie, à condition que l'UE s'implique davantage dans la création de normes techniques pour les technologies numériques, ainsi que dans l'organisation de chaînes d'approvisionnement stratégiques et dans la fourniture d'infrastructures numériques essentielles. C'est ce que le PDG d'Ericsson demandait en 2019 pour la 5G. C'est ce que l'Europe a commencé à faire avec les semiconducteurs. Mais la 6G, le chiffrement post-quantique, les IoT le nécessitent aussi. Est-ce que les EM sont prêts à accepter que l'Europe s'immisce dans leurs économies ? Rien n'est moins sûr, car il y en a 27 à convaincre, les uns les plus différents des autres, et l'Europe devra tout d'abord composer avec cette diversité.

L'Allemagne et la France ont su, au temps de Jules César, passer du statut de nations en guerre à celui de "moteurs jumeaux" d'une Europe unifiée qui serait, selon l'écrivain français Jean Misler, *« presque complète si les Français restaient une heure de moins au bistrot et les Allemands une heure de plus au lit. »*[40] Aujourd'hui, quand être connecté peut-être aussi vital qu'avoir de l'électricité, il est temps de faire fructifier ces différences. Il est nécessaire que la diversité européenne devienne un atout qu'aucun autre pays au monde ne pourrait avoir. Comme pour de nombreuses autres initiatives européennes majeures dans le passé (Airbus), il faudra le leadership combiné de la France et de l'Allemagne pour permettre à l'Europe de faire la différence.

4.2. Les incohérences

Un usage naïf du lobbying

Un autre levier d'action pour l'Europe serait la structuration de l'influence des think-tanks, des lobby européens tant sur nos territoires qu'en dehors de nos frontières. Ces organisations et associations spécifiques sont des outils d'influence, des capteurs d'information et des centres de réflexion majeures que les États-Unis maîtrisent parfaitement. Ils ont déjà largement fait leurs preuves depuis des décennies. [41] Ne pas se mouvoir de notre influence européenne mais actionner ce levier serait une opportunité pour consolider l'écosystème cyber européen, donc la protection de ces acteurs ainsi que nos intérêts. En parallèle de l'élaboration d'outils, de lois, et de directives, il faut forger un état d'esprit européen capable, par sa diplomatie, par la voie de Think thanks, et autres structures d'influence européennes, de défendre ces intérêts, notamment en matière de cybersécurité, à la fois défensive et offensive.

L'actualité démontre que l'Europe éprouve de grandes difficultés à suivre les mêmes objectifs car les États se divisent et manœuvrent, bien trop souvent, individuellement. Le Royaume-Uni a quitté l'UE et connait une instabilité politique et économique peu enviable. La France et l'Allemagne sont en désaccord quasi permanent sur les sujets et enjeux de défense, d'énergie, de dépendance économique, etc. L'Allemagne, malgré son statut d'état historiquement influant, joue la priorité nationale au détriment du projet Européen. Enfin, les Italiens ont élu Giorgia Meloni du parti *Fratelli d'Italia*, mettant à la tête du pays un parti politique prônant la souveraineté nationale, toutefois rassurante auprès des représentants européens[42].

Ces exemples proviennent tous des pays fondateurs de l'UE. Ils démontrent les choix stratégiques pris par les différents gouvernements afin de préserver leurs intérêts à court terme. Cela fait apparaître, entre les lignes des médias, une défiance envers les partenaires européens et les réglementations européennes. Comment se fait-il que l'Autriche et la Belgique n'ont pas implémenté la *Directive NIS* dans les délais ? Quelle est la raison de l'abstention de la Croatie lors du vote du *Cybersecurity Act* ? Pourquoi la Finlande est le seul pays à jour avec le déploiement de la 5G ?

Vue le nombre important de retardataires ou contestataires, il est clair que les priorités de certains États ne sont pas alignées à celles de l'Union Européenne. Tant que la cybersécurité européenne sera à plusieurs vitesses, la coordination sera d'autant plus ralentie et profitera davantage aux concurrents non-européens.

À cette difficulté s'ajoute le *soft power* auprès de la Commission Européenne exercé par les puissances étrangères, les associations, les think-tanks, et les entreprises privées. Leur puissance financière, et leur visibilité auprès de la Commission surpassent de loin celles des organisations européennes.

Les limites de l'"effet Bruxelles"

Ces quinze dernières années, les textes régulant l'écosystème numérique se sont multipliés, et une nette accélération est perceptible depuis ces cinq dernières années. Néanmoins, aujourd'hui, l'Europe est en retard du point de vue technologique, et elle semble s'en rendre réellement compte. Elle essaie donc de mettre de l'ordre dans un Internet devenu un vrai *far West* en imposant des règles ; c'est d'ailleurs ce qu'elle sait faire de mieux. Ainsi, l'effort produit par la Commission européenne pour créer des règles pour chaque élément de la pile technologique mérite d'être reconnu et salué. Et lorsque la réglementation européenne est adoptée par d'autres pays, le succès est au rendez-vous. C'est ce que le professeur américain Anu Bradford a appelé en 2012 "l'effet Bruxelles".

Si nombre des décideurs politiques s'en réjouissent, la littérature académique a été moins impressionnée par ce phénomène, car celui-ci n'est pas sans fin. Selon Chad Damro [43] , chercheur à l'Université d'Edinburgh, définir un tel carcan de règles en montrant l'exemple à d'autres pays pourrait faire de l'UE une superpuissance réglementaire mondiale.

EU Transparency Register data as of: 01 Jan 2021. A total of 1284 results.

Source : UE 2021

#	Name	Head office in	lobbycosts	EP passes	Lobbyists (FTE)	Meetings with EC
1	Google	UNITED STATES	5,875,000€	2	5.5	291
2	Microsoft Corporation	UNITED STATES	5,375,000€	2	7.5	176
3	Shell Companies	NETHERLANDS	4,624,500€	1	10.5	97
4	Facebook Ireland Limited	IRELAND	4,375,000€	4	13.75	177
5	Bayer AG	GERMANY	4,295,000€	6	13.25	44
6	ExxonMobil Petroleum & Chemical	BELGIUM	3,375,000€	4	5	42
7	Huawei Technologies	CHINA	3,125,000€	2	19	70
8	Siemens AG	GERMANY	3,125,000€	1	11.25	68
9	Volkswagen Aktiengesellschaft	GERMANY	3,125,000€	2	19.25	79
10	BASF SE	GERMANY	3,100,000€	10	10.75	38

Investissements en lobby

Au regard de ces chiffres, il apparait très clairement que les intérêts technologiques européens ne bénéficient pas d'investissements suffisants dans l'activité de lobbying auprès des instances européennes, alors qu'en ce qui concerne les Etats-Unis (Apple, Google, Microsoft, Intel, IBM, The Center of Cybersecurity, Policy and law, etc.) et la Chine (Huawei, Hangzhou Hikvision Digital Technology, Lenovo, etc.), les montants dépassent les dizaines de millions d'euros. L'Allemagne est présente principalement sur ces sujets stratégiques nationaux. La France est très nettement sous-représentée en comparaison avec les Etats-Unis et le Royaume-Uni, avec seulement quelques millions, tous secteurs confondus, l'enjeu numérique étant le nerf de la guerre cyber.

Mais cela ne tiendrait à long terme que dans une situation de concurrence réglementaire, où les pays se font concurrence en définissant unilatéralement des règles, plutôt que dans un cadre de coopération où l'on définirait des règles mondiales ou internationales.

Dans ce contexte concurrentiel et non coopératif, les pays peuvent compter sur la puissance de leur économie, un facteur qui a traditionnellement joué en faveur de l'UE, qui reste d'ailleurs le marché intégré le plus riche du monde. Toutefois, ce facteur est susceptible de devenir moins influent au fil du temps, car le poids de l'UE dans l'économie mondiale devrait se réduire progressivement. En réalité, les règles se diffusent non seulement par concurrence réglementaire, mais aussi à travers des normes internationales et une coopération réglementaire. Et sur ce point, l'UE semble moins performante (cf. la normalisation de la 5G dans le Chapitre 2).

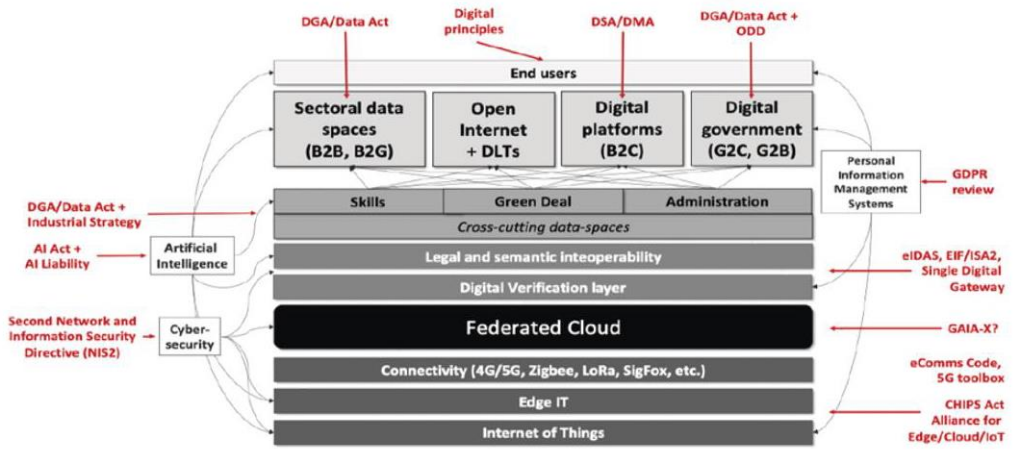
L'incompatibilité industrielle entre le *RGPD* et le développement de certaines applications d'IA ou certaines recherches dans le domaine de la santé est préjudiciable à l'Europe, selon la recherche académique européenne en la matière[44] :

> *It has become apparent that the implementation of GDPR restrictions has created new impediment for academic researchers, health-care professionals and others in the public sector. This problem affects patients and citizens, who are the ultimate beneficiaries of health research.*

Faire des lois pour faire des lois s'avère souvent inefficaces. Mais faire une réglementation pour contraindre les entreprises et protéger les citoyens européens pourrait être louable… Cependant, lorsque cette loi oblige les entreprises européennes à s'exiler hors de l'UE pour pouvoir continuer leurs activités, le manque de cohérence est criant. Or la cohérence est une condition préalable essentielle pour renforcer l'influence de l'UE sur la scène mondiale.

Aujourd'hui, l'UE a prévu un texte législatif pour réguler chaque couche des systèmes opérationnels, comme présenté ci-dessous[45].

Figure 1: Europe's technology stack and (in red) emerging/upcoming regulatory measures for each layer



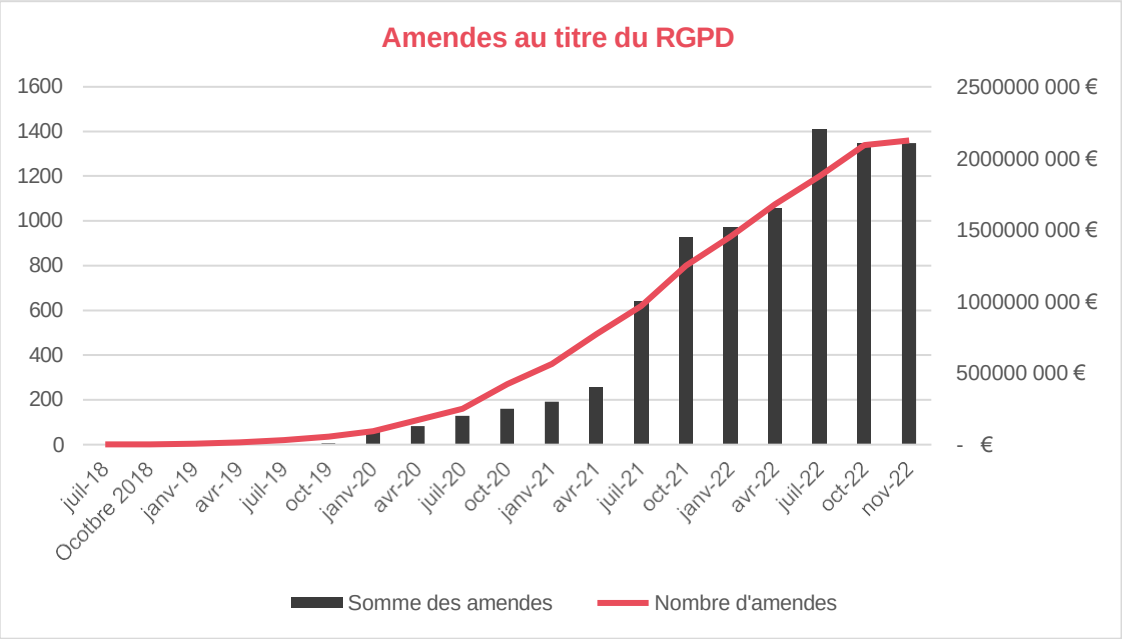
Source: Author's elaboration, based on Renda (2020)

La réglementation, cette "voie de la loi" choisie par l'Europe, se révèle donc insuffisante car les batailles contre les GAFAM ne sont pas réglementaires, ce sont de féroces batailles économiques. L'"effet Bruxelles" reste une stratégie viable tant que l'UE peut prétendre de manière crédible à avoir l'avantage d'être le premier. Mais nous avons démontré que, vis-à-vis de l'autonomie stratégique, l'UE n'est pas l'acteur le plus influent.

De plus, cette voie est aussi polluée par un manque de cohérence. Lorsque presque tous les jours en Europe, des données personnelles finissent entre les mains de criminels, l'efficacité du *RGPD*[46] côté Europe est moins certaine, bien qu'il soit mondialement reconnu et activement copié l'étranger[47]. Le

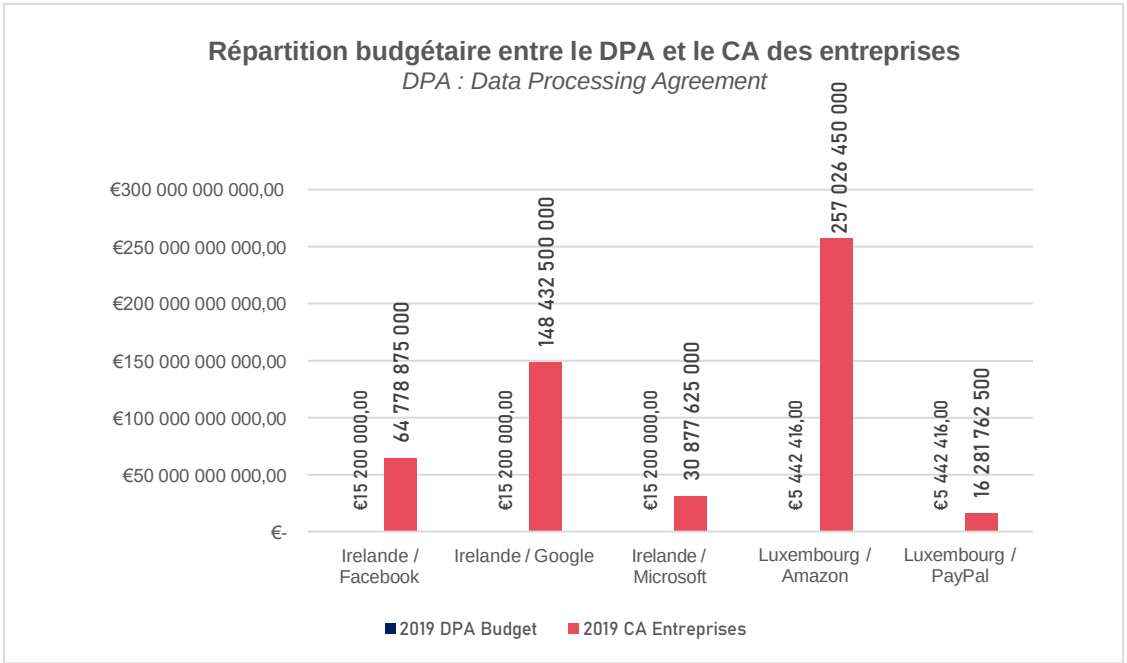
rapport de 2021 d'*Access Now*[48] met en lumière une grande hétérogénéité dans les niveaux d'application au sein de l'UE des 27 : faible proportionnalité des amendes et des montants, difficulté de coopération transfrontalière, impuissance de l'autorité irlandaise face aux géants du numérique, conflits avec les procédures judiciaires nationales, etc.

Et c'est bien logique. Le rôle même du *RGPD* conçu afin de limiter l'utilisation des données personnelles et leur finalité, est incohérent par rapport aux incitations économiques et aux principes de conception des entreprises qui contrôlent l'infrastructure et qui se concentrent sur la collecte, la combinaison et le stockage d'autant de données personnelles que possible, à des fins commerciales. Tout cela pourrait justifier aussi son application fragmentée et la non-conformité généralisée des systèmes.



Données GDPR Enforcement Tracker au 24 2021

Le rapport entre le coût d'implémentation du règlement et le chiffre d'affaires reste nettement en faveur du second. Autrement dit, ces coûts sont parfaitement supportables pour les GAFAM. En revanche ils le sont nettement moins pour la grande majorité des entreprises qui, en Europe, sont des PME.



Données GDPR Enforcement Tracker au 24 2021

Une sécurité numérique sacrifiée au profit d'intérêts économiques

Aujourd'hui, le récit européen est porté sur la nécessité d'une plus grande autonomie stratégique et de davantage de résilience. Tous les secteurs clés sont concernés, l'énergie, l'industrie, le numérique, la défense, la santé, l'agro-alimentaire, pour ne citer qu'eux. Déjà en 2019, l'ENISA rappelait que l'UE est la macro-région avec l'économie la plus digitalisée au monde : *Sailfish, Skype, F-Secure, AVG, Signal, Nokia, Ericsson, Alcatel* en sont les témoins. Cependant, ces vingt dernières années, l'industrie informatique européenne est prise dans l'étau sino-américain. Elle peine à tenir le pas des évolutions technologiques et n'arrive plus à innover : elle perd ainsi, petit à petit, son autonomie numérique acceptant des dépendances dont il sera très difficile de s'en libérer (Microsoft).

Malheureusement, ce récit est souvent affaibli par des décisions qui vont à son encontre. À titre d'exemple, on a vu l'Europe, à travers la présidente de la commission européenne Ursula Van Der Leyen, négocier avec les États-Unis[49], à la même occasion, un partenariat énergétique et l'abandon de certaines exigences européennes sur les données personnelles (l'avenir nous dira si cette négociation aura bien lieu dans ce sens). Dans l'éventualité où l'export des données personnelles des Européens sera effectivement autorisé vers les États-Unis, le récit européen perdra de sa légitimité : si la priorité est donnée aux ressources plutôt qu'à la protection des données, le message d'autonomie en sortira affaibli, le *RGPD* également et tout comme la légitimité de l'UE à exiger une autonomie stratégique. Par ailleurs, cette négociation ne fera que déplacer une dépendance d'Est (le gaz russe) à l'Ouest (le GNL états-unien).

Quand on rajoute à cela l'approche des États-Unis économique de la donnée numérique, il est clair qu'il y a deux approches. La première, un récit dans lequel les actent suivent aux paroles, celui des États-Unis : développer les intérêts énergétiques de l'Europe, et obtenir l'hégémonie sur la donnée numérique. La deuxième approche, un récit qui se contredit, celui de l'UE, qui continue à négliger ses ambitions d'autonomie stratégique, au profit de négociations commerciales discutables, et s'affaiblit de fait, par des actes incohérents, contradictoires, et donc difficiles à défendre.

L'Europe a pourtant les moyens de construire un nouveau récit, bien que son histoire et sa diversité soient souvent considérées comme des faiblesses, nourrissant une certaine forme de fatalité. Néanmoins, il est encore temps d'inverser cette tendance, le récit peut prendre à contre-pieds ces faiblesses, et les adapter à un contexte, pour finalement faire naître un récit évocateur, pertinent et fédérateur pour les EM. Cela pourrait faciliter la convergence des politiques de ces pays dans une trajectoire qui s'identifie à la stratégie européenne de cybersécurité. La cohérence, la coopération, le partage d'expérience et d'information sont des éléments décisifs dans la cybersécurité ; l'Europe doit donc absolument construire ce nouveau récit qui permettra de trouver le juste équilibre de cette nécessaire coopération, devenue aujourd'hui critique, afin que l'Europe ne devienne pas le point faible de sa propre stratégie de sécurité numérique. C'est en parlant d'une seule voix que l'Europe se fera entendre à la table des puissances mondiales.

Une cybersécurité trop souvent facultative

L'évaluation et l'atténuation continues des risques, un personnel de sécurité informatique expérimenté, des routines de maintenance des réseaux et la reprise d'activité après incident… tous ces éléments ont un impact sur la sécurité "réelle" des systèmes d'informations européens. Aujourd'hui, les systèmes sont de plus en plus complexes[50]. Or, la complexité est l'ennemi de la sécurité, comme l'anticipait Börje Ekholm, le CEO d'Ericsson[51] :

> *Compte tenu de la complexité de la future architecture, et des futurs réseaux, la sécurité dans la 5G ne dépendra pas seulement des équipements dans les réseaux. Elle dépendra également des solutions de sécurité déployées, et des paramètres d'exploitation du réseau - essentiellement des décisions que l'opérateur prendra. […] La question de la sécurité est une question globale et elle va être importante. En fin de compte, nous pensons que les opérateurs feront des choix pour le type de clients qu'ils serviront et le type de réseau et d'opérations qu'ils auront, et cela déterminera l'aspect de la sécurité.*

Pourtant, la complexité ne doit pas être une excuse pour recourir à grande échelle à une sécurisation plus importante. Cette sécurisation passe par une forme de volontariat, et la motivation sur laquelle cela

repose est l'une des raisons d'implémentations disparates des solutions de 5G par exemple. Au niveau mondial, la norme 3GPP inclut 9 spécifications de sécurité pour les réseaux 5G. Il est essentiel de souligner que TOUTES les caractéristiques et fonctions des spécifications de sécurité 3GPP doivent être prises en charge par les équipementiers, mais qu'elles sont TOUTES FACULTATIVES pour les fournisseurs de services 5G. Cela a conduit à des mises en œuvre incohérentes de la sécurité dans les réseaux 5G déployés et planifiés. En 2020 *Heavy Reading* a posé la question à plus d'une centaine de professionnels sur quels contrôles ils envisageaient de mettre en place et à quel moment[52].

	Implement most or all before commercial launch	Implement some part before commercial launch	Implement most or all after commercial launch	Implement some part after commercial launch	Depends on vendor compliance
3GPP TS 33.511 – Security Assurance Specification (SCAS) for the Next Generation Node B (gNodeB) Network Product Class	38%	33%	14%	3%	12%
GSMA FS.36 – 5G Interconnect Security	26%	34%	19%	7%	14%
3GPP TS 33.512 5G Security Assurance Specification (SCAS) – Access and Mobility Management Function (AMF)	26%	39%	15%	7%	13%
3GPP TS 33.513 – 5G Security Assurance Specification (SCAS) – User Plane Function (UPF)	23%	41%	18%	3%	15%
3GPP TS 29. 573 5G System; Public Land Mobile Network (PLMN) Interconnection – Release 16	23%	35%	19%	11%	12%
GSMA FS.34 – Key management for 4G and 5G inter-PLMN Security	22%	36%	23%	8%	12%
3GPP TS 33.517 – 5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) Network Product Class	21%	37%	19%	12%	11%
3GPP TS 29. 573 5G System; Public Land Mobile Network (PLMN) Interconnection – Release 15	21%	35%	22%	7%	16%
GSMA FS.21 – Interconnect Signaling Security Recommendation	21%	32%	29%	7%	12%

Source : *Heavy Reader* 2019

Au niveau du 3GPP, il fallait bien obtenir un consensus international. Ainsi, les exigences ont été définies de manière à laisser la liberté à certains pays de ne pas les mettre en œuvre par leurs télécoms nationales, car certaines de ces fonctions de sécurité assurent également la protection de la vie privée.

