
euratechnologies
EXCELLENCE & INNOVATION
Souveraineté numérique : enjeux, perspectives et préconisations à l'échelle de l'Europe
Mars 2022
hello lille
MEL
MÉTROPOLE
EUROPÉENNE DE LILLE

Executive Summary – La souveraineté numérique européenne (1/3)

Cet ExecSum sert d'introduction au concept de la souveraineté numérique européenne.
Ce rapport est divisé en deux parties, la première explique l'origine de la souveraineté numérique européenne, ses enjeux et ses axes d'amélioration. La seconde présente les différentes technologies et secteurs technologiques stratégiques de la souveraineté numérique européenne.

Une notion récente interrogeant la capacité d'autodétermination des Etats dans un monde interconnecté

- Le terme « **Souveraineté numérique** » provient de deux termes très actuels et présents dans les débats publics : la « souveraineté » pour un État, notamment, renvoie à son indépendance, à sa capacité à ne pas se voir imposer la volonté des autres en vertu du principe de non-ingérence, et de sa capacité à décider de sa propre liberté d'organisation interne. Le terme numérique renvoie à l'industrie technologique au sens large, incluant tant les acteurs du secteur que les politiques et la juridiction en la matière. En d'autres termes, le numérique représente-t-il pour les Etats un moyen d'asseoir leur souveraineté ou au contraire une menace qui contribue à l'étiolement de leur autorité ?
- Ces dernières années, les GAFAM (Google, Apple, Facebook devenu Meta, Amazon et Microsoft) et BATX (Baidu, Alibaba, Tencent et Xiaomi) ont, grâce à leur irrésistible montée en puissance, développé la capacité de concurrencer le pouvoir des États et d'affecter la liberté d'autodétermination des individus. Dans un cyberespace où les frontières n'existent pas ou ont tendance à devenir de plus en plus floues, la prise de conscience de cette hégémonie numérique a donné naissance à la notion de souveraineté numérique. La crise sanitaire n'a fait qu'amplifier et mettre en lumière les risques liés à la perte d'indépendance.
- Aujourd'hui, force est de constater que le numérique constitue plus une menace qu'une opportunité pour la souveraineté des États et leur capacité à s'autodéterminer. Ceci est d'autant plus visible dans un contexte européen où les politiques du numérique, non-harmonisées à l'échelle communautaire, ne permettent pas l'avènement de champions du numérique et contribuent à une forte vulnérabilité, particulièrement en matière de cybersécurité, au profit des autres puissances mondiales.

Executive Summary – La souveraineté numérique européenne (2/3)

Des défis majeurs à relever pour l'Union Européenne afin de garantir sa souveraineté numérique de manière pérenne

La souveraineté numérique est une question de choix. Pour garantir la liberté de choix et promouvoir l'indépendance numérique de l'Union européenne, des principes sont à observer et à mettre en œuvre :

- Prendre la maîtrise technologique dans les secteurs stratégiques et émergents du numérique ;
- Se protéger économiquement par la régulation et en légiférant ;
- S'assurer que nos infrastructures numériques soient indépendantes et résilientes ;
- Accélérer le développement d'écosystèmes numériques d'excellence, en investissant massivement dans le financement des start-up, de l'innovation et de la R&D, en favorisant les partenariats stratégiques privés et publics – privés intracommunautaires et, au besoin par souci de nécessité, avec des acteurs hors Union européenne ;
- Former au numérique tous les citoyens en développant et mettant en place de nouvelles formes d'apprentissage et de formation pour que chacun d'entre eux soit armé pour comprendre, utiliser, travailler et innover.

A l'heure actuelle, face aux nombreux défis qui s'imposent, l'Union européenne doit développer une politique numérique harmonisée à l'échelle des 27 Etats-membres et mettre en œuvre les actions suivantes :

- Sensibiliser les citoyens quant aux risques encourus ;
- Investir dans la R&D et contribuer massivement au financement de start-ups qui garantiront demain la protection de nos données ;
- Mettre en place les conditions pour faire émerger des champions du numérique européens ;
- Favoriser et promouvoir l'utilisation de produits européens ;
- Déployer un arsenal législatif adapté afin de préserver notre indépendance numérique.

Un niveau d'investissement trop faible en Europe comparé aux Etats-Unis et à la Chine, limite les efforts pour maintenir et garantir la souveraineté européenne

8 domaines sont présentés dans ce rapport :

Télécommunications	**L'informatique quantique**
Cloud-Computing	**Blockchain**
Cybersécurité	**Semi-conducteurs**
Intelligence Artificielle	**SpaceTech**

Actuellement plusieurs initiatives sont lancées par les différents gouvernements européens et par l'Union européenne afin de garantir et d'améliorer la souveraineté numérique européenne. L'UE a également mis en œuvre une législation adaptée afin de renforcer sa souveraineté numérique en ciblant les pratiques des acteurs de la « Big Tech », le développement des nouvelles technologies et l'utilisation acceptable de la technologie.

Toutefois, même si la réglementation est importante, elle ne suffit pas à favoriser l'innovation européenne, et souvent, elle n'aborde pas la question de la préférence pour des produits et solutions européens.

Si des investissements conséquents ont été réalisés afin de favoriser le développement de solutions et d'entreprises technologiques européennes, les niveaux d'investissement des secteurs public et privé restent encore trop faibles pour concurrencer les budgets chinois et américains. La conséquence est que les efforts européens visant à maintenir et à garantir la souveraineté et la sécurité numériques de l'UE sont en partie vains, puisque l'Europe continue de s'appuyer sur des solutions non-européennes.

Executive Summary – La souveraineté numérique européenne (3/3)

Nos recommandations

Au niveau Européen, il s'agit de

- Encourager **le développement de technologies « made in Europe »** à travers l'investissement, les partenariats européens entre acteurs du secteur public, du secteur public et secteur privé, ainsi que des mesures qui favorisent la production européenne. Créer des incitatifs et aménager la réglementation afin d'attirer des sites de production et de bureaux d'entreprises tech non-européennes ;
- Etablir un **Buy European Act**, de manière à ce que les produits et les solutions qui sont fabriqués ou développés au sein de l'UE soient préférés lors de l'attribution de certains marchés publics. Les investissements de ces marchés seront injectés dans l'économie de l'UE, permettront aux employés européens de se former aux technologies les plus récentes, aux entreprises européennes de se développer et de rentabiliser leurs efforts de R&D et contribueront ainsi aux objectifs de réindustrialisation et au renforcement de la souveraineté numérique puisque, de surcroit, les fournisseurs ou prestataires devront respecter les lois et réglementations européennes ;
- Soutenir la **croissance des acteurs technologiques européens** afin qu'ils puissent rivaliser avec les grandes entreprises technologiques non-européennes, au moyen de financements, de réductions d'impôts, d''attribution de marchés publics, et en accordant des avantages aux entreprises qui contractualisent avec ces acteurs. Une telle mesure renforcerait la souveraineté numérique européenne en offrant des **alternatives pertinentes et performantes aux solutions non-européennes** aux consommateurs, qui ,ainsi, ne verraient plus leur données privées échapper à la protection de la réglementation européenne.

Au niveau national, régional et métropolitain, il s'agit de

- Renforcer et optimiser les politiques d'innovation à travers les outils que les acteurs régionaux et métropolitains ont construits et développés lors des dernières décennies ;
- Améliorer la capacité à obtenir des subventions européennes afin de produire de la technologie locale et de contribuer à la souveraineté numérique;
- Développer l'implantation de sites de production et de développement, en s'assurant pour les sociétés hors UE, qu'elles s'engagent au respect de la souveraineté numérique européenne ;
- Faire le lien entre les acteurs locaux et les entreprises leaders du numérique.