En Europe, l'application de certains aspects de la législation reste encore basée sur le volontariat, aussi bien pour les autorités nationales que pour les opérateurs privés. Dans le cadre du Groupe de coopération NIS, par exemple, l'évaluation des stratégies nationales en matière de sécurité des réseaux et des systèmes d'information ainsi que celle de l'efficacité des centres de réponse aux incidents de sécurité informatique (CSIRT) sont facultatives. Cela vaut également pour l'application de la certification des produits et services informatiques au titre du système de certification prévu dans la proposition de

règlement sur la cybersécurité. Bien que la législation ou la certification ne garantissent pas la résilience, l'arsenal de directives, de règlements, et de certifications a pour objectif d'assurer un niveau homogène de sécurité dans l'ensemble de l'UE, bien que leur caractère facultatif de certaines mesures fasse plutôt penser à une harmonisation minimale, et non maximale.

Très souvent la cybersécurité est perçue comme une source de coût et son budget ne représente pas une priorité pour les COMEX. Pour la 5G, aujourd'hui il y a une obligation de couverture des territoires nationaux avant 2030 mais aucune exigence de qualité du service. De plus, les pays ont eu la liberté de choisir parmi trois catégories de fréquences : hautes, moyennes et faibles et ont distribué les classes de fréquence selon leur propre calendrier. Au quatrième trimestre 2021, la qualité du service[53] déployé était très variable. Il est possible que certains opérateurs commerciaux axés sur les coûts n'accordent pas nécessairement la priorité à la sécurité et ils n'appliquent donc pas les mesures préconisées ni ne visent la performance.

Et cette décision est compréhensible, car le secteur privé, absent du processus d'élaboration des normes et des directives, ne se sent pas concerné. Même « le niveau de cybersécurité le plus haut au monde » visé dans la *Stratégie de cybersécurité* est une notion subjective, même d'un État Membre à un autre. Considérons la cybersécurité de la « manière suivante : au niveau national, nous fixons une barre à une certaine hauteur, et si l'adversaire parvient à la franchir sans être détecté, il peut faire ce qu'il veut, qu'il s'agisse de "perturber un service" ou de "surveiller les appels". Le (National Cyber Security Centre (NCSC) recherche les attaquants qui réussissent à sauter par-dessus la barre pour aider à gérer le risque au Royaume-Uni. Il appartient aux ministres de fixer la hauteur de la barre, puis aux opérateurs supervisés par l'Ofcom et le Department for Digital, Culture, Media & Sport (DCMS), et aidés par le NCSC) d'essayer de faire en sorte que les réseaux répondent à cette attente. »[54] Pour l'Europe la barre n'a pas été fixée et laisser le choix à chaque État Membre d'en décider unilatéralement apporterait du chaos au sein d'un réseau fortement interconnecté.

La différence entre un règlement et une directive européenne

Un règlement est un acte législatif dit contraignant pour tous les États membres (EM) car il est appliqué dans son intégralité sur tout le territoire de l'UE. Le règlement entre en vigueur dès qu'il est ratifié par le Parlement européen et précise des objectifs, des moyens et des sanctions. Exemple : *Cybersecurity Act*, *Digital Markets Act*, *Artificial Intelligence Act*, etc.

Une directive est un acte législatif qui présente des objectifs à atteindre par les EM de l'UE d'une manière générale, laissant aux membres individuels le soin d'interpréter et de faire des lois pour les atteindre. Une directive de l'UE s'applique à certains ou à tous les pays membres. Elle est applicable uniquement après sa transcription dans le droit national à travers le vote national. du Exemple : *Networks and Information Systems Directive* (NIS).

L'UE semble vouloir imposer davantage de règles à tous les EM et surtout que ces règles soient appliquées par tous. D'une part, bien que la NIS2 n'impose pas une certification obligatoire, la CE n'exclut pas cette possibilité dans un avenir très proche. D'autre part, la CE fait appel de plus en plus aux règlements qu'aux directives. Les règlements sont d'application immédiate sans période de transposition. À différence des directives, les règlements concernent tous les états, sans distinction.

L'Allemagne : une souveraineté assumée

L'Allemagne illustre très bien de quelle manière les priorités et choix de chaque EM peuvent ébranler toute la stratégie européenne. C'est encore plus préoccupant lorsque l'état concerné, ici l'Allemagne, joue un rôle de leadership au sein de l'UE.

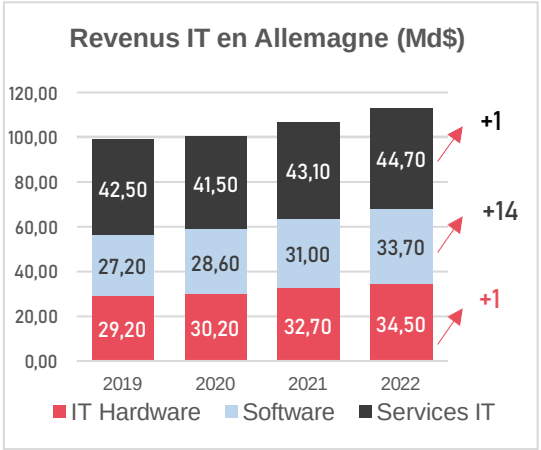
Économiquement, l'Allemagne est le premier exportateur européen[55], et ses relations commerciales avec la Chine[56] et les États-Unis, rendent son économie et sa productivité très dépendante de ses partenaires étrangers. La relation même qu'elle entretient avec les deux puissances économiques risque d'être difficile à tenir à moyen long terme au regard des tensions existantes entre les deux grandes puissances.

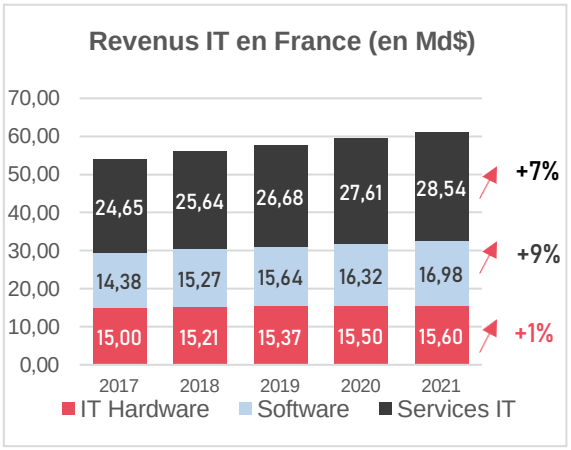
Dans le domaine de la défense, le Chancelier Olaf Scholtz a surpris ses concitoyens et ses partenaires européens, en annonçant cette année le doublement du budget de l'armée, atteignant 1 milliard de dollars[57]. Ainsi l'Allemagne annonce le budget européen le plus important à ce jour, ce qui en ferait la première puissance militaire européenne[58].

Dans le secteur des technologies, l'Allemagne a décidé d'investir 2 milliards de dollars dans le quantique d'ici 2025[59], après avoir fait l'acquisition de *System One*, l'ordinateur quantique d'IBM pour 40 millions d'euros. Cet ordinateur est considéré par son constructeur comme étant « *l'ordinateur quantique le plus puissant d'Europe dans le contexte industriel* » ; c'est aussi le premier ordinateur quantique d'IBM en dehors des frontières nationales. Angela Merkel, docteur en chimie quantique, a déclaré que *System One* pourrait jouer « *un rôle clé dans nos efforts pour la souveraineté technologique et numérique, et bien sûr pour la croissance économique* ». Son fleuron national, l'éditeur logiciel SAP, se trouve dans le top 10 des entreprises tech les plus profitables. L'Allemagne a le plus grand marché du logiciel en Europe avec 95 808 entreprises informatiques (logiciels et matériels)[60].

L'Allemagne est donc un précurseur technologique et l'un des fleurons européens de l'industrie automobile, de la chimie et de l'industrie aéronautique. Compte tenu de ces enjeux industriels, les Allemands ont fait le choix d'acquérir leurs propres licences 5G et des réseaux privés pour des raisons de sécurité : « *Vous ne seriez pas à l'aise de placer vos applications industrielles sur un réseau Wi-Fi, car il n'est pas fiable* »[61], a déclaré Petar Popovski, professeur de connectivité sans fil à l'université d'Aalborg au Danemark. Absence d'interférence, liberté de configuration et de chiffrement des données, choix du lieu de stockage, confiance des utilisateurs… Ce sont autant d'avantages qui, pour des fleurons de l'industrie allemande, n'ont pas de prix. Enfin, grâce à Deutsche Telekom, premier opérateur européen et quatrième au niveau mondial, l'Allemagne possède les réseaux 5G privés les plus développés en Europe.

L'Allemagne est, à juste titre, considérée comme un pays leader en Europe, notamment sur les questions numériques. Il suffit de regarder son positionnement dans le classement des revenus IT pour s'apercevoir. Ci-dessous, nous observons la part de Revenue IT entre le matériel, le logiciel, et le service IT, entre la France et l'Allemagne, et nous pouvons constater très rapidement qu'ils ne progressent ni à la même vitesse, ni sur les mêmes secteurs ITA titre de comparaison, la France et l'Allemagne, ne progressent ni à la même vitesse, ni sur les mêmes secteurs IT :





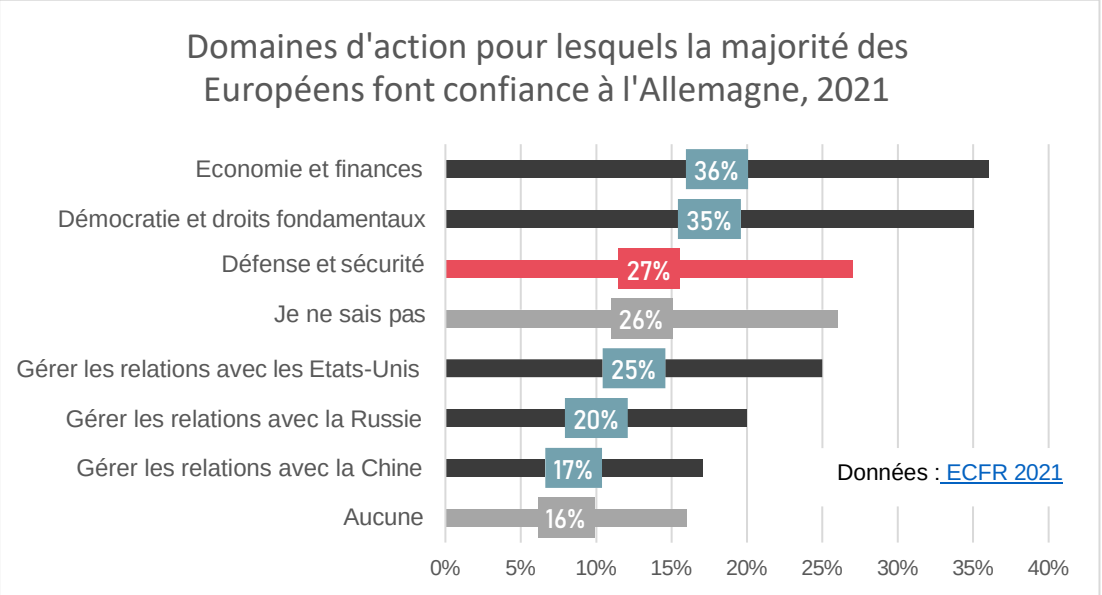
Données :

pour l'Allemagne, adapté de « ITK-Marktzahlen » par Bitkom ITK-Märkte, EITO 2022.International Trade Administration

Pour la France : Statista

Nous retrouvons d'ailleurs ces ambitions dans le financement sur la cybersécurité. En effet, la BSI est l'agence nationale de cybersécurité la plus développée au sein de l'UE, en termes de budget et de personnel.

C'est donc tout naturellement que les Européens sont nombreux à faire confiance à l'Allemagne dans la gouvernance de l'UE.



En Allemagne, les derniers signaux envoyés à l'Europe, et particulièrement à la France, montrent très clairement que l'Allemagne ne fait pas le choix du consensus européen ; elle a décidé d'assumer sa stratégie nationale. Faute d'options européennes crédibles ? Dans certains cas, sans doute, mais ce n'est pas la seule raison. Victime de ses dépendances économiques et militaires mises en place à la fin de la Seconde guerre mondiale, l'Allemagne est aujourd'hui fragilisée et représente une vulnérabilité pour l'Union toute entière.

Le moteur franco-allemand, s'il a existé un jour, aujourd'hui n'existe plus. Dans le domaine de la cybersécurité, Allemagne a participé avec des schémas des certification. Les indices actuels montrent une tendance à vouloir affirmer un leadership national et gagner en autonomie.

L'Europe n'a donc plus de récit approprié pour insuffler des actions communes entre États membres, et les répercussions sur l'industrie numérique européenne, et plus particulièrement le secteur de la cybersécurité, sont notables. L'enjeu d'une mise en confiance des États membres est décisif, à l'heure où l'Europe manque cruellement de ressources pour faire face à la menace. Le sujet de la cyberdiplomatie est un objectif de la stratégie cyber européenne. Elle pourrait être le support du récit européen… Rappelons cependant que la diplomatie est bien souvent utilisée de manière naïvement pacifiste, et qu'elle ne débouche que trop peu souvent sur des actions concrètes.

L'UE doit en tenir compte. D'autres pays voudront probablement s'impliquer davantage dans les problématiques de sécurité. Heureusement cela est possible, même souhaitable puisque, grâce à sa diversité, l'Europe en est capable. Si la diversité européenne devient une richesse, un avantage compétitif, le récit européen devrait catalyser la volonté de diminuer les dépendances hors UE, de booster la performance des secteurs privés nationaux et de comprendre mieux ses partenaires. Autrement dit, de transformer la coopération en collaboration.

Défense

Réarmement auprès de l'industrie états-unienne, faute d'option européenne à court terme, et compte tenu de sa dépendance au marché automobile américain. Le plus important budget défense de l'UE.

Économie

Sa dépendance au marcne chinois et nord-américain a fragilisé son économie, notamment automobile, tant à l'export des véhicules, qu'à l'import des pièces détachées.

Énergie

Sa dépendance au gaz russe a longtemps contribué à la bonne santé de son économie. Aujourd'hui, cette dépendance est considérée une vulnérabilité, pour l'Allemagne, mais aussi pour l'Europe.

Sécurité numérique

Acquisition en 2019 de Quantum System One d'IBM. Installé dans un datacenter d'IBM,une nouvelle dépendance technologique semble se mettre en place à défaut d'une solution européenne.

Réflexions finales

L'"Union Européenne a finalement beaucoup agi dans le domaine de la cybersécurité. De surcroît, les implications de l'action ou de l'inaction de l'Union européenne sont visibles au de-là de ses frontières. L'"effet Bruxelles" - ou l'idée qu'en raison de la taille de son marché, les règlements promulgués par l'UE peuvent inspirer des multinationales qui les transformeront en normes mondiales – est de plus en plus actif. Le *Règlement Général pour la Protection des Données* et l'*Artificial Intelligence Act* ainsi que leur traduction ailleurs dans le monde en sont la preuve.

Mais avoir voulu imposer un cadre réglementaire strict après des années de laxisme (le *RGPD* a été adopté après des années de transfert des données des Européens à l'étranger) n'est pas sans conséquences. Les acteurs européens souffrent déjà d'un cadre réglementaire ambitieux pour certains, trop contraignant pour d'autres. Vouloir mettre sur le marché un produit hautement sécurisé dans ces circonstances relève de la double peine : la conformité légale a un coût, tout comme la sécurité.

Comme nous l'avons vu, la menace cyber ne s'arrête pas aux frontières terrestres : elle profite du réseau mondial et passe sur tous les continents. Un Etat de l'Union européenne qui voudrait renforcer sa cybersécurité ne pourrait donc pas être pleinement efficace. C'est alors qu'échanger sur les menaces cyber identifiées est primordial. Mais cela reste difficile tant au niveau des Etats membres que des entreprises privées ; l'Union européenne n'étant pas une union fédérale, chaque État jouit de sa souveraineté, rien ne peut leur être imposé. Pourtant, il est aujourd'hui impératif que les États de l'Union utilisent les outils mis à leur disposition afin de créer des synergies entre les informations et les compétences de chacun afin de mieux se défendre.

Pour cette raison, la cybersécurité ne doit pas être prise en compte qu'au niveau européen et à travers les recommandations de l'Union européenne. Au niveau des EM, une approche trop centralisée a déjà montré ses faiblesses en France. Typiquement, la rupture de communication identifiée entre l'ANSSI, le gouvernement et le secteur privé est symptôme d'une approche centralisée de la cybersécurité. Or la sécurité, et ce par l'interconnectivité mondiale, dépend de chaque terminal numérique présent sur le réseau. Le Japon a très rapidement identifié cette nécessité de coopération entre le secteur public et le secteur privé, et a imposé un échange permanent entre les deux entités. Dans les dernières décennies, cela lui a permis rapidement de construire son tissu industriel à la fois traditionnel et ultra-innovant sur le plan des technologies. Nous avons à apprendre de l'exemple japonais que vouloir séparer la sécurité et le développement industriel n'est peut-être pas le plus rentable. En découplant industrie et sécurité, l'Europe et ses Etats membres pourraient exceller à se sécuriser, mais échoueraient à maintenir leur compétitivité industrielle. L'approche israélienne est aussi un bon exemple : le gouvernement israélien favorise l'innovation privée tout en assurant une certaine culture militaire ; une fois la solution innovante créé, elle est industrialisée et, en parallèle, réadaptée au domaine de la sécurité militaire. Ainsi, des solutions existent déjà à l'étranger : il suffirait de les adapter au contexte européen pour progresser.

Les failles dans la gouvernance de la 5G doivent servir de leçon, non seulement pour la 6G qui approche mais également pour les autres technologies émergentes (IA, IoT, blockchain, réalité virtuelle, etc). Ces technologies ne représentent pas seulement des avantages compétitifs pour l'industrie des jeux vidéo et d'autres loisirs. Ce sont des technologies sur lesquelles doit se construire la future industrie 4.0. européenne. La performance et la sécurité en sont donc un passage obligé et un casse-tête permanent pour les dirigeants européens.

Mais assurer le lien entre sécurité et industrie n'est pas l'unique objectif que doit poursuivre l'Europe. Comme l'affirmait Guy-Philippe Goldstein, l'Union européenne doit être un acteur de réseau dans l'espace cyber mondial. C'est ici que la diversité des Etats membres autonomes de l'UE est une grande force. Pour chaque État membre, il ne s'agit pas de développer individuellement tous les outils nécessaires à l'entretien de la sécurité sur les réseaux, ou encore de créer des innovations disruptives permettant de devenir des champions mondiaux. Il s'agit en réalité de coopérer avec tous les autres États membres, pour mettre en commun les forces de chacun. Si, en fonction de ses forces et de ses faiblesses, chaque États membre développe une solution particulière nécessaire au réseau mondial, alors l'Europe développera son autonomie. Grâce à sa diversité, le réseau européen pourrait retrouver une position de leader et faire de l'Europe un incontournable technologique. Les bénéfices pour les États membres seront très importants : leurs dépendances à la Chine ou aux États-Unis deviendraient des interdépendances au sein d'un réseau mondial, ce qui réduirait mécaniquement leurs insécurités et vulnérabilités. Si cela doit passer par une confiance sans faille dans les relations entretenues entre tous les États européens, cela

passe aussi par des investissements et des politiques d'incitation à prioriser. Il est nécessaire de soutenir la recherche privée, et pas seulement militaire comme c'est massivement le cas aujourd'hui. Les solutions défensives davantage que les solutions offensives. Mais pas uniquement. Il faut aussi soutenir la mise sur un marché commercial des produits crées et répondant à un besoin du réseau, afin de bénéficier de l'incitation du profit. Finalement, le développement de solutions commerciales doit être prioritaire, et c'est ce dont l'Europe manque. Une position puissante permettra également de corriger la posture vis-à-vis de l'OTAN. Ce statut d'indépendance et d'autonomie cyber inter-régionale ne sera que bénéfique sur le plan économique, pour les domaines de la Recherche et Développement, de l'Industrie et de la Défense.

Dans ce contexte, la performance, si elle va de pair avec la confiance, doit être considérée comme encore plus importante. Développer une culture de la performance et du "rendre compte" du Nord au Sud et de l'Est à l'Ouest est primordial. Pour y arriver, la coordination et la coopération devront se compléter d'une collaboration, mot qu'aucune des personnes interrogées n'a jamais prononcé à l'exception du responsable du écossais. Autrement, nous allons nous épuiser à répondre aux attaques plutôt qu'à les prévenir. Le nouveau récit européen devra conjuguer diversité, collaboration et performance afin de faire de l'Europe un acteur autonome et singulier dans le cyberespace.

"If we adopt the same collaborative mindset and practices that got to the moon and back, and that built the International Space Station, we can alleviate poverty—and do much more." *Ron Garan*

Annexes

ANNEXE I

CLASSEMENT DES OPÉRATEURS TÉLÉCOM

Classement 2014/03	Classement 2022/10	Entreprise	CA en Md$ 2014	CA en Md$ 2022	Pays
1	5	Nippon Telegraph & Telephone	128.9	171.7	Japon
2	1	AT&T	127.4	128.2	États-Unis
3	2	Verizon Communications	115.8	122.3	États-Unis
4	4	China Mobile Com	96.9	116.8	Chine
5	13	Telefónica	80.1	107.1	Espagne
6	3	Deutsche Telekom	74.8	103.5	Allemagne
7	9	Vodafone Group	70.2	57.0	Royaume-Uni
8	6	Comcast	62.6	56.8	Japon
9	10	América Móvil	58.9	52.2	Mexique
10	11	Orange S.A.	55.9	52.7	France
11	7	China Telecommunications	53.4	49.0	Chine
12	15	KDDI	44.1	43.6	Japon
13	8	Softbank	40.7	43.0	Japon
14	14	China Uted Network Com	40.6	42.8	Chine
15	18	Telecom Italia	38.3	34.8	Italie
16	?	Sprint - > T-Mobile	35.3	32.3	États-Unis
17	16	BT Group	29.1	23.4	Royaume-Uni
18	21	Telstra	26.3	22.8	Australie
19	0	CenturyLink -> Lumen	18.0	21.3	États-Unis