Partie. 1 : Sommaire

La souveraineté numérique : un concept aux définitions variables, source d'enjeux stratégiques majeurs pour le monde de demain

La souveraineté numérique pour les États réfère à leur capacité à assurer leur sécurité domestique et extérieure d'un point de vue de politique sur le numérique

- Le concept de souveraineté trouverait son origine à la paix de Westphalie de 1648, qui met fin à la guerre de Trente Ans. Un État était considéré comme souverain s'il remplissait les trois principes de souveraineté :
  - **i) L'assurance de sa souveraineté extérieure** (la capacité d'assurer la protection de ses frontières et de son peuple),
  - **ii) L'assurance de sa souveraineté domestique** (la capacité de gouverner au sein de son territoire et d'y maintenir l'ordre),
  - **iii) Assurer un équilibre des pouvoirs avec les autres États, de sorte qu'il n'y ait pas d'hégémonie dans le système international ;**
- Au fil du temps, le concept de la souveraineté ainsi que ces trois principes qui déterminaient si un état était véritablement souverain ont été remis en question. Au cours des dernières décennies, la mondialisation, l'essor des multinationales, la création d'organisations supranationales ont remis en cause cette notion de souveraineté et ont parfois affaibli ou modifié la manière dont un état est souverain ;
- La souveraineté numérique est une idée popularisée par Pierre Belanger qui a été mentionnée dans la « *loi pour une république numérique* » de 2016, puis dans un rapport au Sénat en 2019. Ce rapport a défini la souveraineté numérique comme la capacité d'un État à agir dans le cyberespace, incluant donc divers sujets technologiques, dont l'infrastructure, les normes technologiques, les plateformes en ligne, le comportement en ligne ainsi que la technologie elle-même ;
- L'émergence de nouvelles technologies et de la montée en puissance d'acteurs faisant partie du monde de la technologie exercent une pression supplémentaire sur la souveraineté des États.

Mais qu'est-ce que cela veut dire pour l'Union européenne, composée de plusieurs États ?

- Pour l'UE et ses États membres, la souveraineté numérique est donc une idée politique, qui fait référence à la conception politique de la souveraineté des États. Dans cette conception de la souveraineté numérique, les acteurs politiques se concentrent sur la manière dont l'industrie technologique affaiblit la souveraineté des états ou comment la technologie peut être utilisée pour accroître celle-ci; c'est ce qui guide leurs décisions et leur stratégie envers le secteur du numérique ;
- Afin de combattre les atteintes à sa souveraineté, l'Europe a présenté la notion de la souveraineté numérique européenne, qui lui permettrait de ne plus être dépendante de logiciels et de matériels informatiques de pays tiers ou conçus par les acteurs de la « Big Tech » ;
- Pour Thierry Breton, commissaire européen chargé du marché intérieur, la souveraineté numérique repose sur : « *La puissance de calcul, le contrôle de nos données et une connectivité sécurisée* » ;
- Charles Michel, Président du Conseil européen, considère la souveraineté numérique comme un moyen d'atteindre l'autonomie stratégique de l'Europe, quelque chose qui consiste à « *pouvoir faire des choix…réduire nos dépendances, pour mieux défendre nos intérêts et nos valeurs* »
- **L'Europe entend parvenir à la souveraineté numérique en favorisant le développement de sa propre infrastructure technologique et de sa propre économie numérique, tout en veillant à ce que les valeurs démocratiques et fondamentales de l'Union européenne se reflètent dans les solutions numériques européennes.**

La souveraineté numérique et les individus : avons-nous vraiment le choix ?

Pour les citoyens et les résidents de l'UE, la souveraineté numérique concerne moins la dimension géopolitique de la dépendance de solutions numériques des pays tiers, et se concentre davantage sur la possibilité d'avoir plusieurs options de solutions numériques. La souveraineté numérique européenne permettrait aux citoyens de ne pas être confrontés à une situation où ils doivent renoncer à une partie de leur vie privée et de leurs informations personnelles afin d'utiliser des solutions ou des technologies performantes.

La technologie est un outil pour les populations…

- La souveraineté numérique est considérée comme un moyen de renforcer la compétitivité des acteurs technologiques européens, d'améliorer la position de l'Europe dans la sphère internationale, mais aussi de protéger les valeurs de l'UE dans le domaine numérique, à savoir la liberté, la démocratie et le respect des droits de l'homme ;
- Les dirigeants de l'UE ont fait valoir que la souveraineté technologique vise également à protéger la culture et les valeurs européennes, dans lesquelles l'autonomie de l'humain est privilégiée en mettant l'accent sur les droits souverains des citoyens sur leurs données et lors de leurs interactions avec l'IA ;
- En outre, les systèmes et applications d'intelligence artificielle considérés comme portant atteinte au libre-arbitre des personnes seront prohibés en vertu du cadre réglementaire proposé par la Commission européenne pour l'IA. Les personnes devront aussi être averties lorsqu'elles interagissent avec une IA plutôt qu'avec une personne physique.

Une prise de conscience grandissante

… mais elle soulève des inquiétudes concernant la confidentialité des données

- Les révélations de Snowden en 2013 ont démontré l'étendue des systèmes de surveillance exploités par la National Security Agency américaine en partenariat avec plusieurs agences nationales d'intelligence et plusieurs acteurs commerciaux dans le monde entier. **Ces révélations ont suscité des inquiétudes quant à la confidentialité des données et ont montré comment le monde du numérique était utilisé à des fins géopolitiques** ;
- Les Européens sont de plus en plus conscients de l'importance de la confidentialité de leurs données, comme l'illustre l'enquête 2020 de l'Agence des droits fondamentaux de l'Union européenne, où **55 % des personnes interrogées ont dit être préoccupées par le fait que des criminels puissent accéder à leurs données et informations personnelles**, et **où 69 % des personnes interrogées ont déclaré avoir entendu parler du RGPD ;**
- Le **RGPD est perçu comme un texte de loi qui protège la confidentialité des données des utilisateurs**, car il limite la collecte excessive de leurs données et permet de refuser une partie de leur collecte.

Le numérique, un enjeu stratégique de premier ordre pour les superpuissances mondiales dessinant les relations internationales

Les relations entre les États et les acteurs « Big Tech »

- La création du poste d'ambassadeur de la technologie au sein du gouvernement danois en 2017 et d'un rôle similaire au sein du gouvernement britannique en 2020 signalent **un changement dans la manière dont les gouvernements abordent les grandes entreprises technologiques** et reflètent leur influence croissante. Ces deux postes sont situés à San Francisco, le centre de la Silicon Valley, plaque tournante de l'industrie technologique américaine. Ces ambassadeurs ont pour vocation de communiquer avec les acteurs via des canaux qui leur sont dédiés, et visent à promouvoir les intérêts de leur pays auprès des grandes entreprises technologiques américaines, en **élevant ces dernières à un statut similaire à celui d'un État-nation** ;
- Microsoft dispose d'un bureau de représentation auprès de l'ONU à New York et d'un bureau dédié aux affaires gouvernementales européennes à Bruxelles, ce qui démontre le lobbying grandissant de ces entreprises dans l'élaboration des politiques européennes.

L'autonomie stratégique

- La notion d'une « *l'autonomie stratégique* européenne » n'est pas nouvelle. Le terme a initialement été utilisé pour discuter des stratégies de l'UE en matière de politique spatiale, de sécurité et de défense, et pour améliorer les capacités militaires de l'UE. L'idée de « *l'autonomie stratégique* » renvoie à ce que l'UE devrait être bien dotée militairement, être en capacité de mener des opérations de gestion de crise de taille modeste, hors zone, particulièrement en Europe, sans l'intervention de l'OTAN ou des Etats-Unis;
- Cette notion s'est depuis élargie pour englober le domaine du numérique en s'intéressant notamment au protectionnisme technologique et au renforcement des capacités européennes dans les domaines de la numérisation, des données, de l'espace, de l'énergie et des technologies émergentes ;
- **Le discours sur la souveraineté numérique est que l'Europe doit préserver son leadership et son autonomie dans divers domaines technologiques clés, afin d'éviter les dépendances et la coercition géopolitique dans les secteurs technologiques en tension** ;
- **L'ensemble des concepts tels que la souveraineté technologique, la souveraineté numérique et la souveraineté des données font écho à la notion de souveraineté numérique européenne.**

La compétition entre États dans la sphère numérique

- Le système international a été décrit comme une arène où les États sont en concurrence permanente les uns avec les autres pour réaliser des gains marginaux. **Dans un monde devenant de plus en plus multipolaire, l'Union européenne doit permettre aux États européens d'exercer une influence politique sur la scène internationale** ;
- Les États entendent utiliser les nouvelles technologies pour se faire entendre sur la scène internationale. Le développement de certaines technologies leur permettra d'être économiquement plus compétitifs et moins dépendants d'autres pays impliqués dans la chaîne de production des technologies (cas des semi-conducteurs). Le développement de nouvelles technologies dans les domaines des cyberarmes, de la cyber résilience, ainsi que du quantique, permettra aux États européens de renforcer leur puissance militaire.