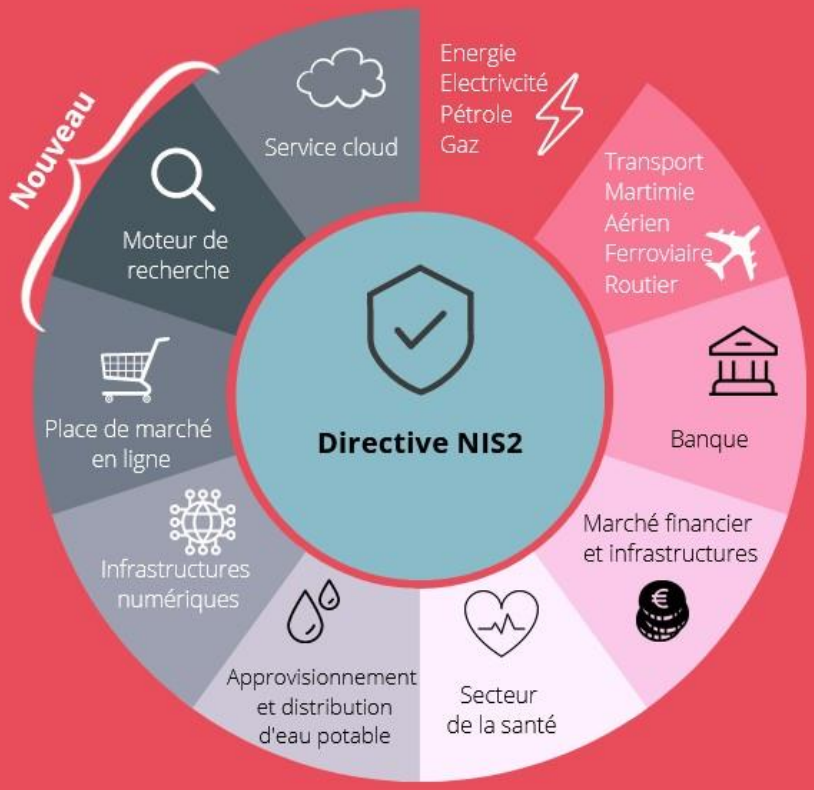
monte dans le classement

descend dans le classement

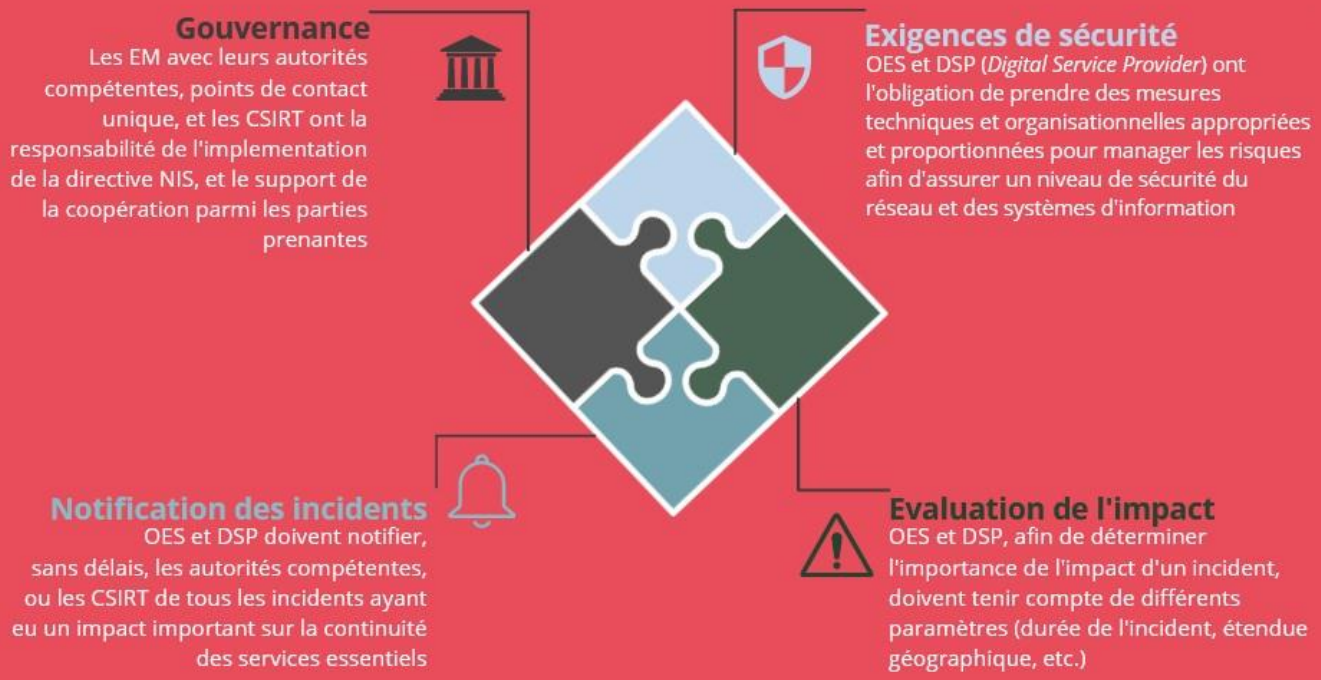
Données : Wikipédia 2014 et 2022

ANNEXE II

LA NOUVELLE DIRECTIVE NIS (NIS2)

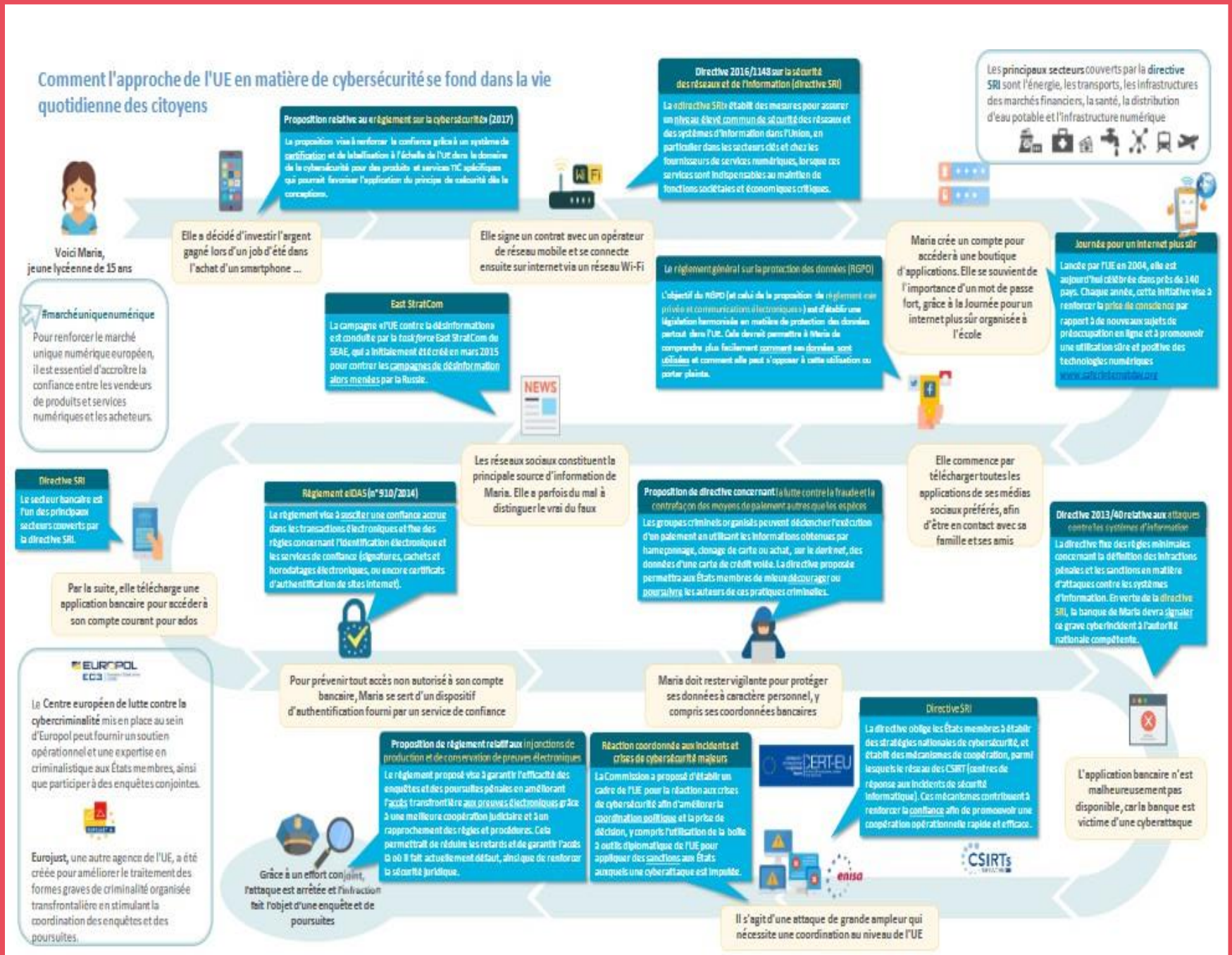


Nouveaux secteurs d'activité concernés par la Directive NIS2



Perspectives de sécurité des systèmes d'information prévues dans la NIS2

Données : Deloitte 2022



Source: Cour des comptes européenne.

ANNEXE IV

INDICE DE SOUVERAINETÉ EU

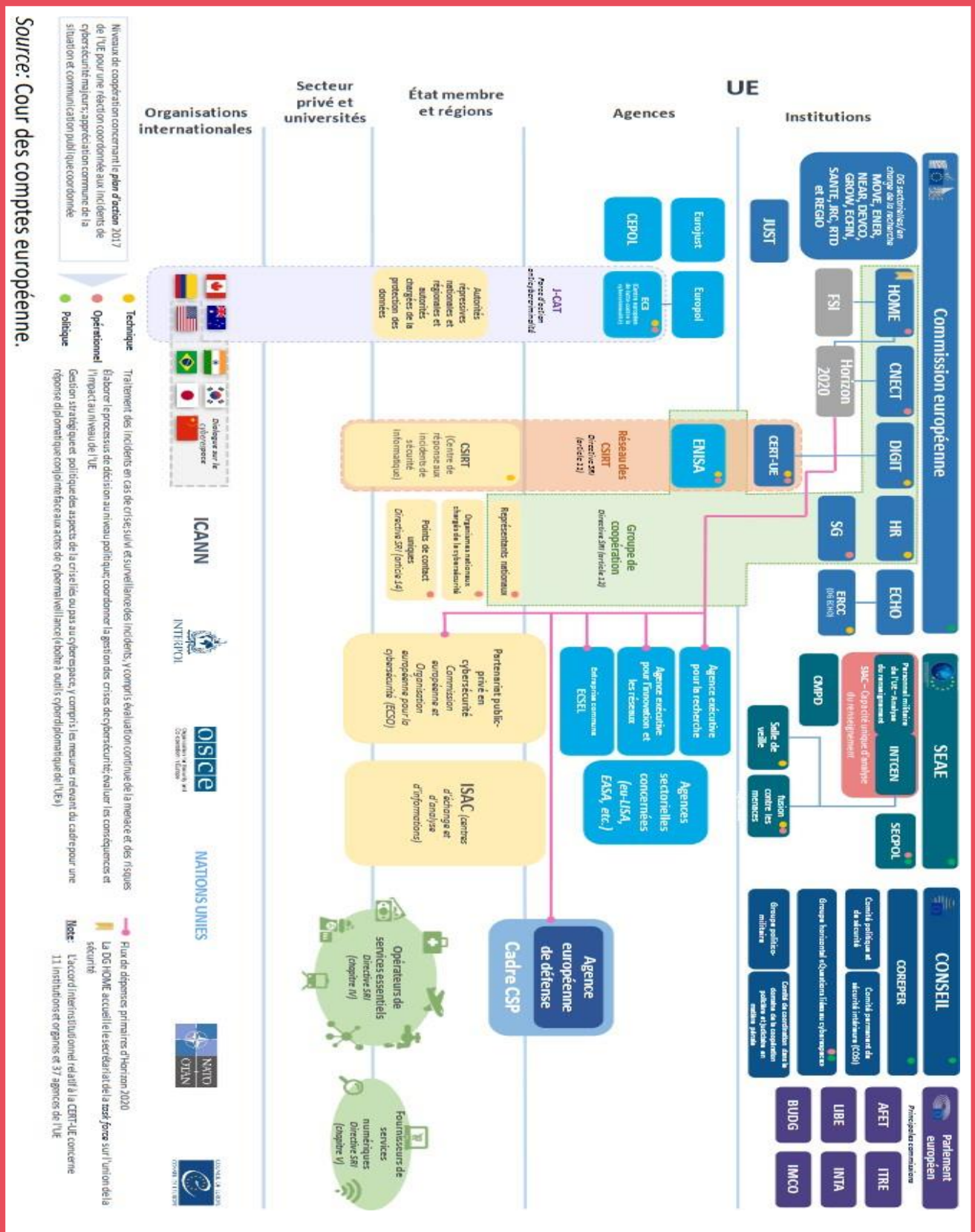
Pays	Global	Engagements	Capacités
Finlande	7,4	8,4	6,5
Luxembourg	7,1	8,5	5,7
Suède	6,8	7,4	6,2
Irelande	6,6	7,6	5,6
Pays-Bas	6,3	7,7	4,9
Danemark	6,1	7,6	4,6
Estonie	5,9	7,9	4,0
Slovénie	5,6	8,3	2,9
Belgique	5,5	7,6	3,4
France	5,4	7,1	3,8
Allemangne	5,3	7,0	3,6
Chypre	5,3	7,9	2,8
Autriche	5,0	6,8	3,2
EU	4,8	6,7	3,0
Espagne	4,8	7,0	2,5
Malte	4,8	6,9	2,7
Portugal	4,6	6,9	2,3
Italie	4,3	6,6	2,1
Lettonie	4,3	6,2	2,3
Lituanie	4,2	6,1	2,4
Grèce	4,1	6,5	1,8
République Tchèque	3,6	5,2	1,9
Pologne	3,6	5,5	1,7
Croatie	3,6	5,5	1,7
Bulgarie	3,5	5,5	1,5
Slovaquie	3,4	5,3	1,5
Hongrie	3,3	4,8	1,8
Roumanie	3,2	4,8	1,6

10 est la note maximum

Données : European Council for Foreign Relations 2022

ANNEXE V

60 STRUCTURES CYBER EN FRANCE

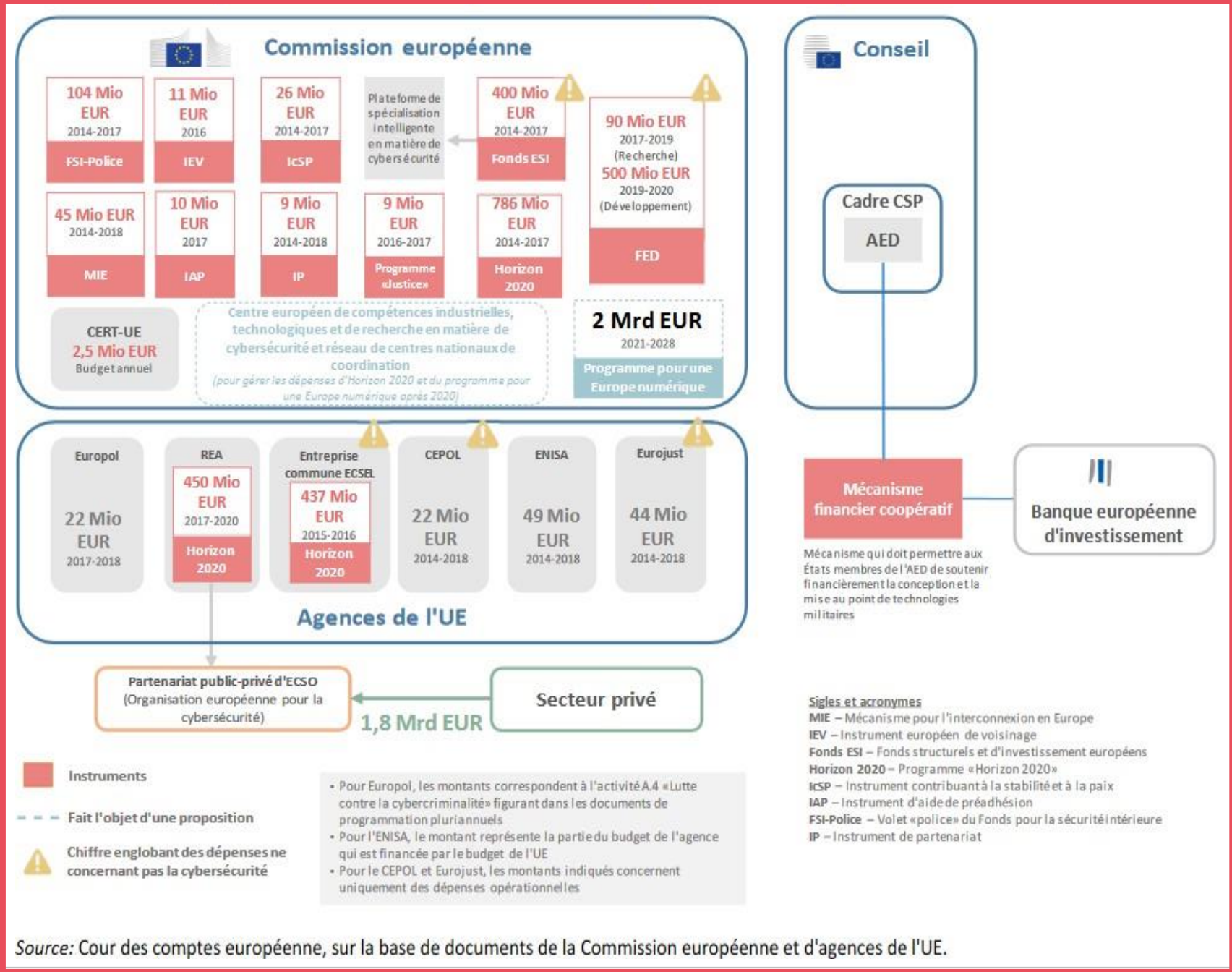


Source: Cour des comptes européenne.

Paysage stratifié et complèxe des acteurs français de la cybersécurité

Source : Cour des Comptes Européenne

DÉPENSES EU DÉDIÉES À LA CYBERSÉCURITÉ



Source: Cour des comptes européenne, sur la base de documents de la Commission européenne et d'agences de l'UE.

Dépenses consécrées par l'UE à la cybersécurité depuis 2014

Données : Cour des Comptes Européenne 2019

NOTIONS DE CHIFFREMENT

Aujourd'hui, le chiffrement repose sur deux classes de solutions : le chiffrement symétrique (basé sur l'existence d'une seule clé e qui est utilisé lorsque celle-ci ne doit pas être communiquée) et le chiffrement asymétrique (qui nécessite une clé publique qui chiffre une clé privée qui doit être transmise). Les solutions les plus utilisées aujourd'hui sont détaillées ci-dessous :

Chiffrement symétrique (données au repos)	Chiffrement asymétrique, ou à clé publique (échange des clefs, données en transit)
Chiffrement par blocs : AES	Factorisation de grands entiers : RSA
Fonctions de hashage : SHA3	Logarithme discret (courbes elliptiques) : ECDH, ECDSA
Sensible à l'algorithme quantique de Groover (diminue de moitié la taille de la clé)	Sensibles à l'algorithme quantique de Shor

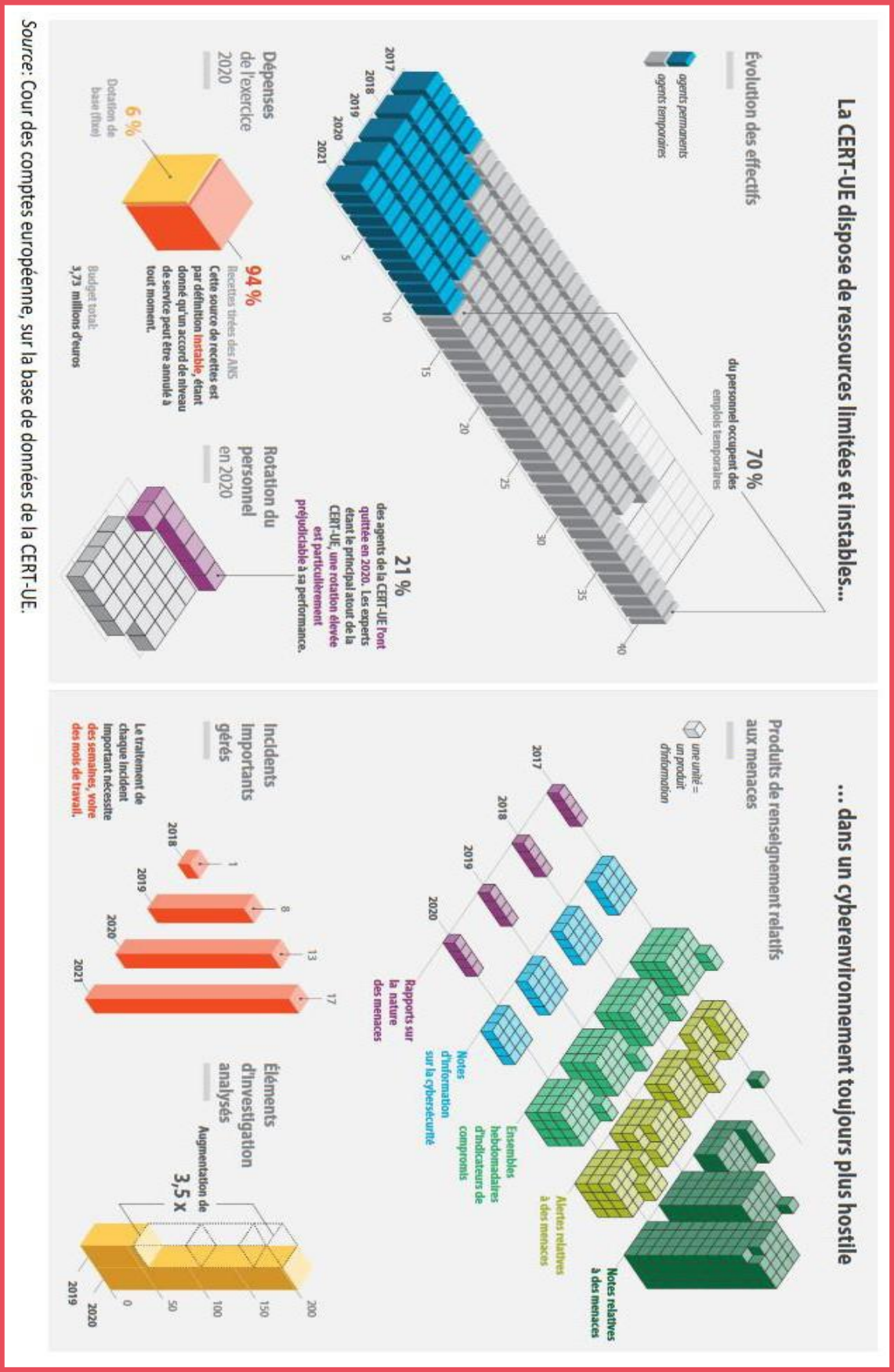
L'échange des clefs dans le chiffrement asymétrique se fait aujourd'hui majoritairement par ECDH, bien que des solutions plus anciennes de RSA subsistent (le RSA demande des clefs plus longues pour assurer le même niveau de sécurité qu'une solution ECDH). Les protocoles internet SSL/TLS et HTTPS utilisent majoritairement ces solutions, tout comme certaines signatures digitales qui incorporent le RSA.

D'autre part, l'AES est la norme pour assurer la confidentialité des données stockées (bases de données, secrets d'états, données sensibles, etc.). L'AES est aujourd'hui la solution de chiffrement de Microsoft, Apple, nombreux VPN et solutions de compression. Le SHA3 est également utilisé et garantit l'intégrité des données.

Les experts en cryptographie pensent que la commercialisation d'ordinateurs quantiques pourrait endommager ces sécurités : compromettre tout le chiffrement à clé publique (asymétrique) et affaiblir le chiffrement symétrique. D'autre part, les ingénieurs en quantum computing affirment que, pour casser une clé RSA, un ordinateur quantique devra être muni de plusieurs milliers de qubits, alors qu'aujourd'hui les avancées technologiques proposent à peine une centaine de qubit[1]. Néanmoins, la certification et l'adoption d'une nouvelle norme technologique prend, selon Moody, mathématicien chez NIST, entre 10 et 20 ans[1]. Il s'avère que l'avènement des premiers ordinateurs quantiques capables de compromettre certaines solutions de chiffrement est prévu dans une dizaine d'années aussi. D'où la décision du NIST de choisir plusieurs solutions et de les entériner en tant que normes avant 2024.

ANNEXE VIII

DIFFICULTÉS DU CERT-EU



Source: Cour des comptes européenne, sur la base de données de la CERT-UE.

Ressources et défis de la CERT-EU

Données : Cour des Comptes Européenne 2022

Bibliographie et entretiens

Œuvres imprimées

GOLDSTEIN, Guy-Philippe. *Cyberdéfense et cyberpuissance au XXIe siècle*. Paris. Balland. 2022.