Les investissements étrangers constituent-ils une menace pour la souveraineté numérique européenne dans la mesure où ils pallient le faible investissement européen ?

Un niveau d'investissement trop faible dans l'UE comparé aux acteurs non-européens…

- Malgré les efforts de l'UE, les investissements européens dans le développement de nouvelles technologies qui permettraient à l'Europe d'être moins dépendante des entreprises technologiques non-européennes sont encore insuffisants ;
- À titre d'exemple, **l'UE a consacré un total de 4 à 5 milliards d'euros à la recherche et au développement de l'intelligence artificielle, alors que les gouvernements chinois et américain y consacrent environ 30 à 40 milliards d'euros par an.** Par ailleurs, le think tank Bruegel a estimé que les objectifs européens en matière d'investissements et de subventions pour le développement des semi-conducteurs étaient faibles par rapport à ceux d'autres acteurs. A titre d'exemple, **Thierry Breton, commissaire européen pour le marché intérieur, visait un investissement de 20 à 30 milliards d'euros d'ici 2030, tandis que le gouvernement sud-coréen prévoit un objectif de 400 milliards de dollars d'ici 2030** ;
- Les investissements dans les start-up en Asie et en Amérique du Nord sont plus élevés qu'en Europe, ce qui limite la croissance des start-up et freine l'innovation. **En novembre 2021, les start-up nord-américaines ont levé un total de 32,2 milliards de dollars, les start-up asiatiques un total de 19,4 milliards de dollars, tandis que le montant des levées de fonds des start-up européennes s'établit à 7,9 milliards de dollars** ;
- Le plus faible niveau d'investissements du secteur public et du secteur privé en Europe a un impact sur la souveraineté numérique européenne. Elle limite la croissance et le développement de solutions et d'acteurs européens dans les domaines technologiques, induisant une dépendance persistante à l'égard de solutions non-européennes.

…parallèlement les acquisitions et investissements dans l'UE proviennent principalement de l'étranger

- **Les capitaux d'investissement dans les start-up européennes proviennent souvent de l'extérieur de l'Europe, constituant une menace pour les pays européens, leurs pépites pouvant être acquises avant d'avoir atteint leur plein potentiel**. La souveraineté technologique des gouvernements en pâtit, car l'acquéreur devient propriétaire des brevets et de la technologie développée par l'entreprise acquise ;
- Les entreprises qui produisent des technologies considérées comme "stratégiques" par les acteurs étatiques font souvent l'objet d'offres d'acquisition, comme en témoigne l'acquisition de plusieurs entreprises européennes (Unity Semiconductor, Huba Control, AMS) spécialisées dans la fabrication de semi-conducteurs par Wise Road Capital, un fonds d'investissement chinois qui a des liens avec le gouvernement chinois ;
- À la suite de l'acquisition de Kuka, un fabricant allemand de robots par la société chinoise Midea en 2017, la commissaire européenne chargée de la concurrence et du numérique, **Margrethe Vestager**, a déclaré que les **États européens devraient acheter des parts dans des entreprises européennes qui produisent de la technologie « stratégique » afin d'empêcher les rachats par des entités étrangères**. En 2020, le gouvernement français a bloqué l'acquisition de Photonis, une entreprise technologique française spécialisée dans la conception, la fabrication et la vente de technologies d'imagerie par photocapteurs, par l'entreprise américaine Teledyne, en invoquant le fait que la vente de cette entreprise (seul fournisseur de caméras de vision nocturne des forces armées françaises), présentait une **"vulnérabilité" élevée en matière de sécurité nationale pour la France.**

Recommandations

- **La comparaison entre les niveaux d'investissement en Europe, aux Etats-Unis et en Chine démontre qu'à moins d'une augmentation significative du niveau d'investissement européen dans les nouvelles technologies, les acteurs du secteur technologique doivent continuer à accepter les investissements étrangers si l'écosystème technologique européen souhaite rester compétitif. Le contrôle des investissements étrangers dans les secteurs stratégiques ne devrait pas être systémique, car cela nuirait encore davantage au développement de la technologie européenne.**
- **L'UE devrait chercher à promouvoir l'investissement de la part du secteur privé dans la recherche et le développement, y compris de la part d'acteurs non-européen. Il est crucial d'augmenter le financement de la R&D afin de permettre la création de technologies européennes, de supporter un écosystème d'innovation dynamique, d'attirer et retenir les talents en Europe. L'UE devrait accueillir et chercher à attirer les investissements étrangers, tout en assurant leur réglementation, pour assurer que les résultats d'une collaboration en matière de recherche restent à la disposition de l'Europe.**

Travailler avec des acteurs technologiques non-européens tout en assurant la souveraineté numérique européenne et en favorisant les technologies « made in Europe »

Appel à la souveraineté numérique tout en restant réaliste

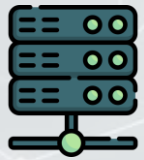
- Il serait tentant d'appeler au boycott des acteurs technologiques non-européens et de remplacer leurs produits et solutions par des alternatives européennes comme le suggèrent les récentes déclarations de la part de plusieurs personnalités politiques européennes en réaction aux menaces de Meta de retirer Instagram et Facebook d'Europe. Pour autant, ces mesures sont peu réalistes, les grands acteurs non-européens du secteur informatique sont impliqués dans presque toutes les phases de la chaîne d'approvisionnement et dans tous les secteurs d'activité. Bien que les acteurs « Big Tech » ne bénéficient pas d'une bonne réputation à la suite de différentes révélations concernant leurs agissements, sur un plan strictement économique et sans solution alternative européenne disponible à l'heure actuelle, s'en passer viendrait à priver plusieurs milliers d'entreprises de leurs outils de travail et les conséquences en seraient désastreuses. Par ailleurs, même si ces solutions alternatives existaient ou venaient à exister, la transition ne pourrait se faire que dans la durée. Sur un plan sociétal, est-il vraiment réaliste d'envisager que les millions d'utilisateurs européens de Facebook, Twitter, Whatsapp et consorts les quittent du jour au lendemain pour une solution alternative européenne ?

Coopération entre acteurs européens et non-européens

- Il semblerait que le meilleur compromis soit de travailler avec les acteurs technologiques non-européens en les incitant, lorsque leurs sites sont sur le sol européen, à respecter les législations et règlements européens en matière de souveraineté numérique;
- L'idée française d'un « cloud de confiance » a permis que des partenariats entre des acteurs du numérique français et de la « Big Tech » se forment comme celui de Thales et Google Cloud. L'offre commune réunira les technologies et services cloud de chacun des partenaires, Google Cloud amenant l'infrastructure logicielle et les applications, Thales la gestion des accès et des identités et la supervision cyber. Ce « cloud de confiance » sera opéré sur une infrastructure matérielle exploitée en France par une coentreprise de droit français, détenue majoritairement par Thales, non soumise au Cloud Act Américain;
- En établissant un « Buy European Act », l'UE pourrait pousser les entreprises technologiques non-européennes à une délocalisation de leur production en Europe pour être en mesure de répondre aux appels d'offres européens;
- Le développement de réglementations qui suivent l'esprit du RGPD et qui visent à protéger les droits des citoyens européens sur d'autres territoires contribuerait à garantir la souveraineté numérique européenne. Ceci permettrait d'assurer une situation équitable puisque les entreprises non-européennes en Europe seraient soumises aux mêmes règles que les entreprises européennes ;
- Intel, l'entreprise technologique américaine connue pour sa production de composants et de processeurs informatiques, ouvrira un site de production de semi-conducteurs en Irlande en 2023 et a déclaré qu'elle comptait investir 80 millions d'euros en Europe sur une période de dix ans pour l'établissement de deux autres usines de fabrication de puces.