HARBULOT, Christian. *Manuel d'Intelligence économique*. Paris. PUF. 2019

HARBULOT, Christian et al. *Guerre économique. Qui est l'ennemi ?* Paris. Nouveau monde Eds. 2022

LAIDI, Ali. *Le Droit, nouvelle arme de guerre économique*. Paris. Acte Sud. 2019

PITRON, Guillaume. *L'enfer numérique*, Paris. Les Liens Qui Libèrent. 2021

VON CLAUSWITZ, Carl. *De la guerre (Vom Krieg).* Paris. Éditions Fayard Mille et une nuit. 2006

Œuvres numériques

ACCESS NOW. *Three Years under the EU GDPR* [PDF]. AccessNow [en ligne]. 2021 [Consulté le 5 mai 2022]. Disponible à l'adresse : https://www.accessnow.org/cms/assets/uploads/2021/05/Three-Years-Under-GDPR-report.pdf

AFNIC et INSTITUT DE LA SOUVERAINETÉ NUMÉRIQUE. *Internet des objets & souveraineté numérique* [PDF]. Afnic [en ligne]. 2021 [Consulté le 4 mai 2022]. Disponible à l'adresse : https://www.afnic.fr/wp-media/uploads/2021/03/Rapport_IoT_ISN_Afnic.pdf

AON. *2020 Cyber Security Risk Report* [PDF]. AON [en ligne]. 2021 [Consulté le 5 avril 2022]. Disponible à l'adresse : https://insights-north-america.aon.com/cyber/2020-cyber-security-risk-report

ATLANTIK-BRÜCKE. *Vertrauen in der Krise. Landkarten geopolitischer Chancen und Risiken* [PDF]. Atlantik-Brücke [en ligne]. 2019 [Consulté le 5 mai 2022]. Disponible à l'adresse : https://www.atlantik-bruecke.org/wp-content/uploads/AtlantikBrueckeUmfrage2019.pdf

BOTHOREL, Éric. *Rapport d'information déposé par la Commission des affaires européennes sur l'avenir de la cybersécurité européenne* [PDF]. Assemblée Nationale. Disponible à l'adresse : https://www.assemblee-nationale.fr/dyn/15/rapports/due/l15b2415_rapport-information.pdf

BOULAY, Benjamin. *L'interculturel en France Orientation des débats et des travaux* (2000-2007) [PDF]. Dans *Hommes et Migrations*, hors-série. Novembre 2008 [Consulté le 5 mai 2022]. *L'interculturalité en débat*. Disponible à l'adresse : https://doi.org/10.3406/homig.2008.4684

BRONNER, Gérald. Le rapport Bronner : *Les Lumières à l'ère numérique* [PDF]. Vie publique [en ligne]. 12 février 2022 [Consulté le 4 septembre 2022]. Disponible à l'adresse : https://www.viepublique.fr/sites/default/files/rapport/pdf/283201.pdf

CARRAPICO, Helena et BARRINHA, André. *The EU as a Coherent (Cyber)Security Actor ?* [PDF]. Journal of Common Market Studies [en ligne]. 10 mai 2017 [Consulté le 4 mai 2022]. Disponible à l'adresse : https://doi.org/10.1111/jcms.12575

COMMISSION EUROPÉENNE. *Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé* [PDF]. CE [en ligne]. 7 février 2013 [Consulté le 4 octobre 2022]. Disponible à l'adresse : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52013JC0001&from=FR

COMMISSION EUROPÉENNE. *Recommendations of 26.3.2019 - Cybersecurity of 5G networks*. CE [PDF]. ECA [en ligne]. 26 mars 2019 [Consulté le 11 mai 2022]. Disponible à l'adresse : https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks

COMMISSION EUROPÉENNE. *Rapport de la Commission au Parlement européen et au Conseil évaluant la cohérence de l'approche adoptée par les États membres pour identifier les opérateurs de services essentiels conformément à l'article 23, paragraphe 1 de la directive 2016/1148/UE concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union* [PDF]. CE. 546 final [en ligne]. 28 octobre 2019 [Consulté le 5 août 2022]. Disponible à l'adresse : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52019DC0546&from=EN

COUR DES COMPTES EUROPÉENNE. *Défis à relever pour une politique de l'UE efficace dans le domaine de la cybersécurité* [PDF]. ECA [en ligne]. Mars 2019 [Consulté le 4 mai 2022]. Disponible à l'adresse : https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_FR.pdf

COUR DES COMPTES EUROPÉENNE. *Cybersécurité des institutions, organes et agences de l'UE. Un niveau de préparation globalement insuffisant par rapport aux menaces* [PDF]. ECA [en ligne]. 2022 [Consulté le 3 septembre 2022]. Disponible à l'adresse : https://www.eca.europa.eu/Lists/ECADocuments/SR22_05/SR_cybersecurity-EU-institutions_FR.pdf

DAMRO, Chad. *Market power Europe: exploring a dynamic conceptual framework* [PDF]. Journal of European Public Policy. [en ligne]. Juin 2015. [Consulté le 4 octobre 2022]. Disponible à l'adresse : https://www.pure.ed.ac.uk/ws/files/19507987/Damro_C._2015_._Market_Power_Europe.pdf

DEMCHAK, Chris et SHAVITT, Yuval. *China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking* [PDF]. Military Cyber Affairs [en ligne]. Juin 2018 [Consulté le 5 juin 2022]. Volume 3. Issue 1. Article 7. Disponible à l'adresse : https://www.researchgate.net/publication/328435903_China's_Maxim_-_Leave_No_Access_Point_Unexploited_The_Hidden_Story_of_China_Telecom's_BGP_Hijacking

DIRECTORATE-GENERAL FOR COMMUNICATIONS NETWORKS, CONTENT AND TECHNOLOGY. *Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres* [PDF]. UE [en ligne]. 20 septembre 2018 [Consulté le 4 mai 2022]. Disponible à l'adresse : https://ec.europa.eu/transparency/documents-register/detail?ref=SWD(2018)403&lang=en

ECONOMIST INTELLIGENCE. *Democracy Index 2021: The China challenge* [PDF]. EIU [en ligne]. 2022 [Consulté le 4 octobre 2022]. Disponible à l'adresse : https://pages.eiu.com/rs/753-RIQ-438/images/eiu-democracy-index-2021.pdf

ERICSSON. *Ericsson Mobility Report* [PDF]. Ericsson [en ligne] Août 2022. [Consulté le 5 septembre 2022]. Disponible à l'adresse : https://www.ericsson.com/4a4be7/assets/local/reports-papers/mobility-report/documents/2022/ericsson-mobility-report-q2-2022.pdf

EUROPEAN ACADEMIES SCIENCE ADVISORY COUNCIL. *International Sharing of Personal Health Data for Research* [PDF]. 8 avril 2021. Disponible à l'adresse : https://easac.eu/fileadmin/PDF_s/reports_statements/Health_Data/International_Health_Data_Transfer_2021_web.pdf

EUROPEAN COMMISSION. *Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime* [PDF]. *EC [en ligne]. (2000) 890 final. 26 janvier 2001 [Consulté le 4 mai 2022]. Disponible à l'adresse :* https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0890:FIN:EN:PDF

EUROPEAN COMMISSION. *Better regulation for growth and jobs in the European Union. Communication from the Commission to the Council and the European Parliament [PDF]. EC [en ligne]. (2005) 97 final, 16 mars 2005 [Consulté le 5 août 2022]. Disponible à l'adresse :* https://aei.pitt.edu/43023/1/com2005_0097.pdf

EUROPEAN COMMISSION. *Foreign Direct Investment In The EU* (PDF). EC [en ligne]. 13 mars 2019 [Consulté le 5 mai 2022]. Disponible à l'adresse : https://trade.ec.europa.eu/doclib/docs/2019/march/tradoc_157724.pdf

EUROPEAN COMMISSION. *NIS Implementation Tracker*. EC [en ligne]. 22 mars 2019 [Consulté le 5 mai 2022]. Disponible à l'adresse : https://www.digitaleurope.org/resources/nis-implementation-tracker/

EUROPEAN COMMISSION. *The EU's Cybersecurity Strategy for the Digital Decade* [PDF]. EC [en ligne]. 16 décembre 2020 [Consulté le 3 mai 2022]. Disponible à l'adresse : https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

EUROPEAN COMMISSION. *State-of-play of the transposition of the NIS Directive*. EC [en ligne]. 7 juin 2022. [Consulté le 5 septembre 2022]. Disponible à l'adresse : https://digital-strategy.ec.europa.eu/en/policies/nis-transposition

EUROPEAN COURT OF AUDITORS. *Challenges to effective EU cybersecurity policy* [PDF]. ECA *[en ligne]*. Mars 2019 [Consulté le 5 mai 2022]. Disponible à l'adresse : https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

EUROPEAN COURT OF AUDITORS. *Déploiement des réseaux 5G au sein de l'UE : des retards et des questions de sécurité encore sans réponse. Rapport spécial n° 03, 2022* [PDF]. Publications Office of the European Union (en ligne). 2022 [Consulté le 4 septembre 2022]. Disponible à l'adresse : https://data.europa.eu/doi/10.2865/337980

EUROPEAN CYBER SECURITY ORGANISATION. *ECS cPPP Progress Monitoring Report 2016-2017* [PDF]. *[en ligne].* 29 octobre 2018 [Consulté le 5 avril 2022]. Disponible à l'adresse : https://www.ecs-org.eu/documents/uploads/progress-monitoring-report-2016-2017.pdf

EUROPEAN UNION EXTERNAL ACTION. *Shared Vision, Common Action: A Stronger Europe* [PDF]. EU [en ligne]. Juin 2016 [Consulté le 5 mai 2022]. Disponible à l'adresse : https://www.eeas.europa.eu/eeas/global-strategy-european-unions-foreign-and-security-policy_en

EUROPOL. *Internet Organised Crime Threat Assessment (IOCTA)* [PDF]. Europol [en ligne]. 27 septembre 2017 [Consulté le 4 mai 2022]. Disponible à l'adresse : https://www.europol.europa.eu/cms/sites/default/files/documents/iocta2017.pdf

GILLEY, Bruce. *Huawei' Fixed Line to Beijing* [PDF]. Far Eastern Economic Review *[en ligne].* 28 décembre 2000-4 janvier 2001 [Consulté le 4 mai 2022]. Disponible à l'adresse : https://web.pdx.edu/~gilleyb/Huawei_FEER28Dec2000.pdf

HUAWEI. *Investment and Holding. Annual Report 2021* [PDF]. 2021 [Consulté le 4 mai 2022]. Disponible à l'adresse : https://www-file.huawei.com/minisite/media/annual_report/annual_report_2021_en.pdf?version=0401

INTERNATIONAL TELECOMMUNICATIONS UNION. *Global Cybersecurity Index 2020* [PDF]. ITU [en ligne]. 2020 [Consulté le 4 mai 2022]. Disponible à l'adresse : https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

KRASTEV, Ivan et LEONARD, Mark. *What Europeans think about the US-China Cold War* [PDF]. ECFR *[en ligne].* 21 septembre 2021 [Consulté le 5 mai 2022]. Disponible à l'adresse : https://ecfr.eu/wp-content/uploads/What-Europeans-think-about-the-US-China-Cold-War-2.pdf

LEONARD, Mark et PUGLIERIN, Jana. *Policy Brief How to Prevent Germany from Becoming Eurosceptic* [PDF]. ECFR [en ligne]. Juin 2021 [Consulté le 5 mai 2022]. Disponible à l'adresse : https://ecfr.eu/wp-content/uploads/How-to-prevent-Germany-from-becoming-Eurosceptic.pdf

MEULLER, Benjamin. *How Much Will the Artificial Intelligence Act Cost Europe?* [PDF] Centre for Data Innovation [en ligne]. Juillet 2021 [Consulté le 5 mars 2022]. Disponible à l'adresse : https://www2.datainnovation.org/2021-aia-costs.pdf

SOPHOS. T*he State of Ransomware 2021* [PDF]. Sophos [en ligne]. Avril 2021 (Consulté le 4 mai 2022]. Disponible à l'adresse : https://assets.sophos.com/X24WTUEQ/at/k4qjqs73jk9256hffhqsmf/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469

U.S. COMMERCIAL SERVICE. *Germany Country Commercial* Guide [PDF]. International Trade Administration [en ligne]. 2022 [Consulté le 10 septembre 2022]. Disponible à l'adresse : https://www.trade.gov/sites/default/files/2022-09/CCGGermany2022.pdf

VERBEEK, Arnold et LUNDQVIST, Maria. *Artificial Intelligence, Blockchain And The Future Of Europe* [PDF]. European Commission Directorate-General for Communications Networks [en ligne], Content and Technology and European Investment Bank. Juillet 2021. [Consulté le 16 septembre 2022]. 49. Disponible à l'adresse : https://www.eib.org/attachments/thematic/artificial_intelligence_blockchain_and_the_future_of_europe_report_en.pdf

YANG, Guang. *Who Are the Leading Players in 5G Standardization?* [PDF]. Strategy Analytics [en ligne]. Mars 2020.. [Consulté le 4 août]. Disponible à l'adresse : https://www.strategyanalytics.com/access-services/service-providers/networks-and-service-platforms/reports/report-detail/who-are-the-leading-players-in-5g-standardization-an-assessment-for-3gpp-5g-activities?slid=2386935&spg=1

Vidéos

CAVE, Danielle. *Australia's 5G decision* [video]. Australian Strategic Policy Institute [en ligne]. 21 juillet 2019 [Consulté le 3 mai 2022]. Disponible à l'adresse : https://www.aspi.org.au/video/australias-5g-decision?__cf_chl_tk=UZdLeV14Rx4i6upsnqgegvVsfxJuVP6v7eeRtEvVblM-1660402142-0-gaNycGzNCH0

CNBC. *Interview with Pekka Lundmark: No green without digital*. CNBC [YouTube]. 3 novembre 2021 [Consulté le 4 octobre 2022]. Disponible à l'adresse : https://youtu.be/ySUSCL7yRt8

JUILLET, Alain. *Le renseignement, outil de l'intelligence économique*. [YouTube]. 16 octobre 2019 [Consulté le 2 mars 2020]. Disponible à l'adresse : https://www.youtube.com/watch?v=vUChdxWxt5o

RAVAIHLE Nicolas. *Le lobbying : Une arme redoutable dans la guerre économique mondiale*. Le 22 septembre 2022 [Consulté le 24 septembre 2022]. Disponible à l'adresse : https://www.youtube.com/watch?v=5KbVwCUFtL0&ab_channel=OPENBOXTV

Entretiens

GOLDSTEIN, Guy-Philippe. Consultant de conseil en stratégie. 13 juillet 2022

PELLETIER, Benjamin. Maître de conférences et professeur à l'EGE. 2 juin 2022

TRICAUD Anne. Cheffe de la division internationale ANSSI pendant la présidence française. 27 juillet 2022

Anonymes : *Certaines professionnels ont un devoir de réserve et se sont entretenus en requérant l'anonymat* :

Deux officiers supérieurs du COMCYBER le 29 juin 2022

Guillaume, responsable cyber manager AWS, le 21 juin 2022

Chargé de mission d'une association européenne pour la cybersécurité Bruxelles, le 9 novembre 2022

Responsible cybersécurité au National Health System Scotland, le 4 août 2022

Notes

PRÉAMBULE

[1] CASTAÑER, Xavier et OLIVEIRA, Nuno. *Collaboration, Coordination, and Cooperation Among Organizations: Establishing the Distinctive Meanings of These Terms Through a Systematic Literature Review*. Journal of Management (en ligne]. Vol. 46. No. 6. Juillet 2020 [Consulté le 4 mai 2022]. pp. 965 – 1001. Disponible à l'adresse : https://journals.sagepub.com/doi/epub/10.1177/0149206320901565
Cette recherche vise à identifier l'utilisation des termes coopération, collaboration et coordination telle qu'elle a été identifiée dans 2220 articles publiés entre 1948 et 2017, en Europe et aux États-Unis, et contenant les définitions proposées de ces termes.

[2] *Ibid.* p. 972.

[3] CONSILIUM EUROPA. Disponible à l'adresse : https://www.consilium.europa.eu/fr/policies/cybersecurity/

1. UNE STRATÉGIE CYBER À LA HAUTEUR DE LA MENACE

1.1. À la croisée des puissances mondiales

[1] Bien qu'Internet englobe the WorldWideWeb, ou www, mais pas seulement, nous allons utiliser le mot Internet pour désigner le *www*.

[2] EUROPEAN COURT OF AUDITORS. *5G Roll-out in the EU : delays in deployment of networks with security issues remaining unresolved. Special report n° 03, 2022* [PDF]. Publications Office of the European Union (en ligne). 2022 [Consulté le 4 septembre 2022]. Disponible à l'adresse : https://data.europa.eu/doi/10.2865/337980

[3] MC KINSEY. *Notes from the AI frontier: Modelling the impact of AI on the world economy*. McKinsey Global Institute [en ligne]. 4 septembre 2018 [Consulté le 4 septembre 2022]. Disponible à l'adresse : https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-AI-frontier-modeling-the-impact-of-ai-on-the-world-economy

[4] KEMP, Simon. *Time spent with connected technologies*. Datareportal [en ligne]. 26 janvier 2022 [Consulté le 5 mai 2022]. Disponible à l'adresse : https://datareportal.com/reports/digital-2022-time-spent-with-connected-tech

[5] BRADSHOW, Samantha et HOWARD, N. Philip. *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation* [Working paper]. Oxford, UK: Project on Computational Propaganda. comprop.oii.ox.ac.uk. 26 septembre 2019. p. 3 [Consulté le 4 août 2022]. Disponible à l'adresse : https://digitalcommons.unl.edu/scholcom/207/

[6] Pour en savoir plus, consulter le Rapport 2022 *The Global Expansion of Authoritarian Rule* publié par la Freedom House à l'adresse : https://freedomhouse.org/report/freedom-world/2022/global-expansion-authoritarian-rule

[7] Donnée Datareportal : https://datareportal.com/reports/digital-2022-time-spent-with-connected-tech

[8] Les biais cognitifs des humains font qu'un internaute est plus enclin à lire et à relayer l'information partagée par une personne de son réseau que celle figurant sur le site internet de sa propre mairie.

[9] Les biais de certains algorithmes d'intelligence artificielle (IA) proviennent de l'utilisation de bases de données biaisées voire discriminatoires lors de la phase d'apprentissage du système IA. Exemple : le chatbot Tay de Microsoft : https://www.cbsnews.com/news/microsoft-shuts-down-ai-chatbot-after-it-turned-into-racist-nazi/ or l'application Visual AI de Google : https://www.wsj.com/articles/BL-DGB-42522

[10] Opérations d'influence, publicités « programmatiques », logiques algorithmiques. Voir Le rapport Bronner : BRONNER, Gérald. *Les Lumières à l'ère numérique* [PDF]. Vie publique [en ligne]. 12 février 2022 [Consulté le 4 septembre 2022]. Disponible à l'adresse : https://www.viepublique.fr/sites/default/files/rapport/pdf/283201.pdf

[11] CERVENNANSKY Marc. *L'extraordinaire pouvoir de manipulation des réseaux sociaux*. 8 mars 2018. [Consulté le 4 octobre 2022]. Disponible à l'adresse : https://www.cap-com.org/actualit%C3%A9s/lextraordinaire-pouvoir-de-manipulation-des-reseaux-sociaux

[12] ECONOMIST INTELLIGENCE. *Democracy Index 2021: The China challenge* [PDF]. EIU [en ligne]. 2022 [Consulté le 4 octobre 2022]. p. 4. Disponible à l'adresse : https://pages.eiu.com/rs/753-RIQ-438/images/eiu-democracy-index-2021.pdf

[13] Jamie Barlett, directeur du Centre d'analyse des réseaux sociaux chez Demos, met en avant une certaine corrélation entre le développement d'Internet et le déclin de la démocratie dans son livre *The People vs Techs : how Internet is Killing Democracy (and how to Save it)*. Ebury Press. 2018.

[14] En France, la Loi pour une République numérique de 2016 (art. 108) impose le maintien de la connexion Internet pour les plus démunis.

[15] Un wiper est un type de malware destructif, au mode opératoire d'autant plus complexe à analyser que le virus s'écrase lui-même, en même temps que les données qu'il efface. Le wiper supprime les données sans aucune possibilité de récupération, endommageant au passage les systèmes d'exploitation infectés, d'où le caractère destructeur.

[16] En 2013 l'analyste américain de la National Security Agency (NSA), Edward Snowden, dévoilait au monde entier certains projets de l'agence permettant aux Etats-Unis d'espionner ennemies et alliés : https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

[17] En 2016 lors des élections présidentielles américaines, du référendum pour le Brexit, et en 2017 lors des présidentielles françaises, les réseaux sociaux sont utilisés afin de manipuler l'opinion publique et de discréditer certains candidats.

[18] DEMCHAK, Chris C. et SHAVITT, Yuval. *China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking* [PDF). Military Cyber Affairs [en ligne]. 2018 [Consulté le 4 août 2022]. Vol. 3 : Iss. 1. Article 7. Disponible à l'adresse : https://digitalcommons.usf.edu/mca/vol3/iss1/7/

[19] Depuis 2016, le gouvernement chinois exploite les technologies digitales permettant la collecte de données biométriques afin de surveiller les activités et les déplacements des Ouïghours à travers les réseaux sociaux chinois, tel que WeChat. Ont ainsi été collectées des données tel que l'ADN, enregistrements de voix et empreintes faciales de toute la population du Xinjiang.

[20] Chiffres au premier trimestre 2022. https://datareportal.com/reports/digital-2022-july-global-statshot

[21] En 2020, 228 pays du monde étaient connectés à Internet.
WOODFORD, Chris. *The Internet*. ExplainThatStuff [en ligne]. 6 juillet 2021 [Consulté le 5 septembre 2022]. Disponible à l'adresse : https://www.explainthatstuff.com/internet.html

[22] Données avril 2022 : KEMP, Simon. *Digital 2022 : Global Overview Report*. Datareportal [en ligne]. 21 avril 2022 [Consulté le 3 septembre 2022]. Disponible à l'adresse : https://datareportal.com/reports/digital-2022-april-global-statshot

[23] *Idem.*

[24] KUZHELEVA-SAGAN, Irina P. et SUCHKOVA Natalya A. *Designing trust in the Internet services*. AI & Soc 31, 381–392 (2016) [Consulté le 3 mai 2022]. Disponible à l'adresse : https://link.springer.com/article/10.1007/s00146-015-0622-7

[25] WEIRENS, Jeffery et al. *New models for building digital trust*. Deloitte [en ligne]. 5 avril 2021 [Consulté le 4 mai 2022]. Disponible à l'adresse : https://www2.deloitte.com/us/en/insights/topics/digital-transformation/the-importance-of-digital-trust-qa.html
Traduction : *« La confiance humaine consiste à comprendre les motivations d'une personne et à croire qu'elle vous soutient. Vous pouvez anticiper ce qu'elle va faire. Vous savez pourquoi elle agit comme elle le fait. [...] C'est quelque chose qui est très souvent oublié lors de la construction de systèmes numériques. Les données en sont l'exemple le plus clair. Je vais vous fournir ce service, et ensuite, sans que ce soit vraiment clair, nous allons vendre vos données à côté. C'est une violation de la confiance. La conséquence est que si je ne comprends pas votre modèle économique, ce que vous me proposez et quelle est la valeur pour vous, je ne peux pas vous faire confiance. C'est cette transparence de la valeur, de la relation et des motivations qui est souvent laissée de côté lorsque les gens parlent de systèmes numériques. Et c'est, l'erreur fondamentale à bien des égards. Une rupture de cette compréhension est une assez bonne approximation des situations que j'ai vues où des questions de confiance se posent. »*

[26] STATISTA. *Europe trust in Internet*. Statista [en ligne]. Avril 2021 [Consulté le 4 mai 2022]. Disponible à l'adresse : https://www.statista.com/statistics/422787/europe-trust-in-the-internet-by-country/

[27] SMITH, Aaron et OLMSTEAD, Kenneth. *Declining Majority of Online Adults Say the Internet Has Been Good for Society*. Pew Research Centre [en ligne]. 30 avril 2018 [Consulté le 2 mai 2022]. Disponible à l'adresse : https://www.pewresearch.org/internet/2018/04/30/declining-majority-of-online-adults-say-the-Internet-has-been-good-for-society/

[28] Ce que le philosophe et économiste écossais Adam Smith appelle « la main invisible ». Source : https://www.britannica.com/topic/invisible-hand

[29] Sous le couvert d'une nécessaire « due diligence » vis-à-vis du contrôle de l'information, Tweeter et Facebook ont censuré une information du The New York Post qui mettait dans une mauvaise lumière le candidat Biden aux élections américaines de 2020. https://stanforddaily.com/2020/10/15/big-tech-v-democracy/

[30] Données 2021 : 59,8% des utilisateurs actifs mensuellement (MAU) âgées entre 16 et 64 ans de Facebook et 59,7% de ceux de Twitter, affirment utiliser les réseaux sociaux respectifs également

pour s'informer sur l'actualité et les évènements. Source : https://datareportal.com/reports/digital-2022-april-global-statshot

[31] Clipper était une puce de chiffrement développée et soutenue par NSA afin de sécuriser les messages voix et les données. La puce utilisait l'algorithme de chiffrement Skipjack classifié secret d'état - pour éviter toute analyse du code -, qui contenait une porte dérobée (*backdoor*).

[32] Suite à l'échec de la puce Clipper, l'Agence Américaine de Sécurité (National Security Agency – NSA) a essayé d'introduire le séquestre de clé (*key escrow*) - une politique selon laquelle tous les systèmes de chiffrement devaient laisser une clé de réserve à un "tiers de confiance" qui la remettrait au FBI sur demande.

[33] La faille de sécurité affectant les protocoles Secure Sockets Layer (SSL) et Transport Layer Security (TLS), était présente, entre autres, dans l'implémentation SSL d'Apple, l'ancien OpenSSL ou le packet Secure Channel (SChannel) de Microsoft. VAUGHAN-NICHOLS, Steven. *FREAK flaw: How to protect yourself now*. ZD NET [en ligne]. 6 mars 2015 [Consulté le 2 mars 2022]. Disponible à l'adresse https://www.zdnet.com/article/how-to-protect-yourself-against-freak/

[34] The Guardian affirme que « le financement du programme - 254,9 millions de dollars pour cette année [2013] - éclipse celui du programme Prism, qui fonctionne à un coût de 20 millions de dollars par an, selon de précédents documents de la NSA. Depuis 2011, les dépenses totales pour l'activation de Sigint ont dépassé les 800 millions de dollars ». BALL, James, BORGER, Julian et GREENWALD, Glenn. Revealed: how US and UK spy agencies defeat internet privacy and security. The Guardian [en ligne]. 6 septembre 2013 [Consulté le 2 mai 2022. Disponible à l'adresse : https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

[35] L'acharnement technologique n'est que le reflet de la transformation numérique du renseignement et de l'espionnage. Il faut dire que casser par des attaques de force brute avec des super ordinateurs les algorithmes de chiffrement d'Internet (HTTPS, voice-over-IP et Secure Sockets Layer, SSH), travailler secrètement avec des organismes de certification pour abaisser le niveau de sécurité des algorithmes dans les logiciels de chiffrement grand public, ou encore collaborer avec les géants technologiques pour installer des portes dérobées dans leur logiciels et application, était inhabituel dans les années 1990.

[36] Le GCHQ s'intéresse particulièrement à l''effort de décryptage. Habitué à faire des écoutes directes sur les câbles transatlantiques, les Britanniques voient cette acticité (le projet Tempora) mise en danger au fur et à mesure que de plus en plus de grandes sociétés Internet cryptent leur trafic, pour répondre à la demande de confidentialité de leurs clients. À horizon 2015, le plan prévoyait la compromission des codes utilisés par 15 grands fournisseurs d'internet et 300 VPN. BALL, James, BORGER, Julian et GREENWALD, Glenn. *Revealed: how US and UK spy agencies defeat internet privacy and security.* The Guardian [en ligne]. 6 septembre 2013 [Consulté le 2 mai 2022. Disponible à l'adresse : https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security Traduction : *« le prix à payer pour que les États-Unis conservent un accès et une utilisation sans restriction du cyberespace ».*

[37] BALL, James, BORGER, Julian et GREENWALD, Glenn. *Revealed: how US and UK spy agencies defeat internet privacy and security.* The Guardian [en ligne]. 6 septembre 2013 [Consulté le 2 mai 2022]. Disponible à l'adresse : https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

[38] TONAR, Remington. TALTON, Ellis. *Why Sidewalk Labs' Toronto Plan Is Flawed*. Forbes [en ligne]. 26 septembre 2019 [Consulté le 9 septembre 2022]. Disponible à l'adresse : https://www.forbes.com/sites/ellistalton/2019/09/26/why-sidewalk-labs-toronto-plan-is-flawed/

[39] ATLANTIK-BRÜCKE. *Vertrauen in der Krise. Landkarten geopolitischer Chancen und Risiken* [PDF]. Atlantik-Brücke. 2019 [Consulté le 5 mai 2022]. p. 17. Disponible à l'adresse: https://www.atlantik-bruecke.org/wp-content/uploads/AtlantikBrueckeUmfrage2019.pdf

[40] *Belt and Road Initiative* est la nouvelle route de la soie technologique et numérique chinoise.

[41] Le 8 avril 2010, China Telecom a détourné 15 % du trafic Internet pendant 18 minutes dans ce qui est considéré comme une expérience à grande échelle et une démonstration des capacités chinoises à contrôler les flux de l'internet. DEMCHAK, Chris C., SHAVITT, Yuval. *China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking*. Military Cyber Affairs [en ligne]. [PDF]. 2018. Vol. 3. Issue 1. p. 3. [Consulté le 3 mai 2022]. Disponible à l'adresse : https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1050&context=mca

[42] L'objectif est de faciliter le partage l'information entre les administrations, et mettre en place un mécanisme de récompenses et de sanctions. Elles concernent dans une grande majorité les entreprises : licence, historique juridique, déclarations fiscales. Pour ce qui est de la mise en place d'un mécanisme de récompenses et sanctions, le SCS permet de pénaliser une entreprise si elle est reconnue coupable par une administration compétente d'avoir enfreint les lois en vigueur. Elle est alors ajoutée sur liste noire et se voit appliquer des sanctions correspondantes. Ces sanctions incluent le plus souvent des restrictions pour l'accès aux financements ou aux marchés publics. Le système aurait été utilisé pour forcer les compagnies aériennes étrangères à appliquer la politique chinoise sur Taiwan. AFNIC et INSTITUT DE LA SUVERANITE NUMERIQUE. Internet des objets & souveraineté numérique [PDF]. Afnic [en ligne]. 2021 [Consulté le 4 mai 2022]. pp. 77-78. Disponible à l'adresse : https://www.afnic.fr/wp-media/uploads/2021/03/Rapport_IoT_ISN_Afnic.pdf

[43] BLOCH, Raphaël. *Amende record, règlementation... À quoi joue Pékin avec ses géants technologiques ?* L'Express [en ligne]. 27 avril 2021 [Consulté le 8 octobre 2022]. Disponible à l'adresse https://lexpansion.lexpress.fr/actualite-economique/amende-record-reglementation-a-quoi-joue-pekin-avec-ses-geants-technologiques_2149353.html

[44] AFNIC et INSTITUT DE LA SUVERANITE NUMERIQUE. Internet des objets & souveraineté numérique [PDF]. Afnic [en ligne]. 2021 [Consulté le 4 mai 2022]. p. 78. Disponible à l'adresse : https://www.afnic.fr/wp-media/uploads/2021/03/Rapport_IoT_ISN_Afnic.pdf

[45] DEMCHAK, Chris et SHAVITT, Yuval. *China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking* [PDF]. Military Cyber Affairs. Juin 2018 [Consulté le 5 juin 2022]. Volume 3. Issue 1. Article 7. p. 1. Disponible à l'adresse : https://www.researchgate.net/publication/328435903_China's_Maxim_-_Leave_No_Access_Point_Unexploited_The_Hidden_Story_of_China_Telecom's_BGP_Hijacking
Un Point of Presence (PoP) est un point de connexion majeur où un opérateur de télécommunications longue distance, tel que Verizon ou British Telecom se connecte à un réseau local et récupère le trafic local - ou trafic de transit - pour le faire progresser vers ses différentes destinations.

[46] Pour des exemples de détournements du trafic Internet et les techniques utilisées, consulter DEMCHAK, Chris et SHAVITT, Yuval. *China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking* [PDF]. Military Cyber Affairs. Juin 2018 [Consulté le 5 juin 2022]. Volume 3. Issue 1. Article 7. p. 1. Disponible à l'adresse : https://www.researchgate.net/publication/328435903_China's_Maxim_-_Leave_No_Access_Point_Unexploited_The_Hidden_Story_of_China_Telecom's_BGP_Hijacking

[47] ASS-SECURITY. *Classement mondial [2020] des 25 entreprises leader de la sécurité électronique*. Ass-security.fr [en ligne]. 18 mars 2020 (Consulté le 23 mai 2022]. Disponible à l'adresse : https://www.ass-security.fr/blog/classement-25-entreprises-securite-electronique/

[48] Le 8 avril 2010, China Telecom a détourné 15 % du trafic Internet pendant 18 minutes dans ce qui est considéré comme une expérience à grande échelle et une démonstration des capacités chinoises à contrôler les flux de l'internet. DEMCHAK, Chris C., SHAVITT, Yuval. *China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking*. Military Cyber Affairs [en ligne]. [PDF]. 2018. Vol. 3. Issue 1. p. 3. [Consulté le 3 mai 2022]. Disponible à l'adresse : https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1050&context=mca

[49] SNOWDEN ,Edward. *"This Will Change Everything, It Already Started".* YouTube. Mars 2022 [Consulté le 5 novembre 2022]. Disponible à l'adresse : https://youtu.be/ouKhLf6PbSA

[50] CAVE, Danielle. et al. *Maping China's Tech Giants* [PDF]. Australian Strategic Policy Institute. Report 15/2019 [Consulté le 4 novembre 2022]. p. 19. Disponible à l'adresse : https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2019-05/Mapping%20China%27s%20technology%20giants.pdf?VersionId=EINwiNpste_FojtgOPriHtlFSD2OD2tL
Traduction : *« Les entreprises chinoises vont continuer à jouer un rôle vital dans la manière dont les gouvernements, les entreprises et les citoyens du monde entier se connectent les uns aux autres. Dans le même temps, cependant, il est important de reconnaître que les activités de ces entreprises ne sont pas simplement commerciales et que, dans certaines circonstances, une analyse des risques est nécessaire. Les politiques et déclarations officielles du CCP montrent clairement que celui-ci perçoit l'expansion des entreprises technologiques chinoises comme un élément crucial de son projet*

plus vaste d'expansion idéologique et géopolitique. Les comités du PCC au sein des entreprises technologiques et les liens étroits (que ce soit par la propriété directe, les obligations légales ou des accords de financement, y compris des prêts et des contrats lucratifs) entre les entreprises et le gouvernement chinois, rendent difficile une posture neutre, même si certaines entreprises pourraient bien le vouloir. Il est également légitime de se demander si les consommateurs mondiaux devraient exiger une surveillance plus approfondie des entreprises technologiques chinoises qui enfreignent les droits de l'homme en Chine et ailleurs. Les gouvernements du monde entier ont du mal à évaluer les implications politiques et sécuritaires d'une collaboration avec les entreprises chinoises, en particulier dans des domaines tels que les infrastructures critiques, par exemple dans la 5G, et dans les partenariats de recherche collaborative qui pourraient impliquer des technologies sensibles ou dual-use. Une partie de cette difficulté est due à un manque de compréhension approfondie de l'environnement parti-état unique qui façonne, limite et détermine le comportement des entreprises chinoises dans le monde. »

[51] C'est le même modus operandi utilisé dans sa politique d'expansion et d'influence au Levant, en Afrique et en Ukraine : faire appel aux mercenaires, à l'exemple du groupe Wagner.

[52] BURT, Tom. *The hybrid war in Ukraine*. Blogs Microsoft [en ligne]. 27 avril 2022 [Consulté le 5 mai 2022]. Disponible à l'adresse : https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/
Traduction : « *Les attaques n'ont pas seulement détérioré les systèmes des institutions en Ukraine mais ont également visé la perturbation de l'accès par la population à une information fiable et aux services vitaux dont dépendent les civils, et ont tenté d'ébranler la confiance envers les dirigeants du pays. Nous avons également observé des activités limitées d'espionnage impliquant des États membres de l'OTAN, ainsi que des activités de désinformation.* »

[53] Source : https://www.phonandroid.com/un-pirate-pro-ukraine-devoile-les-messages-prives-des-hackers-derriere-le-ransomware-conti.html

[54] Source : https://news.sky.com/story/could-the-russian-cyber-attack-on-lithuania-draw-a-military-response-from-nato-12641986

1.2. L'Europe victime de sa diversité et de ses dépendances

[55] EUROPEAN COMMISSION. *Growth, Competitiveness, and Employment. The Challenges and Ways Forward into the 21st Century.* EC [en ligne]. [93) 700 final, 5 décembre 1993 [Consulté le 4 octobre 2022]. Disponible à l'adresse : https://op.europa.eu/en/publication-detail/-/publication/4e6ecfb6-471e-4108-9c7d-90cb1c3096af *et* BANGEMANN GROUP. *Report on Europe and the Global information Society.* Bulletin of the European Union [en ligne], Supplement 2/94. 1994 [Consulté le 4 octobre 2022]. Disponible à l'adresse : https://cordis.europa.eu/article/id/2730-bangemann-report-europe-and-the-global-information-society
Ces deux documents contenaient déjà l'idée que les technologies de l'information et de la communication ne profiteraient à l'économie que si elles étaient articulées de manière cohérente et intégrées aux secteurs d'activité historiques.

[56] EUROPEAN COMMISSION. *Domaines d'action de l'UE*. EC [en ligne]. [Consulté le 4 octobre 2022]. Disponible à l'adresse : https://ec.europa.eu/info/about-european-commission/what-european-commission-does/law/areas-eu-action_fr

[57] EUROPEAN COMMISSION. *Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime* [PDF]. EC (en ligne]. (2000)890 final. 26 janvier 2001 [Consulté le 4 mai 2022]. Disponible à l'adresse : https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0890:FIN:EN:PDF

[58] COUNCIL OF THE EUROPEAN UNION AND EUROPEAN COMMISSION. *eEurope 2002, An Information Society for All- Action Plan. 14 juin 2000 [Consulté le 4 mai 2022]. Disponible à l'adresse :* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum%3Al24221 *et*
COMMISSION OF THE EUROPEAN COMMUNITIES. Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime. EC [en ligne].

(2000) 890 final. 26 janvier 2001 [Consulté le 5 mai 2022]. Disponible à l'adresse : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52000DC0890

[59] EUROPEAN COMMISSION. *Communication from the Commission to the Council and the European Parliament: Critical Infrastructure Protection in the Fight Against Terrorism*. EC [en ligne]. (2004) 702 final, 20 octobre 2004 [Consulté le 5 mai 2022]. Disponible à l'adresse : https://www.eumonitor.eu/9353000/1/j4nvhdfcs8bljza_j9vvik7m1c3gyxp/vikqh28p0xxf

[60] COUNCIL OF THE EUROPEAN UNION. *Council Framework Decision on Attacks against Information Systems*. Official Journal of the European Union [en ligne]. L 69/67, 16 mars 2005 [Consulté le 5 mai 2022]. Disponible à l'adresse : http://data.europa.eu/eli/dec_framw/2005/222/oj

[61] *Idem*.

[62] EUROPEAN COMMISSION. C*ommunication from the Commission to the European Council of June 2006: Europe in the World- Some Practical Proposals for Greater Coherence, Effectiveness and Visibility.* European Commission [en ligne]. 278 final, 8 juin 2006 [Consulté le 4 mai 2022]. pp. 6-9. Disponible à l'adresse : https://op.europa.eu/en/publication-detail/-/publication/3431857c-69e0-4211-n8b95-c14a078e515c/language-en

[63] Données ENISA 2019. Source : *https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/eu-ict-industry-consultation-paper*

[64] TERRASSON, Benjamin. *Microsoft et les institutions européennes : des dysfonctionnements dangereux.* Siècle Digital [en ligne]. 9 juillet 2020 [Consulté le 5 septembre 2022]. Disponible à l'adresse : https://siecledigital.fr/2020/07/09/microsoft-et-les-institutions-europeennes-des-dysfonctionnements-dangereux/

[65] Données 2019. *Top 100 Digital companies*. Forbes [en ligne] : https://www.forbes.com/top-digital-companies/list/#tab:rank

[66] Données 2009. *Les cinq principaux équipementiers télécoms du monde*. Les Echos [en ligne] : https://investir.lesechos.fr/actu-des-valeurs/la-vie-des-actions/encadre-les-cinq-principaux-equipementiers-telecoms-du-monde-1601706

[67] TAZROUT Zacharie. *L'Union européenne accuse un retard conséquent en matière d'intelligence artificielle et de blockchain*. Actuia.com [en ligne]. 3 juin 2021 [Consulté le 7 septembre 2022]. Disponible à l'adresse : https://www.actuia.com/actualite/lunion-europeenne-accuse-un-retard-consequent-en-matiere-dintelligence-artificielle-et-de-blockchain/

[68] KAPKO, Matt. *Hyperscalers Surpass 700 Data Centers Globally*. SDXCentral.com [en ligne]. 21 novembre 2021 [Consulté le 4 octobre 2022]. Disponible à l'adresse : https://www.sdxcentral.com/articles/news/hyperscalers-surpass-700-data-centers-globally/2021/11/

[69] GASNIER, Jean-Pierre. *Que fait l'Europe pour le numérique ?* Linkedin [en ligne]. 10 mai 2019. [Consulté le 5 août 2022]. Disponible à l'adresse : https://www.linkedin.com/pulse/que-fait-leurope-pour-le-num%C3%A9rique-jean-pierre-gasnier/

[70] PINEDA Julett. *Which companies have pulled out of Russia?* Deutsche Welle [en ligne]. 30 octobre 2022 [Consulté le 12 novembre 2022]. Disponible à l'adresse : https://www.dw.com/en/which-companies-have-pulled-out-of-russia-over-the-ukraine-invasion/a-61078955

[71] *L'Otan en état de "mort cérébrale" juge Emmanuel Macron*. TV5 Monde [en ligne]. 8 novembre 2019. Disponible à l'adresse : https://information.tv5monde.com/info/l-otan-en-etat-de-mort-cerebrale-juge-emmanuel-macron-331037

[72] *La volonté d'autonomie de l'UE inquiète l'OTAN*. L'Express (en ligne]. 4 mars 2021 [Consulté le 5 mai 2022].Disponible à l'adresse : https://www.lexpress.fr/actualites/1/monde/la-volonte-d-autonomie-de-l-ue-inquiete-l-otan_2146137.html

[73] L'initiative de la stratégie est le fruit d'un effort combiné entre la Commissaire à l'intérieur de l'époque, Cecilia Malmström (Suède), la haute représentante Catherine Ashton (Royaume-Uni) et la commissaire de la DG Connect, Neelie Kroes (Pays-Bas) soutenues par la DG JUST.

[74] COMMISSION EUROPEENNE. *Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé* [PDF]. CE [en ligne]. 7 février 2013 [Consulté le 4 octobre 2022]. p. 21. Disponible à l'adresse : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52013JC0001&from=FR

[75] COMMISSION EUROPEENNE. *EU grants nearly €49 million to boost innovation in cybersecurity and privacy systems*. EC [en ligne]. 20 mai 2020 [Consulté le 5 juin 2022]. Disponible à l'adresse : https://digital-strategy.ec.europa.eu/en/news/eu-grants-nearly-eu49-million-boost-innovation-cybersecurity-and-privacy-systems

[76] PUGLIERIN Jana et ZERKA Pawel. *European Sovereignity Index* [PDF]. European Council on Foreign Relations [en ligne]. Juin 2022 [Consulté le 5 août 2022]. Disponible à l'adresse : https://ecfr.eu/special/sovereignty-index/#terrain-technology

[77] *Idem*.

[78] EUROPEAN COMMISSION. *The EU's Cybersecurity Strategy for the Digital Decade* [PDF]. EC [en ligne]. 16 décembre 2020 [Consulté le 3 mai 2022]. p. 1263. Disponible à l'adresse : https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

[79] Source : https://contractfortheweb.org/about/
Traduction : « *Le web a été conçu pour rassembler les gens et rendre les connaissances librement accessibles. Ça changé le monde pour de bon et amélioré la vie de milliards de personnes. […] Chacun a un rôle à jouer pour que le web serve l'intérêt général*. »

2. UNE COORDINATION INSTITUTIONNELLE À DIFFÉRENTES ÉCHELLES

2.1. Une coordination verticale complexe

[1] CARRAPICO, Helena et BARRINHA, André. *The EU as a Coherent (Cyber)Security Actor ?* [PDF]. Journal of Common Market Studies [en ligne]. 10 mai 2017 [Consulté le 4 mai 2022]. Disponible à l'adresse : https://doi.org/10.1111/jcms.12575

[2] INTERNATIONAL TELECOMMUNICATIONS UNION. *Global Cybersecurity Index 2020* [PDF]. ITU [en ligne]. 2020 [Consulté le 4 mai 2022]. pp. 3-21. Disponible à l'adresse : https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

[3] Outre les autorités nationales chargées de la cybersécurité et les organismes internationaux tels que le Conseil de l'Europe, les principaux acteurs de la cybersécurité sont les suivants : DG Migration and Home Affairs (cybercrime), le European Cybercrime Centre (EC3) (cybercrime), le European External Action Service (cyber defense), la European Defense Agency (EDA) (cyber défense), la DG for Communications Networks, Content and Technology (sécurité des systèmes d'information), la European Network and Information Security Agency (ENISA) (sécurité des systèmes d'information), les Computer Emergency Response Teams (CERTs) (cybercrime) et les équipes d'intervention en cas d'urgence informatique (CERT) (cybercriminalité).

[4] Des entretiens menés avec des fonctionnaires européens et nationaux à Bruxelles par Helena Carrapico et André Barrinha ont confirmé la place de plus en plus centrale qu'occupe la cybersécurité dans les discussions politiques. CARRAPICO, Helena et BARRINHA, André. *The EU as a Coherent (Cyber)Security Actor ?* [PDF]. Journal of Common Market Studies [en ligne]. 10 mai 2017 [Consulté le 4 mai 2022]. p. 1264. Disponible à l'adresse : https://doi.org/10.1111/jcms.12575

[5] « Les vides juridiques et les différences considérables présentées par les législations des États membres dans ce domaine peuvent freiner la lutte contre la criminalité organisée et le terrorisme et peuvent compliquer une coopération policière et judiciaire efficace en cas d'attaques contre les systèmes d'information. » *Council Framework Decision 2005/222/JHA of 24 February* 2005 *on attacks against information systems*. OJ [en ligne]. L69. 16 mars 2005 [Consulté le 4 mai 2022]. p. 1. Disponible à l'adresse : http://data.europa.eu/eli/dec_framw/2005/222/oj

[6] Entretien avec Anne Tricaud, juillet 2022.

[7] *Council Framework Decision 2005/222/JHA of 24 February* 2005 *on attacks against information systems*. OJ [en ligne]. L 69. 16 mars 2005 [Consulté le 4 mai 2022]. pp. 67-68. Disponible à l'adresse : http://data.europa.eu/eli/dec_framw/2005/222/oj

[8] ENISA : https://www.enisa.europa.eu/about-enisa/about/fr

[9] Le réseau des CSIRTs (Computer Security Response Incident Team) est un réseau composé des CSIRTs désignés par les États membres de l'UE et du CERT-EU ("membres du réseau des CSIRTs"). La Commission européenne participe au réseau en tant qu'observateur. L'ENISA est chargée de soutenir activement la coopération des CSIRTs, de fournir le secrétariat et le soutien actif pour la coordination des incidents sur demande. Le réseau CSIRTs fournit un forum où les membres peuvent coopérer, échanger des informations et instaurer la confiance.

[10] CyCLONe (Cyber Crisis Liaison Organisation Network) vise à contribuer à la mise en œuvre du plan d'action non contraignant de la Commission européenne de réponse en cas d'incident cyber d'ampleur ou de crise transfrontalière.

[11] NIS Cooperation Group (The Network and Information Systems Cooperation Group) a été créé par la Directive NIS pour assurer la coopération et l'échange d'informations entre les États membres.

[12] *The Cybersecurity Strategy*. European Commission [en ligne]. 2013 [Consulté le 4 mai 2022]. Disponible à l'adresse : https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

[13] Anne Tricaud, Cheffe de la Division internationale de l'ANSSI pendant la Présidence française.