Les dominations des acteurs non-européens dans le secteur du numérique représentent des sources d'inquiétudes grandissantes pour la souveraineté numérique européenne (1/2)

- Ces chiffres illustrent la domination des entreprises technologiques américaines dans le monde et en Europe. Les 5 grandes entreprises, souvent désignées par l'acronyme GAFAM, maintenant GAMAM (Google, Apple, Facebook maintenant appelé Meta, Amazon et Microsoft) ont connu un tel développement qu'elles dominent différents secteurs technologiques et disposent par conséquent d'une grande influence politique, financière et sociale sur la société européenne. Cette position dominante, de plus en plus mal perçue par les citoyens et les décideurs européens, freine également la croissance des entreprises technologiques européennes. L'UE et un certain nombre de pays européens ont donc décidé de réglementer les secteurs activités dans lesquels ces entreprises opèrent.



92%

des données du monde occidentales sont stockées sur des serveurs américains.

91.9%

de part de marché mondiale des moteurs de recherche détenue par Google, qui détient également 63,06 % de part de marché mondiale des navigateurs.

39%

des investissements dans les start-up européennes proviennent de l'extérieur de l'Europe, en grande partie des États-Unis.

Le secteur technologique américain vaut plus que les marchés boursiers des 27 Etats membres de l'UE réunis.

2/25

Seulement deux entreprises européenne figure parmi les 25 plus grandes capitalisations boursières d'entreprises technologiques (SAP et ASML).

32%

est la part de l'infrastructure Cloud mondial détenue par AWS au premier trimestre 2021. Microsoft Azure en détenait 20 %, Google Cloud 9%, Alibaba Cloud 6 % et IBM Cloud 5%.

29.49%

des ventes mondiales de smartphones étaient de marque Apple en janvier 2022, devant Samsung (27,18%), Xiaomi (11,54%), Huawei (6,64%), Oppo (5,29%) et Vivo (4,26%) .

Alphabet **136 Mrds $**

le montant de la trésorerie dont Alphabet Inc. disposait en juin 2021. Microsoft disposait alors de 130 milliards de dollars, suivi par Amazon (90 milliards), Meta (64 milliards) et Apple (62 milliards).

Les dominations des acteurs non-européens dans le secteur du numérique représentent des sources d'inquiétudes grandissantes pour la souveraineté numérique européenne (2/2)

329 Mrds $

de revenus cumulés des entreprises Huawei, Baidu, Alibaba, Tencent, Xiaomi en 2018. Comparativement, les revenus cumulés des **GAMAM** cette année-là était de **801 milliards de dollars.**

10 Mrds $

d'investissement par Tencent Holdings en Europe en 2020.

20%

d'augmentation de trafic sur le site web d'AliExpress en 2020. La firme chinoise de commerce électronique a réalisé 31 milliards de dollars rien qu'en Espagne en 2020.

1 Mrd

d'utilisateurs actifs sur TikTok en janvier 2022, une croissance impressionnante puisque la société a faisait état de 55 millions d'utilisateurs en janvier 2018.

les entreprises technologiques chinoises poursuivent leur croissance. En 2018, le CA de Baidu a augmenté de 28 % contre 23 % pour Alphabet, Alibaba de 58 % contre 31% pour Amazon, Tencent de 56 % contre 47% pour Facebook, et Xiaomi de 67 % contre 16% pour Apple.

Le CERT-FR a mis en garde contre l'utilisation d'outils développés par des entreprises russes et a spécifiquement fait référence à Kaspersky, indiquant que la sécurité de ces outils étaient remise en question en raison des liens que l'entreprise a avec le gouvernement russe. En 2017 le gouvernement américain a interdit l'utilisation des logiciels Kaspersky dans les systèmes d'information du gouvernement fédéral.

19%

...la part de marché que Samsung dans les livraisons mondiales de smartphones au quatrième trimestre 2021. L'entreprise sud-coréenne détient également 13 % des parts de marché dans l'industrie mondiale des semi-conducteurs.

48%

des équipements de réseau d'accès radio (RAN) 4G dans les 31 pays européens analysés par Strand Consult provenaient de fournisseurs chinois.

L'Union européenne a déployé une série de mesures afin d'assurer et sécuriser sa souveraineté numérique… avec un succès relatif (1/3)

Rapport de l'UE sur la souveraineté numérique européenne

- Publié par le Parlement européen en 2020, **ce rapport soulignait que les citoyens, les entreprises et les États membres européens étaient de plus en plus inquiets de la perte de contrôle de leurs données, de leur capacité à stimuler l'innovation et de leur capacité à élaborer et à faire appliquer la législation dans le domaine du numérique** ;
- La présidente de la Commission européenne, Ursula von der Leyen, a fait de la politique numérique de l'Europe l'une des priorités de son mandat et a affirmé que l'Europe devait parvenir à une « *souveraineté technologique* » dans les domaines jugés critiques ;
- Dans le contexte d'une Europe qui dépend de solutions offertes par des entreprises technologiques non-européennes et qui est confrontée à leur forte influence sociale et économique, la « *souveraineté numérique européenne* » fait référence à la capacité de l'Europe à agir de manière indépendante dans le domaine numérique ;
- Le rapport avance qu'il existe un soutien croissant pour cette idée de souveraineté numérique, poussant l'UE à prendre des mesures pour renforcer son autonomie stratégique dans le domaine numérique et faire en sorte que l'UE actualise et adapte ses instruments réglementaires et financiers pour promouvoir les valeurs européennes dans divers développements et domaines technologiques.

Le règlement général sur la protection des données de l'UE

- Entré en vigueur en 2018, promulgué comme la « *loi la plus sévère au monde en matière de confidentialité et de sécurité* », **le RGPD impose des obligations aux organisations qui ciblent ou collectent des données liées aux résidents de l'UE** ;
- Il stipule que le traitement des données doit être légal, transparent et équitable pour les utilisateurs, et que seules les données nécessaires aux fins spécifiques légitimes spécifiées à l'utilisateur doivent être stockées et que ces données ne doivent être stockées que pendant la période requise pour cette finalité spécifique ;
- **Les amendes pour violation du RGPD sont plafonnées à 20 millions d'euros ou à 4 % du chiffre d'affaires d'une organisation (le montant le plus élevé étant retenu)** ;
- Du 28 janvier 2021 au 22 janvier 2022, les autorités de protection des données de l'UE ont infligé un total de 1,2 milliards de dollars d'amendes, tandis que les notifications de violations de données des entreprises ont augmenté de 8 % au cours de cette période. **Les Big Tech ont été largement impacté par ce règlement, le Luxembourg ayant infligé une amende de 746 millions d'euros à Amazon et les autorités irlandaises une amende de 225 millions d'euros à Meta** ;
- Si le RGPD a été efficace pour sensibiliser à la confidentialité des données, certaines entreprises ont affirmé qu'il y avait une certaine ambiguïté concernant la conformité. **Un rapport de 2018 d'EY et de l'IAPP a révélé que les entreprises prévoyaient de dépenser 1,3 millions de dollars par an pour se mettre en conformité avec le RGPD**. Certaines entreprises affirment que la loi a eu des conséquences négatives sur leur croissance. De plus, chaque pays nomme une autorité de protection des données qui veille à l'application du RGPD, ce qui signifie qu'il n y a pas d'approche uniforme sur ce sujets. Par conséquence, certains pays infligent plus d'amendes que d'autres ;
- **La crainte des amendes élevées et les impacts négatifs d'une violation de la réglementation sur l'opinion public ont contribué à renforcer l'efficacité de la réglementation en incitant les entreprises à modifier leurs pratiques.**