[14] KRASTEV, Ivan et LEONARD, Marc. *What Europeans think about the US-China Cold War* [PDF]. ECFR. 21 septembre 2021 [Consulté le 5 mai 2022]. p. 3. Disponible à l'adresse : https://ecfr.eu/wp-content/uploads/What-Europeans-think-about-the-US-China-Cold-War-2.pdf

Traduction : *« Les citoyens sont plus susceptibles de croire qu'une nouvelle guerre froide sera menée par Bruxelles et Washington plutôt que par Paris et Berlin, ou Varsovie, Rome et Madrid »*

[15] Source : https://www.politico.eu/article/eu-slams-china-as-systemic-rival-as-trade-tension-rises/

[16] WOOD, Maria. *What the People of Other NATO Countries Think About America*. The Wall St 24/7 [en ligne]. 1 avril 2022 [Consulté le 5 mai 2022]. Disponible à l'adresse : https://247wallst.com/special-report/2022/04/01/what-every-nato-nation-thinks-about-america/#

[17] BUSSIÈRE, Cammile. *Europe de la cyberdéfense – Nouvelles technologies*. Nouvelles du Jour [en ligne]. 8 mai 2022 [Consulté le 2 août 2022]. Disponible à l'adresse : https://nouvelles-dujour.com/europe-de-la-cyberdefense-nouvelles-technologies/

[18] Source : https://www.euractiv.com/section/cybersecurity/news/german-eu-presidency-pushes-for-cybersecurity-by-design-in-connected-devices/

[19] Source : https://presidence-francaise.consilium.europa.eu/media/c2tgcx2w/dp-bilan-de-la-pr%C3%A9sidence.pdf

[20] EUROPEAN PARLIAMENT. *MEPs adopt Cybersecurity Act and want EU to counter IT threat from China*. EP [en ligne]. 12 mars 2019 [Consulté le 5 mai 2022]. Disponible à l'adresse : https://www.europarl.europa.eu/news/en/press-room/20190307IPR30694/meps-adopt-cybersecurity-act-and-want-eu-to-counter-it-threat-from-china

[21] Proposition de Résolution Européenne du Sénat français du 9 décembre 2017. Source : https://www.senat.fr/leg/ppr17-079.html

[22] Nous y reviendrons dans le Chapitre 3.

[23] La *Directive NIS* a été votée avec un vote favorable à l'unanimité. Source : Conseil de l'UE : https://data.consilium.europa.eu/doc/document/ST-9206-2016-INIT/fr/pdf

[24] *Cybersecurity Act* : https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0881

[25] Carte 2019 téléchargeable à l'adresse : https://www.ihemi.fr/articles/organisation-france-europe-cybersecurite-cyberdefense-V2

[26] BOTHOREL, Eric. *Rapport d'information déposé par la Commission des affaires européennes sur l'avenir de la cybersécurité européenne* [PDF]. Assemblée Nationale. p. 32. Disponible à l'adresse : https://www.assemblee-nationale.fr/dyn/15/rapports/due/l15b2415_rapport-information.pdf
Tandis que le CCN et le CNPIC ont sous leur autorité un centre de réponse d'urgence – le CCN-CERT – responsable des opérateurs de services essentiels publics, l'INCIBE- CERT, sous l'autorité du CNPIC et du SESIAD, assure cette mission pour les opérateurs de services essentiels appartenant au secteur privé.

[27] Donnée Commission Européenne : https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-competence-centre

[28] AFP. *Face à la recrudescence des attaques, l'Agence européenne de cybersécurité veille*. Courrier International [en ligne]. 10 novembre 2021 [Consulté le 4 mai 2022]. Disponible à l'adresse : https://www.courrierinternational.com/depeche/face-la-recrudescence-des-attaques-lagence-europeenne-de-cybersecurite-veille.afp.com.20211110.doc.9rc328.xml

[29] BSI. Données 2021 : https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Presse/BSI-Kurzprofil.pdf?__blob=publicationFile&v=4

[30] COUR DES COMPTES EUROPEENNE. *Défis à relever pour une politique de l'UE efficace dans le domaine de la cybersécurité* [PDF]. ECA [en ligne]. Mars 2019 [Consulté le 4 mai 2022]. p. 20. Disponible à l'adresse : https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_FR.pdf
Les dépenses de cybersécurité inscrites au budget du gouvernement fédéral américain pour 2019 s'élevaient à environ 15 milliards de dollars (plus de 22 milliards pour 2023) alors que la France annonce un budget d'un milliard d'euros pour 2023 et l'Allemagne 13 milliards d'euros.

[31] *Ibid.*

[32] EUROPEAN COURT OF AUDITORS. *Challenges to effective EU cybersecurity policy* [PDF]. ECA. Mars 2019 [Consulté le 5 mai 2022]. p. 24. Disponible à l'adresse : https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

[33] CARRAPICO, Helena et BARRINHA, André. *The EU as a Coherent (Cyber)Security Actor ?* [PDF]. Journal of Common Market Studies [en ligne]. 10 mai 2017 [Consulté le 4 mai 2022]. p. 1264. Disponible à l'adresse : https://doi.org/10.1111/jcms.12575

Traduction : « *Il y a des problèmes de coordination entre, mais aussi au sein des institutions, qui sont liés à l'évolution historique des différents domaines de cybersécurité, ainsi qu'à la perception que chaque domaine connaît encore des défis distincts différents. Il n'est pas rare de trouver des projets dont les objectifs sont en conflit à ceux d'autres institutions (Entretien, Parlement européen, 2016). En outre, les États, à travers le Conseil, semblent être plus réticents que d'autres institutions (comme le Parlement européen) à renforcer les pouvoirs de l'UE dans ce domaine (Entretien, CERT-EU, 2016)* ».

[34] EUROPEAN CYBER SECURITY ORGANISATION. *ECS cPPP Progress Monitoring Report 2016-2017* [PDF]. 29 octobre 2018 [Consulté le 5 avril 2022]. Disponible à l'adresse : https://www.ecs-org.eu/documents/uploads/progress-monitoring-report-2016-2017.pdf

[35] COMMISSION EUROPÉENNE. *Industrie de la défense : l'UE prend des mesures pour investir près de 1,2 milliard d'euros dans 61 projets de coopération industrielle dans le domaine de la défense* [CP]. CE [en ligne]. 20 juillet 2022. Disponible à l'adresse : https://ec.europa.eu/commission/presscorner/detail/fr/IP_22_4595

[36] *Audition du général de division aérienne Didier Tisseyre à l'Assemblée Nationale le 4 mars 2020*. Assemblée Nationale [en ligne]. 4 mars 2020 [Consulté le 5 mai 2022]. Compte rendu n° 40. Disponible à l'adresse : https://www.assemblee-nationale.fr/dyn/15/comptes-rendus/cion_def/l15cion_def1920040_compte-rendu.pdf

[37] EUROPEAN COURT OF AUDITORS. *Challenges to effective EU cybersecurity policy* [PDF]. ECA. Mars 2019 [Consulté le 5 mai 2022]. p. 31. Disponible à l'adresse : https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

[38] Liste des projets Open RAN actifs en 2021 disponible à l'adresse : https://www.ookla.com/articles/5g-europe-mapping-the-future-q1-2022

[39] Les géants américains du logiciel jouent un rôle croissant dans le secteur des communications mobiles. Google aurait un Mobile Core dans son portefeuille, Microsoft a racheté Affirmed Networks en mars 2020 et Metaswitch Networks en mai 2020. Par ailleurs, l'initiative Open RAN a été fortement stimulée par Facebook. Après avoir perdu tous les fournisseurs traditionnels du secteur de la téléphonie mobile il y a plusieurs années, les États-Unis recommencent à pénétrer le marché de la téléphonie mobile, et de manière encore plus forte. Les entreprises américaines de logiciels ont reconnu très tôt cette désagrégation entre logiciel et matériel et ont saisi les opportunités. L'évolution du secteur de la téléphonie mobile est évidente au quotidien : de plus en plus de personnes passent des appels vocaux via Facebook (appel WhatsApp), Apple (FaceTime), Microsoft (Skype), etc. Source : https://www.serentschy.com/mobile-operators-in-the-vendor-dilemma/

[40] Aux Pays-Bas, Huawei a sous-enchéri en 2019 de 60 % par rapport à la société suédoise Ericsson pour fournir des équipements de réseau pour le réseau 5G KPN. Source : https://www.washingtonpost.com/world/national-security/for-huawei-the-5g-play-is-in-europe--and-the-us-is-pushing-hard-for-a-ban-there/2019/05/28/582a8ff6-78d4-11e9-b7ae-390de4259661_story.html

[41] EUROPEAN COMMISSION. *The EU and China signed a key partnership on 5G, our tomorrow's communication networks*. EC [en ligne]. 28 septembre 2015 [Consulté le 3 mai 2022]. Disponible à l'adresse : https://ec.europa.eu/commission/presscorner/detail/en/IP_15_5715

[42] *PRC National Intelligence Law*. China LawTranslate [en ligne]. 27 juin 2017 [Consulté le 5 mai 2022]. Disponible à l'adresse : https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/

[43] EUROPEAN PARLIAMENT. *Security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them* [PDF]. Europarliament [en ligne] P8_TA(2019)0156. 2019 [Consulté le 5 mai 2022]. Disponible à l'adresse : https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_EN.pdf

[44] HUAWEI. *Investment and Holding. Annual Report 2021* [PDF]. 2021 [Consulté le 4 mai 2022]. Disponible à l'adresse : https://www-file.huawei.com/minisite/media/annual_report/annual_report_2021_en.pdf?version=0401

[45] Les opérateurs américains ont dû débourser 2,7 milliards de dollars pour les fréquences 5G, sommes similaires aux montants français et presque trois fois supérieures à ceux de l'Allemagne et de l'Italie.

[46] GILLEY, Bruce. *Huawei' Fixed Line to Beijing* [PDF]. Far Eastern Economic Review.28 décembre 2000-4 janvier 2001 [Consulté le 4 mai 2022]. Disponible à l'adresse : https://web.pdx.edu/~gilleyb/Huawei_FEER28Dec2000.pdf

[47] NAKASHIMA, Ellen. *U.S. pushes hard for a ban on Huawei in Europe, but the firm's 5G prices are nearly irresistible*. The Washington Post [en ligne]. 29 mai 2019 [Consulté le 22 août]. Disponible à l'adresse : https://www.washingtonpost.com/world/national-security/for-huawei-the-5g-play-is-in-europe--and-the-us-is-pushing-hard-for-a-ban-there/2019/05/28/582a8ff6-78d4-11e9-b7ae-390de4259661_story.html

[48] NAKASHIMA, Ellen. *U.S. pushes hard for a ban on Huawei in Europe, but the firm's 5G prices are nearly irresistible*. The Washington Post [en ligne]. 29 mai 2019 [Consulté le 22 août]. Disponible à l'adresse : https://www.washingtonpost.com/world/national-security/for-huawei-the-5g-play-is-in-europe--and-the-us-is-pushing-hard-for-a-ban-there/2019/05/28/582a8ff6-78d4-11e9-b7ae-390de4259661_story.html

[49] Pour le Cloud certifié au niveau substanciel les exigences de la brique 5C de la BSI allemande ont servi comme source d'inspiration. Pour le niveau élevé, en revanche, c'est le référenciel de certification français SecNumCloud qui a servi de modèle ; celui-ci formule des exigences afin de limiter l'impact des lois d'extra-territorialité.

[50] SADMI, Franck. *Cybersecurity Act* [podcast]. NoLimitSécu.fr [en ligne]. 2022. Épisode 345. [Consulté le 16 août 2022]. Disponible à l'adresse : https://www.nolimitsecu.fr/cybersecurity-act/

2.2. Une coopération transversale inégale

[51] Source : European Consilium : https://data.consilium.europa.eu/doc/document/ST-8377-2019-INIT/fr/pdf

[52] ITRE : Commission de l'industrie, de la recherche et de l'énergie.

[53] Lorsque le Conseil de l'UE est appelé à acter suite à une proposition de la CE ou du Haut Représentant, la majorité qualifiée est nécessaire pour l'adoption. Cela signifie que 55% de EM ont voté en faveur (15 pays) et que ces pays représentent au moins 65% de la population européenne. Source Conseil de l'UE : https://data.consilium.europa.eu/doc/document/ST-8377-2019-INIT/fr/pdf

[54] HERMANN, Vincent. *Au Sénat, vives oppositions au projet d'agence européenne de cybersécurité toute-puissante*. NextImpact [en ligne]. 22 novembre 2017 [Consulté le 5 juillet 2022]. Disponible à l'adresse : https://www.nextinpact.com/article/27621/105662-au-senat-vives-oppositions-au-projet-dagence-europeenne-cybersecurite-toute-puissante

[55] EUROPOL. *Internet Organised Crime Threat Assessment*. 2017

[56] EUROPEAN COURT OF AUDITORS. *Challenges to effective EU cybersecurity policy* [PDF]. ECA. Mars 2019 [Consulté le 5 mai 2022]. p. 9. Disponible à l'adresse : https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

[57] *Idem*. Les coûts peuvent inclure : la perte de revenus, les coûts de réparation des systèmes endommagés, les responsabilités potentielles en cas de vol d'actifs ou d'informations, les incitations à la fidélisation des clients, la hausse des primes d'assurance, l'augmentation des coûts de protection (nouveaux systèmes, employés, formation), le règlement potentiel des coûts de conformité ou des litiges.

[58] AON. *2020 Cyber Security Risk Report* [PDF]. AON. 2021 [Consulté le 5 avril 2022]. pp. 3-10. Disponible à l'adresse : https://insights-north-america.aon.com/cyber/2020-cyber-security-risk-report

[59] SOPHOS. T*he State of Ransomware 2021* [PDF]. Sophos. Avril 2021 [Consulté le 4 mai 2022]. p. 9. Disponible à l'adresse : https://assets.sophos.com/X24WTUEQ/at/k4qjqs73jk9256hffhqsmf/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469

[60] RIEB-MARCHIE, Valéry. *Reconnaissance mutuelle des certificats de sécurité entre France et Allemagne*. Lemag IT [en ligne]. 15 juin 2022. [Consulté le 8 août 2022]. Disponible à l'adresse : https://www.lemagit.fr/actualites/252521561/Reconnaissance-mutuelle-des-certificats-de-securite-entre-France-et-AllemagneEuropean Union Agency for Cybersecurity

[61] Le Groupe de coopération NIS est composé de représentants des États membres de l'UE, de la Commission européenne et de l'ENISA. La présidence est occupée par l'État membre exerçant la

présidence du Conseil de l'Union européenne. Chaque État membre de l'UE a désigné un point de contact unique sur la sécurité des réseaux et des systèmes d'information qui est chargé d'assurer la coopération transfrontalière avec les autres États membres et avec le groupe de coopération

[62] EUROPOL. *Internet Organised Crime Threat Assessment*. 2017

[63] EUROPEAN COURT OF AUDITORS. *Challenges to effective EU cybersecurity policy* [PDF]. ECA. Mars 2019 [Consulté le 5 mai 2022]. p. 9. Disponible à l'adresse : https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

[64] *Idem*. Les coûts peuvent inclure : la perte de revenus, les coûts de réparation des systèmes endommagés, les responsabilités potentielles en cas de vol d'actifs ou d'informations, les incitations à la fidélisation des clients, la hausse des primes d'assurance, l'augmentation des coûts de protection (nouveaux systèmes, employés, formation), le règlement potentiel des coûts de conformité ou des litiges.

[65] AON. *2020 Cyber Security Risk Report* [PDF]. AON. 2021 [Consulté le 5 avril 2022]. pp. 3-10. Disponible à l'adresse : https://insights-north-america.aon.com/cyber/2020-cyber-security-risk-report

[66] SOPHOS. T*he State of Ransomware 2021* [PDF]. Sophos. Avril 2021 [Consulté le 4 mai 2022]. p. 9. Disponible à l'adresse : https://assets.sophos.com/X24WTUEQ/at/k4qjqs73jk9256hffhqsmf/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469

[67] Bien que 3GPP se veut un organisme de certification réunissant plus de 600 organisations privées et des milliers des délégués, il se différencie des autres organismes par sa haute technicité et volonté d'assurer l'équité car, en effet, il n'a pas de comité directeur. Les décisions sont prises à l'unanimité seulement, par consensus, pas de vote ni de majorité, en sachant que les ingénieurs participants et les entreprises qu'ils représentent ont, en théorie, intérêt à voter pour des normes efficaces qui seront utilisées globalement. Tous les travaux et réunions sont ouverts au public et se font en toute transparence.

[68] Ericsson avait seulement 3% du marché chinois de la 5G et Nokia 1%[68] en 2021. Source : https://www.lesechos.fr/tech-medias/hightech/5g-nokia-et-ericsson-toujours-a-la-peine-sur-le-marche-chinois-1336674

[69] CAVE Danielle, et al. *Mapping China's technology giants*. ASPI [en ligne]. 2019. Report No. 15 [Consulté le 17 Septembre 2022]. p. 3. Disponible à l'adresse :https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2019-05/Mapping%20China%27s%20technology%20giants.pdf?VersionId=EINwiNpste_FojtgOPriHtlFSD2OD2tL

[70] La Chine a doublé sa participation à la 5G par rapport au lancement de la 3G et de la 4G.

[71] EKHOLM, Börje. *La 5G en Europe : il est temps de reconnaître les faits*. Ericsson [en ligne]. 25 mars 2020. [Consulté le 13 août 2022]. Disponible à l'adresse : https://www.ericsson.com/fr/blog/2019/12/5G-Europe-reconnaitre-les-faits

[72] NOKIA CORP. *Nokia reaches 4,000 5G essential patent families milestone*. Global Newswire [en ligne]. 11 novembre 2021. [Consulté le 13 juillet 2022]. Disponible à l'adresse : https://www.globenewswire.com/news-release/2021/11/11/2332220/0/en/Nokia-reaches-4-000-5G-essential-patent-families-milestone.html

[73] YANG, Guang. *Who Are the Leading Players in 5G Standardization?* [PDF]. Strategy Analytics [en ligne]. Mars 2020. p. 9. [Consulté le 4 août]. Disponible à l'adresse : https://www.strategyanalytics.com/access-services/service-providers/networks-and-service-platforms/reports/report-detail/who-are-the-leading-players-in-5g-standardization-an-assessment-for-3gpp-5g-activities?slid=2386935&spg=1

L'audit a été fait à la demande du Ministère Fédéral des Affaires Economiques et de l'Energie allemand (BMWi). Strategy Analytics précise que le nombre de contributions n'est pas un indicateur représentatif de leadership au sein de 3GPP car beaucoup de contributions n'apportent pas de solution technologique innovante. En effet, La Chine est reconnue pour le grand nombre de contributions qui, en réalité, ne font pas avancer le protocole et sont ensuite abandonnées ; ce qui compte pour eux c'est de faire le premier pas, beaucoup de premiers pas, faire du volume donc, et pas de la qualité. Regarder quelle entreprise coordonne les groupes de travail n'est pas un bon

indicateur de leadership non plus. Nous y retrouvons les européens Orange et Nokia en compagnie du chinois Huawei, mais par la suite on n'entendra plus parler du premier.

[74] *Ibid*. p. 14.

[75] Le top 13 a généré plus de 77% des propositions et d'éléments de normalisation.

[76] STATISTA. *Largest listed telecommunications companies in 2019 and 2020, by revenue* [graphique]. 2020 [Consulté le 14 août 2022]. Disponible à l'adresse : www.statista.com/statistics/1149427/telcos-by-revenue/

[77] À titre d'exemple, pour des entreprises avec un chiffre d'affaires issu d'activités télécom de plus de 8 milliards d'euros (les 4 fleurons européens en font tous partie), la participation annuelle par membre individuel s'élèverait à un peu plus de 104K€. Chaque unité de contribution est taxée 3 380 euros. Source : 3GPP. *Who can become an Individual Member of 3GPP and how much does it cost?* [FAQs]. 3GPP [en ligne]. 2022. [Consulté le 4 août 2022]. Disponible à l'adresse : https://www.3gpp.org/about-3gpp/3gpp-faqs#M1

[78] TANAKA, Akito. China in pole position for 5G era with a third of key patents. Nikkei [en ligne]. 3 mai 2019. [Consulté le 3 août 2022]. Disponible à l'adresse : https://asia.nikkei.com/Spotlight/5G-networks/China-in-pole-position-for-5G-era-with-a-third-of-key-patents

[79] Un représentant du Gouvernement chinois occupe actuellement la présidence de IEC, et un mandataire de la Chine a été placé à la tête de l'ISO après que l'organisation ait été dirigée par un fonctionnaire chinois pendant de nombreuses années. La stratégie semble marcher parfaitement car, rien qu'en 2019, la Chine a soumis 830 propositions de normes à l'ITU, sous la baguette de son Secrétaire Général, le chinois Houlin Zhao, en poste depuis 2014. Depuis 2018, la Chine est passée de 14 contributions fiancées à 20, c'est d'ailleurs l'évolution la plus spectaculaire enregistrés ces cinq dernières années. Pendant les deux mandats et l'appui actif de Houlin Zhao en tant que Directeur du Telecommunication Standardization Bureau, la Chine est devenue le deuxième pays, après les États-Unis, en nombre d'entités enregistrées en tant que membres de l'ITU. Rien qu'en 2021, 145 nouvelles normes ont été soutenues à l'ITU par des entités chinoises, contre 46 en 2015, ce qui est six fois plus que celles soutenues par les entités occidentales.

[80] L'Europe ensemble à la Russie a le taux de pénétration des services mobiles le plus élevé au monde : 128% à l'Ouest, 140% au Centre et à l'Est, contre 106% pour les Etats-Unis et 120% pour la Chine. Source : Ericsson : https://www.ericsson.com/4a4be7/assets/local/reports-papers/mobility-report/documents/2022/ericsson-mobility-report-q2-2022.pdf

[81] CNBC. *Interview with Ericsson CEO, Börje Ekholm, from the World Economic Forum 2019*. CNBC [en ligne]. 22 Janvier 2019. [Consulté le 3 Août 2022]. Disponible à l'adresse : https://www.cnbc.com/2019/01/22/cnbc-interview-with-ericsson-ceo-brje-ekholm-from-the-world-economic-forum-2019.html
Traduction : « *Ce qui compte dans la technologie mobile, c'est qu'elle se développe plus rapidement que toutes les technologies précédentes : nous avons plus de 8 milliards d'abonnements dans le monde aujourd'hui. Cela a été possible parce que nous avons une norme mondiale. Donc, pour nous [Ericsson], protéger ce modèle de norme mondiale est vraiment important, c'est ce qui nous donne la connectivité que nous avons aujourd'hui ».*

[82] La compétition pour certifier des algorithmes de chiffrement post-quantique (PQ) s'intègre dans une série d'autres certifications du NIST telles que le chiffrement par blocs (« block cipher » qui a fait certifier l'AES utilisé à grande échelle aujourd'hui, la fonction Hash qui a entériné le SHA-3 et le chiffrement « poids plume » (« Lightweight crypto ») dont le processus a commencé en 2019 et court toujours. Source : NIST https://csrc.nist.gov/CSRC/media/Presentations/Round-2-of-the-NIST-PQC-Competition-What-was-NIST/images-media/pqcrypto-may2019-moody.pdf

[83] Ces algorithmes doivent être résistants à des attaques par ordinateur classique, à des attaques par ordinateur quantique, avoir un niveau de sécurité similaire aux solutions classiques d'aujourd'hui et être compatibles avec la technologie d'aujourd'hui.

[84] Selon les professionnels du quantum computing. Source : https://csrc.nist.gov/csrc/media/Presentations/2022/the-beginning-of-the-end-the-first-nist-pqc-standa/images-media/pkc2022-march2022-moody.pdf

[85] BALL, James. et al. *Revealed: how US and UK spy agencies defeat internet privacy and security.* The Guardian [en ligne]. 6 septembre 2013 [Consulté le 2 mai 2022]. Disponible à l'adresse : https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

[86] NATIONAL INSTITUT of STANDARD and TECHNOLOGY, *NIST Removes Cryptography Algorithm from Random Number Generator Recommendations*. NIST [en ligne]. 21 avril 2014 [mis à jour 8 janvier 2018], [consulté le 3 mai 2022]. Disponible à l'adresse : https://www.nist.gov/news-events/news/2014/04/nist-removes-cryptography-algorithm-random-number-generator-recommendations

[87] Les noms de domaines .eu, .edu, .org et les domaines des états seraient concernés en priorité et ensuite, progressivement, les domaines .com et les domaines restants.