L'Union européenne a déployé une série de mesures afin d'assurer et sécuriser sa souveraineté numérique… avec un succès relatif (2/3)

Horizon Europe

- Doté d'un budget de **95,5 milliards d'euros**, ce programme facilite la collaboration PME/ETI, grands groupes et laboratoires et renforce l'impact de la recherche et de l'innovation dans l'élaboration et la mise en œuvre des politiques de l'UE. Le programme soutient également la création et la diffusion des connaissances et des technologies. **Le programme vise à stimuler la capacité d'innovation la compétitivité, et la croissance de l'emploi en Europe, et à assurer la souveraineté numérique européenne ;**
- **Le Conseil européen de l'innovation fait partie de ce programme**, il identifie et soutient les solutions technologiques de pointe afin de créer de nouveaux marchés et de se développer au niveau international. L'EIC dispose d'un budget de 10 milliards d'euros et propose cinq modes de financement différents ;
- **Horizon Europe** et les initiatives similaires qui visent à fournir un financement public à l'innovation technologique sont une occasion de stimuler la compétitivité européenne, mais aussi, par effet indirect, de contribuer à la croissance des Big Tech : **bon nombre des projets de start-up ou d'entreprises européennes s'appuient sur leurs offres technologiques. Le secrétaire général de Cispe, une fédération européenne de** fournisseurs de clouds, **confirme qu'une partie des 150 milliards d'euros de fonds publics alloués au secteur numérique**, arriveront dans la poche des GAFAM.

Le Digital Services Act Package de l'UE

- **Le Digital Services Act Package de l'UE est une proposition législative faite par la Commission européenne en décembre 2020 pour la création d'un espace numérique plus sûr, où les droits des utilisateurs sont garantis, et d'un terrain d'expérimentation sécurisé pour les entreprises** ;
- La **loi sur les services numériques (DSA)** entend réglementer et renforcer la transparence des intermédiaires, des réseaux sociaux, des stores d'applications et des plateformes en ligne (partage de contenu, voyagistes, etc…) : **ils seront tenus expliquer le fonctionnement de leurs algorithmes, seront davantage responsables du contenu publié et auront l'obligation de retirer les contenus jugés illicites** ;
- La **loi sur les marchés numériques (DMA)** propose des règles qui régissent les gatekeepers qui jouent un rôle systémique dans le marché intérieur et qui font office de goulots d'étranglement entre les entreprises et les consommateurs pour des services numériques importants. **La DMA vise à garantir que les grandes plateformes en ligne ne fonctionnent pas comme un oligopole et n'abusent pas de leur pouvoir** ;
- Le DMA et le DSA sont deux projets de l'UE pour réglementer le comportement perçu comme abusif des grandes entreprises technologiques. **Ainsi, le gouvernement français espère faire adopter ces deux propositions pendant la présidence française de l'UE.**

L'Union européenne a déployé une série de mesures afin d'assurer et sécuriser sa souveraineté numérique… avec un succès relatif (3/3)

Imposition

- Les principaux acteurs de l'industrie technologique ne se contentent pas de dominer les marchés européens, **ils utilisent à leur avantage le manque d'uniformité des règles d'imposition dans l'UE et paient ainsi un montant d'impôts bien inférieur à celui payé par les entreprises locales de taillent identiques, quelque soit le secteur d'activité. Cette pratique constitue aussi une atteinte à la souveraineté des États de l'UE** ;
- Grace au numérique, les entreprises peuvent tirer des revenus dans des juridictions où elles n'ont pas nécessairement une présence physique, ce qui déclenche habituellement l'assujettissement à l'impôt local ;
- **En 2018, la France a tenté de créer une taxe sur les services numériques au niveau européen, mais devant le refus d'un certain nombre d'États membres, la France a décidé de l'appliquer sur son seul territoire. Cet taxe de 3% sur le chiffre d'affaires brut des plateformes numériques générant plus de 750 millions d'euros, aurait du entrer en vigueur en 2020. Devant les menaces américaines d'imposer des droits de douane à hauteur de 2,4 milliards de dollars sur les marchandises françaises, la France a décidé de surseoir à** son application. Depuis, c'est le statut-quo qui, bien sur, profite aux Big Tech ;
- **En 2021, l'OCDE a réussi à établir un consensus mondiale pour réformer le taux d'imposition international des sociétés. Ce consensus stipule que les multinationales (dont les Big Tech) dont le revenu est supérieur à 750 millions d'euros seront soumises à un taux d'imposition minimum de 15 %.** Son entrée en vigueur est prévue en 2023.

Des pistes de réflexion pour sécuriser notre souveraineté numérique : développer une technologie "Made in Europe" et un "Buy European Act"

Tech « Made in Europe »

Définition et enjeux

- Le « *Made in Europe* » ne fait pas uniquement référence aux technologies développées par des acteurs européens, mais englobe l'ensemble des **technologies produites et développées au sein de l'Union européenne, quelque soit la nationalité de l'acteur.** En outre, il impose aux opérateurs et propriétaires des technologies « *Made in Europe* » de **respecter les règles et les valeurs de l'Union européenne.**
- **Ce label « *Made in Europe* » aurait la faculté de soutenir l'innovation technologique européenne, de favoriser l'emploi européen, de contribuer à l'effort européen de réindustrialisation, et serait en mesure d'apaiser les inquiétudes concernant la souveraineté des données.**
- **Localiser la production de technologies sur le sol européen atténuerait le risque de perturbation des approvisionnements ou des matériaux en raison de crises comme celle du Covid ou d'une influence venu de l'extérieure. Cela permettrait également d'accroître le niveau de contrôle de l'UE sur les processus de production, renforçant ainsi l'autonomie stratégique et la souveraineté européenne.**

Initiatives passées et présentes

- **L'Alliance européenne pour les matières premières**, annoncée en septembre 2020, est un groupe d'industriels qui souhaite sécuriser les approvisionnements européens de métaux stratégiques et de terres rares, utilisés notamment pour la fabrication de batteries et d'équipements pour les énergies renouvelables. **L'UE dépend actuellement de la Chine pour la production de batteries, puisque 93 % du magnésium nécessaires à leur production sont importés de ce pays.**
- La COVID 19 a mis en évidence la forte dépendance, en particulier de l'Asie, de l'UE pour son approvisionnement en semi-conducteur. L'UE a donc décidé d'augmenter sa capacité de production afin qu'elle représente 20% de la production mondiale, contribuant ainsi à sa réindustrialisation, au « Made in Europe » et au renforcement de sa souveraineté numérique.

Informations supplémentaires

- En 2005 une tentative de créer ce label « *Made in Europe* » a vu le jour dans le cadre de la proposition d'un règlement sur l'identification de l'origine de certains produits. Le label « *Made in Europe* » serait l'équivalent d'une appellation d'origine protégée, **indiquant qu'un produit est principalement fabriqué dans l'UE. Cependant, ce label se révèle être plus un outil marketing, dont la mise en œuvre est complexe, et, finalement peu utilisé.**
- **Il est important de garder à l'esprit la complexité du secteur informatique, qui se compose de nombreux types d'acteurs et de technologies. Il serait impossible de tout produire en Europe tout en fournissant aux citoyens et aux industries européennes les dernières technologies avec un service de haute qualité. C'est pourquoi il est important que l'UE évite toute tentation techno-nationaliste.**

Recommendation sur l'open-source

L'Open-Source, un vecteur de la souveraineté numérique européenne

- L'open-source est un code source accessible librement aux utilisateurs ce qui leur permet de l'étudier, de le modifier et de le redistribuer dans l'atteinte d'objectifs multiples. Ce modèle de développement logiciel décentralisé encourage la collaboration et améliore la transparence ;
- L'open-source peut être un outil pour la souveraineté et possède un grand potentiel pour la stratégie numérique de l'Europe, en servant d'alternative aux logiciels propriétaires. L'open source permet aux utilisateurs de faire leurs propres choix technologiques et est souvent associé à l'interopérabilité et à la portabilité ouverte ;
- Le développement de la technologie en open-source est une réelle opportunité pour la création de start-ups, car elles peuvent développer de nouvelles solutions basées sur cet écosystème libre et ouvert beaucoup plus facilement, comme le démontre une récente étude de la Commission européenne.

Des pistes de réflexion pour sécuriser notre souveraineté numérique : développer une technologie "Made in Europe" et un "Buy European Act"

	Définition	Initiatives passées et présentes	Informations supplémentaires
« Buy European Act »	▪ Le « *Buy European Act* » est **une mesure permettant aux gouvernements et administrations publiques européennes de privilégier l'achat de solutions et de produits innovants fabriqués et développés en Europe.** ▪ Les partisans du « *Buy European Act* » plaident pour la mise en place d'un quota pour les solutions et les produits européen, et argumente **qu'une mesure comme celle-ci contribuerait à renforcer l'industrie européenne, à soutenir l'emploi européen et à améliorer la souveraineté numérique européenne.**	▪ L'idée d'un « *Buy European Act* » n'est pas nouvelle, elle fut évoquée pour la première fois au sein de l'Assemblée nationale en 1993. ▪ En 2012, le Président français Nicolas Sarkozy a proposé la mise en place d'un quota de marchés publics européens qui seraient réservés aux PME européennes. Cette proposition sera vite écartée par les instances européennes. ▪ En 2017 le Président français Emmanuel Macron propose une initiative similaire, où les administrations publiques et les autorités européennes réservent des contrats aux entreprises ayant au moins plus de la moitié de leurs opérations de production situées en Europe. Malgré l'opposition de l'UE, le Président Macron réaffirme sa position dans un message à la population française en 2019 ; **argumentant que l'UE devrait assumer une préférence pour les entreprises et les solutions européennes lorsqu'il s'agit d'industries stratégiques et de marchés publics, comme le font la Chine et les Etats-Unis.**	▪ Le « *Buy European Act* » s'inspire largement du Buy American Act, qui réserve l'accès aux contrats de certains marchés publics aux entreprises américaines. ▪ Une législation similaire existe en Chine, où en août 2021 il fut révélé que le gouvernement chinois avait publié de nouvelles directives obligeant les hôpitaux, les entreprises et les acheteurs publics chinois à acheter des produits fabriqués en Chine lorsqu'il s'agissait de certains produits.

Les défis actuels et futurs de la souveraineté numérique européenne dans différents secteurs industriels et technologiques

Part. 2 : Table des matières

Les défis actuels et futurs de la souveraineté numérique européenne dans différents secteurs industriels et technologiques

euratechnologies
EXCELLENCE & INNOVATION

Domaine #1 : Télécommunications

Télécommunications

Définition	▪ Il s'agit de **technologies permettant la transmission d'informations** ; ▪ Ces technologies ont évolué au fil du temps : l'information était autrefois transmise par le télégraphe, puis par les ondes radio, les transistors, les réseaux informatiques et l'internet via les réseaux locaux. Avec l'avènement des communications sans fil, elle est transmise à l'aide de réseaux cellulaires, de l'internet sans fil en recourant à des équipements tels que des antennes, des satellites et des fibres optiques pour les longues distances.
Pourquoi ce domaine est-il essentiel ?	▪ Ces technologies sont considérées comme **stratégiques car elles assurent la continuité des affaires, des services publics et des échanges sociaux par la transmission fluide des données et des informations entre les pays et régions**; ▪ **La sécurité des réseaux de télécommunication et qu'ils ne soient pas utilisés à des fins d'espionnage ou de surveillance sont des enjeux majeurs et stratégiques pour assurer la** souveraineté numérique européenne ; ▪ **La majeure partie du trafic Internet intercontinental mondial circule sur des câbles sous-marins, posés sur les fonds océaniques**. Cette infrastructure et ses installations de contrôle terrestres, propriété d'opérateurs privés ou d'états, sont également considérées comme une cible potentielle pour la collecte de données sensibles à des fins d'espionnage, ou de destruction partielle ou totale dans le cadre d'activités terroristes ou de conflit armé. Leur intégrité et leur protection sont des enjeux de cybersécurité cruciaux et indispensables pour garantir une souveraineté numérique.

Les problématiques existantes liées à la souveraineté numérique européenne dans ce domaine

- **Le déploiement de réseaux mobile 5G par Huawei est controversé depuis que Washington a accusé l'entreprise d'avoir des liens avec le gouvernement chinois et que l'utilisation de la technologie d'Huawei est un risque pour la sécurité nationale.** En conséquence, Huawei a été banni des réseaux 5G aux Etats-Unis, en Australie, en Nouvelle-Zélande, et plus récemment au Royaume-Uni ;
- Les pays européens ont également subi des pressions de la part du gouvernement américain pour interdire Huawei de leurs réseaux 5G
- En 2019, la France a voté une loi obligeant les opérateurs souhaitant déployer des réseaux 5G à demander une autorisation au gouvernement français pour chaque ensemble d'équipements et pour chaque zone géographique dans laquelle ils souhaitent installer de l'infrastructure 5G. En vertu de cette loi, le gouvernement français a délivré des autorisations pour l'utilisation d'équipements Huawei dans certaines zones, et a rejeté d'autres demandes.
- **En 2020, l'UE a initié la « *boite à outil 5G* », des mesures qui visent à atténuer les risques et qui prévoient notamment d'éviter les dépendances majeures sur un seul fournisseur.**

- En mai 2021, le radiodiffuseur public danois DR a révélé que de 2012 à 2014, **la NSA** (Agence nationale de sécurité américaine) **avait mis sur écoute des dirigeants suédois, norvégiens, français et allemands.**
- L'opération d'espionnage, baptisée **Opération Dunhammer**, a été **menée avec l'accord des services secrets danois**.
- Le Danemark étant le point d'atterrissage de plusieurs câbles transatlantiques et un point de transit pour les câbles terrestres européens, **la NSA a mis sur écoute ces câbles sous-marins à l'aide d'un système d'interception appelé Xkeyscore**, depuis une base située à Sandagergårdan, près de Copenhague.
- XKeyscore est **en mesure de surveiller l'ensemble du trafic Internet et mobile ainsi que d'intercepter des communications** telles que des courriels, des appels téléphoniques, des SMS et des messages de **discussion envoyés aux numéros de téléphone et aux adresses mail** de dirigeants européens, et probablement bien plus.
- Si l'espionnage interétatique n'est pas vraiment une nouveauté, le fait que les informations concernant les tracés des câbles sous-marins et leurs points d'atterrissage soient publiques **fait craindre de nouvelles menaces**. Un **groupe terroriste** disposant des ressources nécessaires **pourrait mener des actions de piratage, endommager ou détruire ces installations**.