3. UNE COMPRÉHENSION PARTAGÉE DE LA CYBERSÉCURITÉ

3.1. Les limites de la coopération verticale

[1] EUROPEAN UNION EXTERNAL ACTION. *Shared Vision, Common Action: A Stronger Europe* [PDF]. EU [en ligne]. Juin 2016 [Consulté le 5 mai 2022]. pp. 5-6. Disponible à l'adresse : https://www.eeas.europa.eu/eeas/global-strategy-european-unions-foreign-and-security-policy_en

[2] AFP. *L'Estonie a subi les cyberattaques les plus importantes depuis 2007": des cyberattaques revendiquées par des pirates russes ont été déjouées*. Lalibre.be [en ligne]. 18 août 2022 [Consulté le 3 septembre 2022]. Disponible à l'adresse : https://www.lalibre.be/international/europe/2022/08/18/lestonie-a-subi-les-cyberattaques-les-plus-importantes-depuis-2007-des-cyberattaques-revendiquees-par-des-pirates-russes-ont-ete-dejouees-EZV3BTW3UFCFLB3DOZG7Z622DM/
GUYONNET Paul. *Derrière l'affaire de la cyberattaque aux Pays-Bas, le puissant GRU, le service de renseignement militaire russe*. Huffington Post [en ligne]. 5 octobre 2018 [Consulté le 7 septembre 2022]. Disponible à 'adresse : https://www.huffingtonpost.fr/international/article/derriere-l-affaire-de-la-cyberattaque-aux-pays-bas-le-puissant-gru-le-service-de-renseignement-militaire-russe_132480.html

[3] ENISA Press Release. *WannaCry Ransomware: First ever case of cyber cooperation at EU level*. Press Release [en ligne]. 15 mai 2017 [Consulté le 15 septembre 2022). Disponible à l'adresse : https://www.enisa.europa.eu/news/enisa-news/wannacry-ransomware-first-ever-case-of-cyber-cooperation-at-eu-level

[4] EUROPOL media & press. *Ransomware gang arrested in Ukraine with Europol's support*. Press Release [en ligne]. [Consulté le 27 août 2022]. Disponible à l'adresse : https://www.europol.europa.eu/media-press/newsroom/news/ransomware-gang-arrested-in-ukraine-europol%E2%80%99s-support

[5] VITARD Alice. *Les polices française, américaine et ukrainienne arrêtent deux opérateurs de ransomwares*. L'usine digitale [en ligne]. 4 Octobre 2021 [Consulté le 7 juillet 2022]. Disponible à l'adresse : https://www.usine-digitale.fr/article/les-polices-francaise-americaine-et-ukrainienne-arretent-deux-operateurs-de-ransomwares.N1146942

[6] CHARBONNIER Nathanaël. *Cybercriminalité : une vaste opération dans 17 pays permet l'interpellation de sept pirates informatiques*. Francetvinfo [en ligne]. 9 novembre 2021 [Consulté le 7 juillet 2022]. Disponible à l'adresse : https://www.francetvinfo.fr/replay-radio/un-monde-d-avance/cybercriminalite-une-vaste-operation-dans-17pays-permet-l-interpellation-de-septpirates-informatiques_4821597.html

[7] COUR DES COMPTES EUROPÉENNE. *Défis à relever pour une politique de l'UE efficace dans le domaine de la cybersécurité* [PDF]. ECA [en ligne]. Mars 2019 [Consulté le 4 mai 2022]. p. 20. Disponible à l'adresse : https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_FR.pdf

[8] *Wannacry* et *Petya* sont deux attaques majeures qui ont lieu en 2017. Il il s'agit de deux des pires failles de sécurité informatique jamais exploitées qui affectent presque toutes les puces informatiques fabriquées au cours des 20 dernières années.

[9] *L'Europe de la cyberdéfense se construit brique après brique.* Rendre notre monde + sûr [en ligne]. 18 janvier 2022 [Consulté le 4 mai 2022]. Disponible à l'adresse : https://rendre-notre-monde-plus-sur.goron.fr/leurope-de-la-cyberdefense-se-construit-brique-apres-brique/

[10] EUROPOL. *Internet Organised Crime Threat Assessment (IOCTA)* [PDF]. Europol [en ligne]. 27 septembre 2017 [Consulté le 4 mai 2022]. p. 12. Disponible à l'adresse : https://www.europol.europa.eu/cms/sites/default/files/documents/iocta2017.pdf
« L'absence de criminalisation à l'échelle européenne de la possession d'identifiants de paiement en ligne volés/compromis pose des problèmes d'enquête importants dans ce domaine ».

[11] COMMISSION EUROPÉENNE. *Rapport de la Commission au Parlement européen et au Conseil évaluant la cohérence de l'approche adoptée par les États membres pour identifier les opérateurs de services essentiels conformément à l'article 23, paragraphe 1 de la directive 2016/1148/UE*

concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union [PDF]. CE. 546 final. 28 octobre 2019 [Consulté le 5 août 2022]. Disponible à l'adresse : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52019DC0546&from=EN

[12] COMMISSION EUROPÉENNE. *Rapport de la Commission au Parlement européen et au Conseil évaluant la cohérence de l'approche adoptée par les États membres pour identifier les opérateurs de services essentiels conformément à l'article 23, paragraphe 1 de la directive 2016/1148/UE concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union* [PDF]. CE. 546 final. 28 octobre 2019 [Consulté le 5 août 2022]. p. 31. Disponible à l'adresse : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52019DC0546&from=EN et
EUROPEAN COMMISSION. *NIS Implementation Tracker*. EC [en ligne]. 22 mars 2019 [Consulté le 5 mai 2022]. Disponible à l'adresse : https://www.digitaleurope.org/resources/nis-implementation-tracker/ et
State-of-play of the transposition of the NIS Directive. Disponible à l'adresse : https://digital-strategy.ec.europa.eu/en/policies/nis-transposition

[13] EUROPEAN COMMISSION. *Foreign Direct Investment in The EU* (PDF). EC. 13 mars 2019 [Consulté le 5 mai 2022]. p. 94. Disponible à l'adresse : https://trade.ec.europa.eu/doclib/docs/2019/march/tradoc_157724.pdf

[14] *Ibid.* p.32.

[15] *Idem.*

[16] EUROPEAN COMMISSION. *Foreign Direct Investment in The EU* [PDF]. EC. 13 mars 2019 [Consulté le 5 mai 2022]. p. 34. Disponible à l'adresse : https://trade.ec.europa.eu/doclib/docs/2019/march/tradoc_157724.pdf

[17] *Ibid*.

[18] LAUSSON Julien. *Neelie Kroes veut que l'Europe soit leader sur la 5G*. Numerama [en ligne]. 6 septembre 2013 [Consulté le 5 juin 2022]. Disponible à l'adresse : https://www.numerama.com/politique/26920-neelie-kroes-veut-que-l-europe-soit-leader-sur-la-5g.html

[19] TREFFIS TEAM. *Nokia's $16.6 Billion Acquisition Of Alcatel-Lucent Explained*. Forbes [en ligne]. 16 avril 2015 [Consulté le 4 octobre 2022]. Disponible à l'adresse : https://www.forbes.com/sites/greatspeculations/2015/04/16/nokias-16-6-billion-acquisition-of-alcatel-lucent-explained/

[20] Il est pertinent de noter qu'Alcatel-Lucent était en 2015 un acteur incontournable sur le marché américain des équipements sans fil, ayant des contrats de longue durée avec les principaux opérateurs - Verizon et AT&T - ainsi que sur le marché mondial des routeurs, occupant la deuxième place après Cisco. L'acquisition s'est fit pour un montant de 11 Md€.

[21] ESCANDE, Philippe. *Nokia : Le fantôme d'Alcatel hante les forêts finlandaises*. Le Monde [en ligne]. 3 mars 2020 [Consulté le 5 mars 2022]. Disponible à l'adresse : https://www.lemonde.fr/economie/article/2020/03/03/nokia-le-fantome-d-alcatel-hante-les-forets-finlandaises_6031637_3234.html

[22] La technologie de semi-conducteurs choisie pour les stations de base permettait plus de flexibilité et de personnalisation. En théorie, c'était une bonne nouvelle pour ses clients et ses ingénieurs. De plus, cela facilitait l'intégration des différentes technologies de Nokia et d'Alcatel-Lucent. Mais cette technologie était également beaucoup plus coûteuse à fabriquer, ce qui réduisait la rentabilité et rendait plus difficile de rivaliser avec la concurrence en termes de prix pour les kits de la 5G.

[23] Avec le temps les langues se sont libérées et on a appris un peu plus sur l'origine de la chute de Nokia : des décisions prises sur des suppositions, qui se sont révélées fausses, un PDG autoritaire et des choix technologiques sans avenir (le hardware au détriment du software).

[24] JUILLET, Alain. *Le renseignement, outil de l'intelligence économique*. YouTube. 16 octobre 2019 [Consulté le 2 mars 2020]. Disponible à l'adresse : https://www.youtube.com/watch?v=vUChdxWxt5o

[25] Augmentation de 40% des investissements dans la R&D entre 2019 et 2021. Source PDG Nokia: https://youtu.be/ySUSCL7yRt8

[26] McCASKILL, Steve. *Nokia reaps rewards of 5G demand but supply issues could have future impact*. TechRadar [en ligne]. 29 avril 2022 [Consulté le 10 août 2022]. Disponible à l'adresse : https://www.techradar.com/news/nokia-reaps-rewards-of-5g-demand-but-supply-issues-could-have-future-impact

[27] Les objectifs de l'UE vis-à-vis de la 5G étaient ambitieux : un lancement d'offres commerciales dans chaque Etat Membre avant fin 2020 et une couverture des grandes villes et axes principaux de transport avant 2025.

[28] Interview avec *Le Monde* le 17 avril 2021, intervention à la Conférence Viva Technology en 2019,

[29] CNBC. *Interview with Pekka Lundmark: No green without digital*. CNBC [YouTube]. 3 novembre 2021 [Consulté le 4 octobre 2022]. Disponible à l'adresse : https://youtu.be/ySUSCL7yRt8
Traduction : *« L'infrastructure est critique pour la 5G en Europe. Chaque pays européen procède à sa propre attribution de fréquences. Une décision qui rend l'ensemble du système inefficace. Il y a longtemps, l'intention était que l'Europe ait une approche coordonnée des fréquences 5G. La Finlande est le seul pays d'Europe à avoir appliqué cette décision. Nous avons donc beaucoup à faire pour concurrencer l'Asie et les États-Unis. »*

[30] La bande de 3,6 GHz a été le plus largement attribuée : 23 des 27 États membres ont attribué cette bande. La deuxième bande la plus populaire est la bande de 700 MHz, qui a été attribuée dans 20 des 27 EM. La bande la moins populaire est la bande des 26 GHz, qui n'a été attribuée que dans 8 EM. Enfin, 2 EM n'ont assigné aucune des bandes pionnières. Source : https://www.ookla.com/articles/5g-europe-mapping-the-future-q1-2022

[31] ERICSSON. *Börje Ekholm: Europe needs to act fast on 5G or lose out*. Ericsson [en ligne]. 16 mai 2019 [Consulté le 2 avril 2022]. Disponible à l'adresse : https://www.ericsson.com/en/news/2019/5/borje-ekholm-europe-needs-to-act-with-speed-on-5g
Traduction : « *Aujourd'hui, une vente aux enchères de fréquences est considérée comme un succès si elle rapporte un maximum d'argent aux recettes fiscales du gouvernement […] mais la réalité est que nous devons prendre en compte tous les autres avantages que vous obtiendriez en développant rapidement l'infrastructure des télécommunications. »*

[32] CHFFIN, Zéliha. *« Je pense profondément que la 5G va nécessiter plus de régulation ». Interview avec le président de l'Arcep*. Arcep [en ligne]. 20 janvier 2020 [Consulté le 3 mai 2022]. Disponible à l'adresse : https://www.arcep.fr/actualites/les-prises-de-parole/detail/n/je-pense-profondement-que-la-5g-va-necessiter-plus-de-regulation.html

[33] BAZOGE, Mickaël. *Déploiement 5G avec des équipements Huawei : plainte de Free contre l'Anssi*. iGénération [en ligne]. 2 septembre 2021 [Consulté le 4 août 2022]. Disponible à l'adresse : https://www.igen.fr/telecoms/2021/09/deploiement-5g-avec-des-equipements-huawei-plainte-de-free-contre-lanssi-124901

[34] CHAFFIN, Zéliha. *Fréquences 5G : en Allemagne, les enchères rapportent 6,55 milliards d'euros*. Le Monde [en ligne]. 13 juin 2019 [Consulté le 3 août 2022]. Disponible à l'adresse : https://www.lemonde.fr/economie/article/2019/06/13/frequences-5g-en-allemagne-les-encheres-rapportent-6-55-milliards-d-euros_5475698_3234.html

[35] *Idem*.

[36] ERICSSON. *Börje Ekholm: Europe and 5G: Address the reality -- not the myths*. Ericsson [en ligne]. 20 mai 2019 [Consulté le 2 avril 2022]. Disponible à l'adresse : https://www.ericsson.com/en/blog/2019/5/europe-and-5g-address-the-reality-not-the-myths
Traduction : « *De nombreux consommateurs européens dépensent par semaine plus dans les cafés que pour le haut débit mobile par mois. Un gain à court terme, mais une souffrance à long terme* ».

[37] *Idem.*

[38] ERICSSON. *Börje Ekholm: Europe needs to act fast on 5G or lose out*. Ericsson [en ligne]. 16 mai 2019 [Consulté le 2 avril 2022]. Disponible à l'adresse : https://www.ericsson.com/en/news/2019/5/borje-ekholm-europe-needs-to-act-with-speed-on-5g
Traduction : « *Les États-Unis et la Chine considèrent la 5G comme une infrastructure nationale essentielle et l'épine dorsale de la numérisation de la société […] Ce n'est pas une coïncidence si les grands gagnants de la 4G - tels qu'Alibaba, Netflix et Tencent - sont apparus aux États-Unis et en Chine, et non en Europe.* »

[39] KECHICHE, Silwia. *5G in Europe: Reflecting on the Progress So Far and Mapping the Future*. Ookla [en ligne]. 23 février 2022[Consulté le 4 mai 2022]. Disponible à l'adresse : https://www.ookla.com/articles/5g-europe-mapping-the-future-q1-2022

[40] HEINRICH, Tobias et al. *Foreign direct investment reviews 2021: European Union*. White&Case [en ligne]. 20 décembre 2021 (Consulté le 5 mai 2022]. Disponible à l'adresse : https://www.whitecase.com/insight-our-thinking/foreign-direct-investment-reviews-2021-european-union

[41] Source : Commission Européenne.

[42] COUR DES COMPTES EUROPENNES. *Défis à relever pour une politique de l'UE efficace dans le domaine de la cybersécurité* [PDF]. ECA Europe [en ligne]. Mars 2019 [Consulté le 15 septembre 2022]. Disponible à l'adresse : https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_FR.pdf

[43] ENISA. *EU ICT Industrial Policy : Breaking the Cycle of Failure* [PDF]. ENISA [en ligne]. Juillet 2019 [Consulté le 5 mai 2022]. p. 8. Disponible à l'adresse : https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/eu-ict-industry-consultation-paper

[44] La technologie de Skype était développée depuis l'Estonie (pays d'origine des trois premiers programmeurs du logiciel), plus précisément dans la capitale Tallinn ou Skype possède toujours des bureaux. Le nombre important d'Estoniens impliqués dans le projet a fait de Skype la fierté de ce pays qui tentait depuis le milieu des années 1990 de devenir un spécialiste mondial de l'économie numérique.
Rachat de Skype par Microsoft : Cisco débouté par la justice. ZDnet [en ligne]. 11 décembre 2013 [Consulté le 5 août 2022]. Disponible à l'adresse : https://www.zdnet.fr/actualites/rachat-de-skype-par-microsoft-cisco-deboute-par-la-justice-39796244.html

[45] Skype a été fondé en 2003 au Luxembourg par le suédois Niklas Zennström et le danois Janus Friis et développé par les programmeurs estoniens Ahti Heinla, Priit Kasesalu et Jaan Tallinn2. Ces trois Estoniens étaient déjà à l'origine du logiciel KaZaA. Un des noms initiaux du projet était Sky peer-to-peer, abrégé en « Skyper ». Pour des raisons de disponibilité du nom, les fondateurs ont finalement décidé d'abandonner le « r » final.

[46] Telecom Package et toutes les règles en découlant + EU Consumer law + la Directive (EU) 2019/770 concernant les contrats de fourniture de contenu numérique et de services numériques + General Data Protection Regulation (*RGPD*).

[47] BUSINESS EUROPE. *Impact of EU regulation on innovation* [PDF]. [en ligne]. Décembre 2016 [Consulté le 12 avril 2022]. Disponible à l'adresse : https://www.businesseurope.eu/sites/buseur/files/media/reports_and_studies/2016-12-02_impact_of_eu_regulation_on_innovation_-_repository_of_industry_cases.pdf

[48] VOBING Tobias. *Survey Shows: Companies Are Unhappy With the GDPR*. Buse.de [en ligne]. 17 novembre 2022 [Consulté le 17 octobre 2022]. Disponible à l'adresse : https://buse.de/en/blog-en/labor-law/survey-shows-companies-are-unhappy-with-the-gdpr/

[49] EUROPEAN COMMISSION. *Better regulation for growth and jobs in the European Union. Communication from the Commission to the Council and the European Parliament* [PDF]. EC(2005) 97 final, 16 mars 2005 [Consulté le 5 août 2022]. Disponible à l'adresse : https://aei.pitt.edu/43023/1/com2005_0097.pdf

[50] *The Artificial Intelligence Act* (AIA) est un règlement européen horizontal qui s'appliquera à tout produit qui contient des éléments d'intelligence artificielle. The Center for Data Innovation anticipe une augmentation de 17 % de frais généraux sur toutes les dépenses liées à l'IA afin d'assurer la conformité avec l'AIA.

[51] MEULLER, Benjamin. *How Much Will the Artificial Intelligence Act Cost Europe?* [PDF] Centre for Data Innovation. Juillet 2021 [Consulté le 5 mars 2022]. p. 3. Disponible à l'adresse : https://www2.datainnovation.org/2021-aia-costs.pdf

[52] *Ibid*. p. 1. Traduction : *« S'il est adopté, AIA sera la réglementation la plus restrictive au monde pour les outils d'intelligence artificielle (IA). Il limitera non seulement le développement et l'utilisation de l'IA en Europe, mais imposera également des coûts importants aux entreprises et aux consommateurs. »*

[53] GRAGOUIAN, Dionys. *How businesses should respond to the EU's Artificial Intelligence Act*. WeForum (en ligne). 8 février 2022 [Consulté le 5 mai 2022]. Disponible à l'adresse : https://www.weforum.org/agenda/2022/02/how-businesses-should-respond-to-eu-artificial-intelligence-act/
Traduction : *« L'UE frappe à nouveau avec une nouvelle série de règlements qui visent l'utilisation de l'intelligence artificielle (IA) pour faire face à la variété des risques associés à l'adoption sociétale de l'IA. Comme son frère, le Règlement général sur la protection des données (RGPD), the Artificial Intelligence Act (AIA) a des dents, avec des amendes pouvant atteindre 30 millions d'euros, soit 6 % du chiffre d'affaires mondial. »*

[54] VERBEEK, Arnold et LUNDQVIST, Maria. *Artificial Intelligence, Blockchain And The Future Of Europe* [PDF]. European Commission Directorate-General for Communications Networks, Content and Technology and European Investment Bank. Juillet 2021. 49. p. 42. Disponible à l'adresse : https://www.eib.org/attachments/thematic/artificial_intelligence_blockchain_and_the_future_of_europe_report_en.pdf

[55] MEULLER, Benjamin. *How Much Will the Artificial Intelligence Act Cost Europe?* [PDF] Centre for Data Innovation. Juillet 2021 [Consulté le 5 mars 2022]. p. 9. Disponible à l'adresse: https://www2.datainnovation.org/2021-aia-costs.pdf Les entreprises du classement Fortune 500 ont dépensé 8Md$ pour se conformer au *RGPD*. Les entreprises américaines de plus de 500 employés ont dépensé jusqu'à 10 millions de dollars chacune pour se conformer au *RGPD*, 150Md$ au total.

[56] Le PPP est un accord contractuel de long terme entre une autorité publique et un partenaire privé dans le cadre duquel ce partenaire assure et finance des services publics à partir d'un équipement, avec un partage des risques associés. Source : OCDE, *Principes applicables à la gouvernance publique des partenariats public-privé*, 2012

[57] Visites des responsables français aux FIC :
2018: Gérard COLLOMB, Ministre d'Etat, Ministre de l'Intérieur
2019: Laurent Nunez, Secrétaire d'État auprès du Ministre de l'Intérieur, et Florence Parly, Ministre des Armées
2020: Christophe Castaner, Ministre de l'Intérieur
2021: Florence Parly, Ministre des Armées
2022: Gérard Darmanin, Ministre de l'Intérieur, Florence Parly, Ministre des Armées, Cedric O, Secrétaire chargé de la transition numérique et des communications électroniques.

[58] EUROPEAN DATA PROTECTION SUPERVISOR. *Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services*. EDPS (en ligne). 2 juillet 2020 [Consulté le 4 mai 2022]. Disponible à l'adresse : https://edps.europa.eu/sites/edp/files/publication/20-07-02_edps_euis_microsoft_contract_investigation_en.html#recommendations-6

[59] EUROPEAN AUDITORS COURT. *Cybersecurity of EU institutions, bodies and agencies : Level of preparedness overall not commensurate with the threats* [PDF]. 5/2022. ECA [en ligne]. 29 mars 2022 [Consulté le 3 septembre 2022]. Disponible à l'adresse : https://www.eca.europa.eu/Lists/ECADocuments/SR22_05/SR_cybersecurity-EU-institutions_FR.pdf

3.2. Une coopération linéaire qui peine à trouver sa ligne directrice

[60] EUROPEAN COURT OF AUDITORS. *Challenges to effective EU cybersecurity policy* [PDF]. ECA. Mars 2019 [Consulté le 5 mai 2022]. p. 34. Disponible à l'adresse : https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

[61] *Ibid.* p. 30.

[62] Pour en savoir plus sur le Traffic Light Protocol (TLP), visiter https://www.cert.be/fr/le-traffic-light-protocol-tlp

[63] THIERRY, Gabriel. *L'Anssi envoyée au Monténégro pour contrer la cyberattaque en cours*. Zdnet [en ligne]. 29 août 2022. [Consulté le 6 septembre 2022]. Disponible à l'adresse : https://www.zdnet.fr/actualites/l-anssi-envoyee-au-montenegro-pour-contrer-la-cyberattaque-en-cours-39946388.htm

[64] Monténégro : https://www.nato.int/cps/fr/natohq/news_144647.htm?selectedLocale=fr

[65] KARAYAN, Raphaële. *La France se porte au secours du Monténégro, cible d'une cyberattaque*. Usine digitale Zdnet [en ligne]. 30 août 2022. [Consulté le 6 septembre 2022]. Disponible à l'adresse : https://www.usine-digitale.fr/article/la-france-se-porte-au-secours-du-montenegro-cible-d-une-cyberattaque.N2037452

[66] Actuellement 60 projets PESCO sont en cours de développement.

[67] ADAM, Louis. *Cybersécurité : l'UE envoie ses experts en Ukraine*. Zdnet [en ligne]. Le 23 février 2022. [Consulté le 6 septembre 2022]. Disponible à l'adresse : https://www.zdnet.fr/actualites/cybersecurite-l-ue-envoie-ses-experts-en-ukraine-39937895.htm

[68] PESCO : https://www.pesco.europa.eu/about/

[69] GAIA-X : https://gaia-x.eu/
Les membres fondateurs du côté allemand incluent Beckhoff Automation, BMW, Bosch, DE-CIX, Deutsche Telekom, German Edge Cloud, Deutsche Telekom, PlusServer, SAP, Siemens, Fraunhofer-Gesellschaft, International Data Spaces Association et l'Association européenne des fournisseurs de Cloud CISPE. Du côté français, on note l'engagement de Amadeus, Atos, Docaposte, Électricité de France (EDF), Institut Mines-Télécom (IMT), Orange, Outscale, OVHcloud, Safran et Scaleway (source *Wikipedia*) *GAIA-X*, Wikipédia. https://en.wikipedia.org/wiki/GAIA-Xhttps://gaia-x.eu/wp-content/uploads/2022/07/Gaia-X-Factsheet_V5_28072022.pdf

[70] FILIPPONE, Dominique. *Gaia-X : le sponsoring sino-américain agace, Scaleway s'en va*. Le monde informatique [en ligne]. 18 novembre 2021 [Consulté le 2 mai 2022]. Disponible à l'adresse : https://www.lemondeinformatique.fr/actualites/lire-aws-veut-aider-au-developpement-de-la-5g-privee-87694.html

[71] Gaia-X, Members' Directory: https://gaia-x.eu/membership/members-directory/

[72] Sont membres d'ECSO Atos, Airbus, Thalès Microsoft, la Poste, Deloitte, Accenture, Bureau Veritas, Schneider Electric, Siemens, ISC2, Autostrade per l'Italia, EDF, CERT Romania, Ministère de défense estonien, FSecure.