Télécommunications

Initiatives européennes

- Observatoire européen de la 5G : Lancé en 2018, l'Observatoire européen de la 5G a initialement évalué l'atteinte des objectifs fixés par le plan d'action 5G. L'un de ces **objectifs** était de **favoriser une approche européenne coordonnée de la 5G** avec la **libération des bandes de fréquences pionnières de la 5G** et d'avoir des lancements commerciaux d'ici 2020. Actuellement dans sa troisième phase, l'Observatoire se concentre principalement sur la **boîte à outils de sécurité 5G** et sur les objectifs de l'UE fixés par son **initiative de Décennie numérique**, qui comprennent : la **couverture 5G de toutes les zones habitées** d'ici 2030, le **déploiement paneuropéen de corridors 5G**, la **limitation de la dépendance à l'égard d'un seul fournisseur** 5G et **l'amélioration de la sécurité des réseaux** 5G. L'Observatoire examine des questions telles que la couverture 5G, l'attribution du spectre et les politiques publiques pour stimuler la croissance de la 5G ;
- Plan d'action de l'UE en faveur de la 5G : Une initiative stratégique de l'UE qui vise à mettre en œuvre la 5G au sein de l'UE. Établi par la Commission européenne en 2016, le plan a défini **une feuille de route pour les investissements publics et privés dans les infrastructures 5G au sein de l'UE**. Certaines des principales mesures du plan sont les suivantes : la promotion **d'un déploiement précoce** dans les principales **zones urbaines** et **le long des principales voies de transport**, la **promotion d'essais multipartites** paneuropéens pour transformer cette innovation en solutions commerciales complètes, et l'union des principaux acteurs pour **travailler à la promotion de normes mondiales** ;
- Boîte à outils de l'UE pour la sécurité 5G : **La boîte à outils 2020 de l'UE pour la sécurité 5G est un ensemble de mesures prises pour renforcer les exigences de sécurité des réseaux mobile ; évaluer les risques posés par les fournisseurs et limiter toute dépendance à l'égard d'un seul fournisseur et stimuler les capacités 5G propres à l'UE ;**
- PPP d'infrastructure 5G est un **partenariat entre la Commission européenne et l'industrie européenne des TIC**. Le 5G-PPP vise **à fournir des solutions, des architectures, des technologies et des normes pour les infrastructures de communication**. Les principaux défis du 5G-PPP consistent à fournir une capacité de zone sans fil 1 000 fois supérieure à celle de 2010, à créer un Internet sûr, fiable, sans coupure et une indisponibilité de service perçue nulle et à faciliter les déploiements denses de communication sans fil pour connecter plus de 7 trillions d'appareils sans fil desservant plus de 7 milliards de personnes.

euratechnologies
EXCELLENCE & INNOVATION

Domaine #2 : Cloud-computing

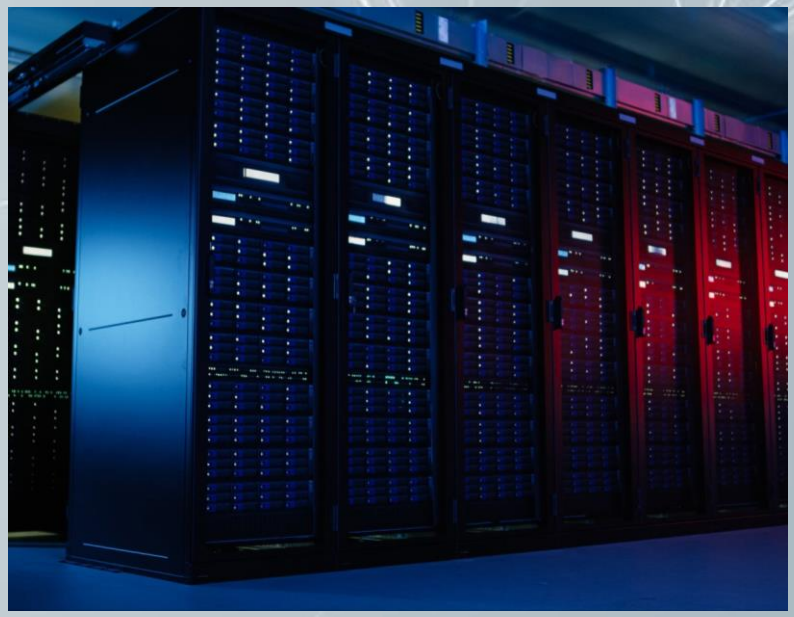
Cloud-computing

Définition	▪ Le cloud-computing **est la fourniture et l'hébergement de différents services via Internet, notamment le stockage de données, les serveurs, les bases de données, les réseaux et les logiciels. Le stockage en nuage permet d'enregistrer des fichiers dans une base de données distante et de les récupérer à la demande. Le cloud computing ne nécessite pas de gestion directe de la part de l'utilisateur ;** ▪ Le cloud computing est utilisée pour la sauvegarde de fichiers, l'hébergement de sites web, les courriels, mais peut également permettre par exemple « le jeu en nuage », où un processus (le jeu vidéo) s'exécute sur des serveurs distants et est diffusé directement sur les appareils d'un utilisateur.
Pourquoi ce domaine est-il essentiel ?	▪ Le cloud computing est stratégique car il est utilisé par la quasi-totalité de la population, pour un usage professionnel ou personnel. Les informations personnelles et professionnelles sont hébergées sur des services en nuage, et **donc la sécurité de ces solutions de cloud computing et l'intégrité de ces solutions et de leurs fournisseurs sont essentielles pour garantir la sécurité des citoyens, des États et des entreprises, ainsi que leur droit à la vie privée** ; ▪ En outre, diverses lois sur la collecte et le traitement des informations stockées sur des serveurs font que l'emplacement de ces serveurs revêt une importance stratégique ; ▪ **La forte influence qu'exercent les fournisseurs de services de cloud computing (IBM, Google, Amazon, Microsoft, Alibaba) en raison de la quantité massive d'informations qu'ils hébergent et de l'oligopole qu'ils forment constitue une menace pour la souveraineté numérique européenne. Cette influence empêche l'établissement d'un acteur européen de cette taille sur le marché des solutions de cloud computing, limite l'influence des tentatives européennes et nationales de réglementer les activités de ces entreprises et suscite des inquiétudes quant à la confidentialité des données.**

Cloud-computing

Les Problématiques existantes liées à la souveraineté numérique européenne dans ce domaine

- Certains considèrent le secteur du cloud computing comme un oligopole, **où 5 entreprises contrôlent environ 80 % du marché (Alibaba, Google, IBM, Microsoft, AWS). C**e marché **présente des barrières à l'entrée élevées**, en raison de la saturation du marché et des coûts importants associés au développement d'une solution de cloud computing. Le nombre restrient d'acteurs dans le domaine du cloud computing réduit les points de défaillance. **Si un fournisseur tombe en panne, de nombreuses entreprises voient leurs activités perturbées, comme ce fut le cas pour Google en juin 2019, puis en août et décembre 2020** ;
- La loi chinoise sur le renseignement national exige que toutes les entreprises et individus basés en Chine (y compris tout fournisseur de Cloud opérant en Chine, quelque soit son pays d'origine) coopèrent avec les missions de renseignement d'importance nationale chinoise. La loi nationale chinoise sur le renseignement n'a pas d'application extraterritoriale, **ce qui signifie que les données stockées par des fournisseurs chinois en dehors de la Chine ne sont pas concernées** ;
- **Le Cloud Act, une législation américaine, permet au gouvernement américain d'avoir accès aux données stockées sur des serveurs situés aux États-Unis ou qui sont stockées par des fournisseurs américains de services de cloud computing, quelle que soit la localisation d'un serveur. La portée extraterritoriale du Cloud Act en fait une menace claire pour la souveraineté numérique européenne.** On estime actuellement que **92 % des données du monde occidental sont stockées sur des serveurs situés aux États-Unis**, qu'il s'agisse **d'informations personnelles d'utilisateurs, d'informations d'entreprises européennes ou d'institutions gouvernementales européennes.**



Cloud-computing

Initiatives européennes

- Le gouvernement français, par son soutien financier aux initiatives CloudWatt et Numergy en 2012, a tenté de développer des acteurs nationaux, alternatives à des acteurs comme IBM, AWS ou Azure, mais sans succès. Le gouvernement français continue de soutenir le développement de solutions de cloud computing françaises et européennes via sa stratégie nationale sur la technologie du cloud computing, centrée sur les cloud computing qualifiées de "dignes de confiance", en plaçant le cloud computing "au centre" des administrations françaises, et via des investissements publics, européens et privés pour accompagner de ldéveloppement de l'activité des acteurs français tels que OVHcloud, Scaleway, Outscale, ainsi que des PME et des start-up qui développent des solutions de cloud computing**. Au fil des années, OVH s'est imposé comme un acteur reconnu du cloud computing, et l'entreprise n'hésite pas à se présenter comme une alternative aux offres non européennes et comme un défenseur de la souveraineté des données ;**
- Le projet Gaia-X**, qui regroupe des acteurs privés français et allemands**, a pour ambition **de créer un écosystème fiable et sécurisé autour des offreurs de cloud computing européens.** Le projet rassemble des entreprises, des institutions de recherche, des associations, des administrations et des politiciens pour travailler ensemble à l'établissement d'une "infrastructure de données fédérée et sécurisée" ;
- L'important projet d'intérêt européen commun pour l'Infrastructure de cloud computing'informatique en nuage de nouvelle génération (IPCEI-CIS) est une initiative lancée en 2021, impliquant environ 80 projets et 180 entreprises de douze États membres de l'UE. L'objectif du projet est d'établir une infrastructure de cloud computing européenne, d'aider l'UE à devenir le leader technologique sur ce marché et de mettre en place une infrastructure numérique ouverte et évolutive permettant aux utilisateurs industriels de partager des données afin qu'ils puissent exploiter tout le potentiel de la numérisation. Chaque État membre finance le projet de son pays et les entreprises qui participent aux IPCEI.