[73] Les entreprises certifiées sont visibles à l'adresse : https://www.cybersecurity-label.eu/labelled-companies/

[74] ECSO http://latest-ecso.devalchemiser.com/activities/market-deployment-investments-and-international-collaboration/

[75] *Telefónica, Deutsche Telekom Et Vodafone Utilisent La Blockchain Pour Le Règlement D'itinérance*. 14 Juillet 2022 [Consulté le 22 Juillet 2022]. Disponible à l'adresse : https://passioncrypto.com/telefonica-deutsche-telekom-et-vodafone-utilisent-la-blockchain-pour-le-reglement-ditinerance/

[76] PERRIN-MONLOUIS Pierre. *Singtel, Orange, Deutsche Telekom e Telefónica stanno collegando ecosistemi di start-up nel sud-est asiatico, in Africa, in Europa, in America Latina e nel Medio Oriente*. Edubourse.it [en ligne]. 20 octobre 2021 [Consulté le 17 juin 2022]. Disponible à l'adresse : https://edubourse.com/it/finance-actualites-actu-89484/

[77] LOUBIERE, Paul. *Accord Thalès-Google : Bercy abandonne le cloud souverain pour le plus grand bonheur des GAFAM*. Challenges (en ligne]. 11 octobre 2021 [Consulté le 5 octobre 2022]. Disponible à l'adresse : https://www.challenges.fr/high-tech/accord-thales-google-bercy-abandonne-le-cloud-souverain-pour-le-plus-grand-bonheur-des-gafam_784302

4. OBSTACLES ET INCOHÉRENCES

4.1. Les obstacles à la coopération

[1] PUGLIERIN Jana. ZERKA Pawel. *European Sovereignity Index* [PDF]. European Council on Foreign Relations [en ligne]. Juin 2022 [Consulté le 5 août 2022]. Disponible à l'adresse : https://ecfr.eu/special/sovereignty-index/#terrain-technology

[2] D'AIMALE, Charles et al. *Comment "débloquer" le marché de l'assurance cyber en France ?* [PDF] Télécom Paris [en ligne]. Juin 2017 [Consulté le 5 mai 2022]. Pp 7. Disponible à l'adresse : https://www.telecom-paris-alumni.fr/global/gene/link.php?doc_id=73&fg=1

[3] D'AIMALE, Charles et al. *Comment "débloquer" le marché de l'assurance cyber en France ?* [PDF] Télécom Paris [en ligne]. Juin 2017 [Consulté le 5 mai 2022]. p 10. Disponible à l'adresse : https://www.telecom-paris-alumni.fr/global/gene/link.php?doc_id=73&fg=1

[4] LEVY, Ian. *Security, complexity and Huawei; protecting the UK's telecoms networks* [blog]. National Cyber Security Centre [en ligne]. 22 février 2019 [Consulté le 3 mai 2022]. Disponible à l'adresse : https://www.ncsc.gov.uk/blog-post/blog-post-security-complexity-and-huawei-protecting-uks-telecoms-networks

Traduction : « À l'heure actuelle, personne n'achète de services de télécommunications en fonction de leur niveau de sécurité. Une entreprise ne serait donc pas récompensée si elle investissait davantage que ses concurrents dans la création d'un service plus sûr. Cela conduit à une situation étrange où vous n'êtes pas récompensé pour avoir fait ce qu'il faut, ce qui rend la chose difficile à faire à long terme. »

[5] EUROPEAN COMMISSION. *5G Observatory. Quarterly Report 16*. CE [en ligne]. Juillet 2022 [Consulté le 5 mai 2022]. p. 6. Disponible à l'adresse : https://5gobservatory.eu/wp-content/uploads/2022/08/QR-16_Final_PDF.pdf

[6] Source European 5G Observatory : https://5gobservatory.eu/market-developments/5g-services/

[7] EUROPEAN COURT OF AUDITORS. *Challenges to effective EU cybersecurity policy* [PDF]. ECA [en ligne]. Mars 2019. p. 22. Disponible à l'adresse : https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

[8] CERULUS, Laurent. *Ericsson boss bemoans lack of European support on 5G*. Politico [en ligne]. 25 juillet 2019 [Consulté le 6 mai 2022]. Disponible à l'adresse : https://www.politico.eu/article/borje-ekholm-global-5g-battle-ericsson-ceo-bemoans-lack-of-european-support/

[9] CERULUS, Laurent. *EU nudges Germany to cut down on Huawei*. Politico [en ligne]. 10 novembre 2022 [Consulté le 23 novembre 2022]. Disponible à l'adresse : https://www.politico.eu/article/eu-nudges-germany-to-cut-down-on-huawei/

[10] Le raisonnement d'une opération militaire se façonne en trois temps. Le temps 3 anticipe la finalité de l'effet majeur du temps 2 pour la réalisation globale d'une opération.

[11] Carl Von Clausewitz : *« La grande incertitude d'informations en période de guerre est d'une difficulté particulière parce que toutes les actions doivent, dans une certaine mesure, être planifiées avec une légère zone d'ombre qui (…) comme l'effet d'un brouillard ou d'un clair de lune, donne aux choses des dimensions exagérées ou non naturelles »*. VON CLAUSEWITZ, Carl. *De la Guerre (Vom Krieg).* Éditions Mille et une Nuit. Paris. 2006.

[12] HARBULOT, Christian et al. *Guerre Economique Qui est l'ennemi ?* Paris. Nouveau monde Editions. 2022. p12.

[13] EUROPEAN UNION, European Court of Auditors, *5G roll-out in the EU : delays in deployment of networks with security issues remaining unresolved* [Special report]. Publications Office of the European Union. N° 03.2022 [Consulté le 5 août 2022]. Disponible à l'adresse : https://data.europa.eu/doi/10.2865/011861

[14] EDUCATION FIRST. *EF English Proficiency Index* [PDF]. Education First. 2022 [Consulté le 5 septembre 2022]. Disponible à l'adresse : https://www.ef.com/assetscdn/WIBIwq6RdJvcD9bc8RMd/cefcom-epi-site/reports/2022/ef-epi-2022-english.pdf

[15] *Ibid*. pp. 12-16.

[16] INSTITUT d'ÉTUDES DE GÉOPOLITIQUE APPLIQUÉE. *Madrid : 2022 : Un sommet pivot pour l'OTAN* [Conférence]. Paris. 28 octobre 2022.

[17] *Idem.*

[18] ALIX, Christophe. *Nokia va à nouveau réduire ses effectifs en France*. Libération [en ligne]. 15 janvier 2019. Disponible à l'adresse : https://www.liberation.fr/france/2019/01/15/nokia-va-a-nouveau-reduire-ses-effectifs-en-france_1703150/

[19] Entretien réalisé en juin 2022 lors des travaux de groupe sur les risques interculturels à l'Ecole de Guerre Economique.

[20] *What do the French really think of the Germans*. The Local [en ligne]. 3 juillet 2014 [Consulté le 5 mai 2022]. Disponible à l'adresse : https://www.thelocal.fr/20140703/what-do-the-french-really-think-of-the-germans/

[21] BOULAY, Benjamin. *L'interculturel en France Orientation des débats et des travaux* (2000-2007) [PDF]. Dans *Hommes et Migrations*, hors-série. Novembre 2008 (Consulté le 5 mai 2022]. *L'interculturalité en débat*. pp. 61-95. Disponible à l'adresse : https://doi.org/10.3406/homig.2008.4684

[22] EUROSTAT. *Eurostat: Non-EU Citizens Account For 5.3% of EU Population*. Schenghen Visa [en ligne]. 31 mars 2022 [Consulté le 5 septembre 2022]. Disponible à l'adresse : https://www.schengenvisainfo.com/news/eurostat-non-eu-citizens-account-for-5-3-of-eu-population/

[23] BOULAY, Benjamin. *L'interculturel en France Orientation des débats et des travaux* (2000-2007) [PDF]. Dans *Hommes et Migrations*, hors-série. Novembre 2008 (Consulté le 5 mai 2022]. *L'interculturalité en débat*. pp. 61-95. Disponible à l'adresse : https://doi.org/10.3406/homig.2008.4684

[24] LEVY, Ian. *The future of telecoms in the UK* [blog]. National Cyber Security Centre[en ligne]. 28 janvier 2020 [Consulté le 3 mai 2022]. Disponible à l'adresse : https://www.ncsc.gov.uk/blog-post/the-future-of-telecoms-in-the-uk

[25] EDUCATION FIRST. *EF English Proficiency Index* [PDF]. Education First.2022 [Consulté le 5 septembre 2022]. p. 12. Disponible à l'adresse : https://www.ef.com/assetscdn/WIBIwq6RdJvcD9bc8RMd/cefcom-epi-site/reports/2022/ef-epi-2022-english.pdf

[26] ACE CAPITAL PARTNERS. *Baromètre Ace de l'investissement européen en cybersécurité* [PDF]. DocPlayer [en ligne]. Mai 2021 [Consulté le 3 mai 2022]. Disponible à l'adresse : https://docplayer.fr/213380871-Barometre-ace-de-l-investissement-europeen-en-cybersecurite-2-eme-edition-mai-version-fr.html

[27] *Idem*.

[28] DIRECTORATE-GENERAL FOR COMMUNICATIONS NETWORKS, CONTENT AND TECHNOLOGY. *Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres* [PDF]. UE [en ligne]. 20 septembre 2018 [Consulté le 4 mai 2022]. Disponible à l'adresse : https://ec.europa.eu/transparency/documents-register/detail?ref=SWD(2018)403&lang=en

[29] EUROPEAN COMMISSION. *Joint Communication to The European Parliament, The European Council and The Council. Increasing resilience and bolstering capabilities to address hybrid threats* [PDF]. EC JOIN(2018) 16 final. 13 juin 2018 [Consulté le 5 mai 2022]. p.8. Disponible à l'adresse : https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018JC0016&rid=1

[30] CAVE, Danielle. *Australia's 5G decision* [video]. Australian Strategic Policy Institute [en ligne]. 21 juillet 2019 [Consulté le 3 mai 2022]. Disponible à l'adresse : https://www.aspi.org.au/video/australias-5g-decision?__cf_chl_tk=UZdLeV14Rx4i6upsnqgegvVsfxJuVP6v7eeRtEvVblM-1660402142-0-gaNycGzNCH0

Traduction : *« Si vous faites entrer une entreprise dans votre réseau 5G, qui est une pièce vraiment critique de l'infrastructure nationale et que d'autres infrastructures nationales vont s'appuyer sur ce réseau 5G, vous devez pouvoir faire confiance à cette entreprise et elle doit être très transparente. Et le problème avec Huawei est que nous n'avons pas ça. […] Lorsqu'il s'agit d'un réseau 5G, vous devez*

vous préoccuper de la sécurité plus que des coûts. Et si l'équipement est très bon marché, cela n'a pas d'importance si vous ne pouvez pas assurer la sécurité ».

[31] *Idem.*
Traduction *: « Pour ceux qui veulent l'interdire [Huawei], le défi est de savoir quelle est l'alternative. Pour ceux qui penses pouvoir le gérer, cela revient à se mettre le doigt dans l'œil. »*

[32] STOLTON, Samuel. *EU Commission pressed on controversial links to Palantir*. Euractiv [en ligne]. 11 juin 2020 [Consulté le 5 mai 20222]. Disponible à l'adresse : https://www.euractiv.com/section/digital/news/eu-commission-pressed-on-controversial-links-to-palantir/

[33] STOLTON, Samuel. *Commission kept no records on Davos meeting between von der Leyen and Palantir CEO*. Euractiv [en ligne]. 8 juin 2020 [Consulté le 5 mai 2022]. Disponible à l'adresse : https://www.euractiv.com/section/data-protection/news/commission-kept-no-records-on-davos-meeting-between-von-der-leyen-and-palantir-ceo/
Traduction : *« Pour que les Européens aient foi en notre Union, ses institutions doivent être ouvertes et irréprochables en matière d'éthique, de transparence et d'intégrité. »*

[34] LEONARD, Mark et PUGLIERIN, Jana. *Policy Brief How to Prevent Germany from Becoming Eurosceptic* [PDF]. ECFR [en ligne]. Juin 2021. p. Disponible à l'adresse : https://ecfr.eu/wp-content/uploads/How-to-prevent-Germany-from-becoming-Eurosceptic.pdf

[35] CONNOR, Richard. *Germans trust China more than the US, survey finds*. DeutscheWelle [en ligne]. 2 août 2019 (Consulté le 5 mai 2022]. Disponible à l'adresse : https://www.dw.com/en/germans-trust-china-more-than-the-us-survey-finds/a-47435595?maca=en-EMail-sharing

[36] POUSHTER, Jacob et AUSTIN, Sarah. *The U.S.-German Relationship Remains Strong.* Pew Research Center [en ligne]. 17 octobre 2022 [Consulté le 10 mai 2022]. Disponible à l'adresse : https://www.pewresearch.org/global/2022/10/17/us-german-relationship-remains-strong/

[37] FORRESTER. *By The End Of 2023, Only 1 In 5 European Citizens Will Still Trust Their Government*. Forbes [en ligne]. 28 novembre 2022 [Consulté le 29 novembre 2022]. Disponible à l'adresse : https://www.forbes.com/sites/forrester/2022/10/28/by-the-end-of-2023-only-1-in-5-european-citizens-will-still-trust-their-government/

[38] CAPGEMINI. *5G in Industrial Operations*. [PDF] Capgemini [en ligne]. 2019 [Consulté le 4 septembre 2022]. Disponible à l'adresse : https://www.capgemini.com/wp-content/uploads/2019/06/5G-in-industrial-operations-Report.pdf

[39] GOUJARD, Clothilde et CERULUS, Laurens. *Inside Gaia-X: How chaos and infighting are killing Europe's grand cloud project*. Politico [en ligne]. 26 octobre 2021 [Consulté le 3 mai 2022]. Disponible à l'adresse : https://www.politico.eu/article/chaos-and-infighting-are-killing-europes-grand-cloud-project/
Traduction : *« Les grands joueurs, ils font ce qu'ils font. D'abord, ils frappent à la porte, puis ils mettent le pied dans la porte... Très rapidement, il est devenu clair que ces gars-là étaient dominants dans les groupes techniques. »*

[40] *What do the French really think of the Germans*. The Local [en ligne]. 3 juillet 2014 [Consulté le 5 mai 2022]. Disponible à l'adresse : https://www.thelocal.fr/20140703/what-do-the-french-really-think-of-the-germans/

4.2. Les incohérences

[41] L'affaire des ventes de Mirage 2000.5 à Taiwan en 2002. LAIDI, Ali. *Le droit, la nouvelle arme de guerre économique*, Paris. Acte Sud. 2019. p. 281.

[42] JACQUÉ, Philippe et CAVAL, Allan. *L'Italie : les premiers pas de Giorgia Meloni, entre apaisement à Bruxelles et polémique à Rome*. Le Monde [en ligne]. 4 novembre 2022 [Consulté le 11 novembre 2022]. Disponible à l'adresse : https://www.lemonde.fr/international/article/2022/11/04/italie-pour-giorgia-meloni-des-premiers-pas-apaises-a-bruxelles-et-deja-une-polemique-a-rome_6148440_3210.html

[43] DAMRO, Chad. *Market power Europe: exploring a dynamic conceptual framework* [PDF]. Journal of European Public Policy. 2015 [Consulté le 4 mai 2022].22.no. 9: 1336-1354. Disponible à l'adresse : https://www.researchgate.net/publication/279163630_Market_Power_Europe_Exploring_a_Dynamic_Conceptual_Framework

[44] EUROPEAN ACADEMIES SCIENCE ADVISORY COUNCIL. *International Sharing of Personal Health Data for Research* [PDF]. 8 avril 2021. p. 23. Disponible à l'adresse : https://easac.eu/fileadmin/PDF_s/reports_statements/Health_Data/International_Health_Data_Transfer_2021_web.pdf
Traduction *:* « *Il est devenu évident que la mise en œuvre du RGPD a introduit des obstacles au transfert international de données en dehors de l'UE/EEE, ce qui crée des problèmes pour le partage des données de santé pour la recherche dans le secteur publique. Ce problème affecte les patients et les citoyens qui sont les bénéficiaires finaux de la recherche dans la santé. »*
En 2019 le nombre de projets de collaboration entre des structures hospitalières américaines et des pays de l'UE était d'environ 5 000, la plupart ayant débuté avant l'entrée en vigueur du *RGPD*. Le *RGPD* ne prévoit aucun cadre pour mettre à jour ces accords antérieur. La proportion de ces projets impliquant le partage de données n'est pas connue, mais elle est estimée comme probablement élevée.

[45] RENDA, Andrea. *Beyond the "Brussels Effect"*. Fondation for European Progressive Studies [PDF]. Mars 2022. Disponible à l'adresse : https://feps-europe.eu/wp-content/uploads/downloads/publications/220301 beyond the brussels effect.pdf

[46] Voté en 2016, le *RGPD* fixe les obligations des organisations et entreprises en matière d'utilisation et de traitement des données personnelles des utilisateurs de services, les données personnelles désignant toute information qui, directement ou indirectement, peut permettre d'identifier une personne. Il s'agit du premier règlement européen concentrant et unifiant la législation relative à la protection des droits des utilisateurs, et fixant des sanctions dissuasives en cas de non-respect des obligations.

[47] DPO CONSULTING. *RGPD : vers une harmonisation mondiale ou pourquoi vous ne pourrez pas l'éviter*. Zdnet [en ligne]. 13 mai 2019 [Consulté le 15 septembre 2022]. Disponible à l'adresse : https://www.zdnet.fr/actualites-partenaires/rgpd-vers-une-harmonisation-mondiale-ou-pourquoi-vous-ne-pourrez-pas-l-eviter-39884553.htm

[48] ACCESS NOW. *Three Years under the EU GDPR* [PDF]. AccessNow [en ligne]. 2021 [Consulté le 5 mai 2022]. Disponible à l'adresse : https://www.accessnow.org/cms/assets/uploads/2021/05/Three-Years-Under-GDPR-report.pdf

[49] LATOMBE, Philippe. *Souveraineté énergétique et numérique : mais pour qui roule Ursula von Der Leyen ?*. La Tribune [en ligne]. Le 10 Octobre 2022. [Consulté le : 11 Octobre 2022]. Disponible à l'adresse : https://www.latribune.fr/opinions/tribunes/souverainete-energetique-et-numerique-mais-pour-qui-roule-ursula-von-der-leyen-936120.html

[50] Pour un aperçu sur la complexité de la technologie 5G, lire le blog de Ian Levy, Directeur du National Cyber Security Centre britannique :
LEVY, Ian. *Security, complexity and Huawei; protecting the UK's telecoms networks* [PDF]. National Cyber Security Centre [en ligne]. 22 février 2019 [Consulté le 3 mai 2022]. Disponible à l'adresse : https://www.ncsc.gov.uk/pdfs/blog-post/blog-post-security-complexity-and-huawei-protecting-uks-telecoms-networks.pdf

[51] EKHOLM, Börje. *Europe needs to act fast on 5G or lose out*. Ericsson [en ligne]. 16 mai 2019 [Consulté le 5 mai 2022]. Disponible à l'adresse : https://www.ericsson.com/en/news/2019/5/borje-ekholm-europe-needs-to-act-with-speed-on-5g

[52] HODGE, Jim. *Standalone 5G core security: Standards multiplicity and key management singularity*. Heavy Reading [en ligne]. 17 décembre 2020 [Consulté le 5 novembre 2022]. Disponible à l'adresse : https://www.lightreading.com/5g/standalone-5g-core-security-standards-multiplicity-and-key-management-singularity-/a/d-id/766227

[53] KECHICE, Sylwia. *5G in Europe: Reflecting on the Progress So Far and Mapping the Future. OOKLA* [en ligne]. 22 février 2022 [Consulté le 3 mai 2022]. Disponible à l'adresse : https://www.ookla.com/articles/5g-europe-mapping-the-future-q1-2022

[54] LEVY, Ian. *Security, complexity and Huawei; protecting the UK's telecoms networks* [PDF]. National Cyber Security Centre [en ligne]. 22 février 2019 [Consulté le 3 mai 2022]. Disponible à l'adresse : https://www.ncsc.gov.uk/blog-post/blog-post-security-complexity-and-huawei-protecting-uks-telecoms-networks

[55] AFP. *Les exportations allemandes en baisse.* Capital [en ligne]. 2 novembre 2022 [Consulté le 7 novembre 2022]. Disponible à l'adresse https://www.capital.fr/entreprises-marches/les-exportations-allemandes-en-baisse-1450830

[56] LAU Von Jörg. *"Accro à la Chine" : l'Allemagne s'inquiète de l'emprise de Pékin sur son économie.* Courrier International [en ligne]. 11 août 2022 [Consulté le 28 août 2022. Disponible à l'adresse : https://www.courrierinternational.com/une/economie-accro-a-la-chine-l-allemagne-s-inquiete-de-l-emprise-de-pekin-sur-son-economie

[57] SCHMITZ Rob. *Germany is building what's expected to become Europe's largest military*. Npr.org [en ligne]. 17 mars 2022 [Consulté le 15 juin 2022]. Disponible à l'adresse : https://www.npr.org/2022/03/17/1087137501/germany-is-building-whats-expected-to-become-europe-s-largest-military

[58] Groupe Vauban. *Les pièges du réarmement allemand pour la France*. La Tribune [en ligne]. 28 mars 2022 [Consulté le 17 mai 2022]. Disponible à l'adresse : https://www.latribune.fr/opinions/les-pieges-du-rearmement-allemand-pour-la-france-907088.html

[59] Reuters Staff. *Germany to support quantum computing with 2 billion euros*. Reuters [en ligne]. 11 mai 2021 [Consulté le 7 juillet 2022]. Disponible à l'adresse : https://www.reuters.com/article/us-germany-quantumcomputer-idUSKBN2CS0W9

[60] U.S. COMMERCIAL SERVICE. *Germany Country Commercial* Guide [PDF]. International Trade Administration [en ligne]. 2022 [Consulté le 10 septembre 2022]. p.18. Disponible à l'adresse : https://www.trade.gov/sites/default/files/2022-09/CCGGermany2022.pdf

[61] STUPP, Catherine. *German Industrial Firms Plan to Build Private 5G Networks*. The Wal Street Journal [en ligne]. 6 avril 2020 [Consulté le 5 avril 2022]. Disponible à l'adresse : https://www.wsj.com/articles/german-industrial-firms-plan-to-build-private-5g-networks-11586191739

ANNEXES

[1] En novembre 2021 IBM dévoile au monde son processeur Eagle à 128 quantum bits et promet un processor à 1121 qubits pour 2023. Source : IBM. *IBM Quantum breaks the 100-qubit processor barrier*. IBM blog [en ligne]. 17 novembre 2021 [Consulté le 4 septembre 2022]. Disponible à l'adresse : https://research.ibm.com/blog/127-qubit-quantum-processor-eagle

[2] GARISTO,Dan. *What Is the Future of Quantum-Proof Encryption?* Interview with Dustin Moody (NIST). IEEE [en ligne]. 8 juillet 2022 [Consulté le 4 août 2022]. Disponible à l'adresse: https://spectrum.ieee.org/post-quantum-cryptography-nist

Nous remercions l'ensemble de l'équipe pédagogique ainsi que le corps enseignant de l'EGE, plus particulièrement Béatrice Ghorra, Benjamin Pelletier, Fabien Renaudin et Nicolas Ravailhe pour leurs précieux conseils et le temps accordé.

Merci également à tous ceux qui ont joué le jeu de l'interview pour leur partage d'expérience.

Nous remercions également Tara.