euratechnologies
EXCELLENCE & INNOVATION

Domaine #3 : Cybersécurité

Cybersécurité

Définition

- La cybersécurité n'est pas une technologie, mais **un domaine qui fait appel à des solutions technologiques, à l'élaboration de politiques et à des pratiques humaines pour faire du cyberespace un environnement plus sûr et protéger les utilisateurs des cybermenaces** ;
- Le cyberespace est composé d'infrastructures (infrastructures câblées ou sans fil supportant le réseau, connecteurs physiques tels que fils, câbles, routeurs, serveurs, ordinateurs et objets), de protocoles et d'applications (qui permettent à l'information de circuler d'un utilisateur à l'autre), et de la couche "sociale" avec laquelle les utilisateurs interagissent (éléments disponibles sur le Web) ;
- **Pour les acteurs étatiques, la cybersécurité est à la fois offensive et défensive, et c'est un domaine qui implique la sécurité des données et des systèmes du secteur public, mais aussi la sécurité de toute entreprise ou service jugé "critique" pour le fonctionnement de l'État.**

Pourquoi ce domaine est-il essentiel ?

- Il existe différents types de cybermenaces : On parle d'attaque **DDoS (distributed denial-of-service)** lorsque les attaquants visent à rendre une machine ou une ressource réseau indisponible pour l'utilisateur en perturbant les services de l'hôte connecté à un réseau. Pour ce faire, ils inondent généralement la cible de demandes visant à surcharger le système. Les assaillants utilisent des réseaux de zombies, c'est-à-dire un réseau d'appareils infectés par un logiciel malveillant, pour les contrôler à distance afin de lancer une attaque DDoS. On parle **d'attaque par ransomware** lorsque **les pirates volent et cryptent les informations des utilisateurs et exigent une rançon pour permettre aux utilisateurs de récupérer les informations,** leur accès à ces informations ou pour ne pas publier ces informations. **Un ver informatique est un type de programme informatique malveillant qui se reproduit de lui-même pour se propager à d'autres ordinateurs, souvent en recherchant d'autres ordinateurs sur le même réseau que son hôte. Les vers peuvent être codés pour supprimer des fichiers sur un système hôte, les crypter ou exfiltrer des données**. Les attaques par hameçonnage constituent une autre cybermenace considérée comme moins sophistiquée que les exemples précédents. Les cybercriminels utilisent l'ingénierie sociale pour amener les utilisateurs à leur remettre des données ou des ressources, ou utilisent le phishing pour installer des logiciels malveillants sur les appareils des utilisateurs en les incitant à cliquer sur un lien ou à télécharger une pièce jointe. Ces attaques sont généralement menées par courrier électronique ou par SMS ;
- **Les cybermenaces représentent un danger pour les individus car elles volent leurs informations personnelles ou les dépouillent**. Elles constituent un danger pour tous types d'entreprises, car elles dérobent leurs informations confidentielles ou perturbent leur chaîne d'approvisionnement. Une attaque contre des petites et moyennes entreprises peut entraîner l'arrêt complet de leur activité et concourir à ternir leur réputation et à la perte de confiance de leurs clients ;
- **Les cybermenaces visent également les acteurs étatiques en s'attaquant aux institutions gouvernementales pour voler des informations ou interrompre leurs activités**. Elles peuvent également viser les infrastructures critiques essentielles au fonctionnement de la société ou d'un pays, comme les réseaux électriques, les systèmes de gestion du trafic, les services financiers, etc.

Les problématiques existantes liées à la souveraineté numérique européenne dans ce domaine

- La **cyberattaque NotPetya de 2017, qui a largement ciblé l'Ukraine (**80 % de tous les appareils infectés étaient situés en Ukraine), illustre comment le **cyberespace est utilisé par des états pour mener des opérations militaires.** Le logiciel malveillant a chiffré de manière irréversible des enregistrements, il n'y avait pas de clés de déchiffrement, bloquant l'accès des utilisateurs à leur machine. L'attaque emble être la plus vaste cyberattaque perpétrée par un État, le GRU russe ayant été désigné comme responsable de l'attaque. Plusieurs ministères, banques, dont la Banque nationale d'Ukraine, réseaux de métro et les systèmes de surveillance des radiations de la centrale nucléaire de Tchernobyl ont été touchés. **Une évaluation de la Maison Blanche chiffre les dommages causés par le logiciel malveillant NotPetya à plus de 10 milliards de dollars**. Maersk, l'entreprise responsable d'environ un cinquième du transport maritime mondial, touchée par cette attaque, **a mis 10 jours pour reconstruire ses réseaux et lui a coûté près de 300 millions de dollars**. Ces exemples démontrent bien à quel point les cyberattaques ont un impact important, organisationnel et financier ;
- **En 2021, il a été révélé que des traces du logiciel espion Pegasus, un logiciel espion qui cible les smartphones, développé par la société israélienne de cyberarmement NSO Group, ont été trouvées sur les téléphones de cinq ministres français.** Le projet Pegasus, enquête sur l'utilisation de ce logiciel espion, a révélé que **les clients de NSO l'avaient également utilisé pour cibler des militants des droits de l'homme, des journalistes et des avocats.** En janvier 2022, il a été révélé **que les téléphones de diplomates finlandais avaient été infectés par ce logiciel malveillant.**

Cybersécurité

Initiatives européennes

- Le centre de compétence européen en matière de cybersécurité : Situé à Bucarest, le **Centre de compétences en cybersécurité vise à améliorer les capacités et la compétitivité de l'Europe en matière de cybersécurité** en coordonnant la recherche et les investissements dans ce domaine. Pour ce faire, il travaille avec un réseau de centres de coordination nationaux ;
- Exercices cybernétiques de l'OTAN : Organisés chaque année en Estonie, ces exercices visent à améliorer les capacités cybernétiques des CERT nationales et la coordination entre celles-ci, c'est l'occasion pour ces équipes de s'entraîner et de renforcer l'enseignement de la cyberdéfense. Tallin est le siège du **centre d'excellence de la cyberdéfense coopérative de l'OTAN** ;
- CERT-UE : **Équipe d'intervention en cas d'urgence informatique dédiée à l'UE**, le CERT-EU **assure la cybersécurité des organes, agences et institutions de l'UE** et est composé d'experts en sécurité informatique des principales institutions de l'UE. Ce CERT fonctionne en coordination avec d'autres CERT dans les États membres pour répondre aux cybermenaces et aux cyber incidents ;
- PESCO : La **coopération structurée permanente** est **l'institution de l'UE qui assure la coopération entre les États membres dans le domaine de la défense**. Elle ne s'occupe pas exclusivement des cybermenaces mais travaille à la coordination des politiques et accueille des projets qui tournent autour de la défense du cyberespace européen ;
- Les équipes de réaction rapide aux cybermenaces : Elles permettent aux États membres de cette initiative de s'entraider pour améliorer leur cyber-résilience et de répondre collectivement aux cyber-incidents. Les CRRT travaillent ensemble pour développer des boîtes à outils déployables conçues pour détecter, reconnaître et atténuer les cybermenaces ;

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Cybersécurité

Initiatives européennes

- Directive sur la sécurité des réseaux et de l'information (NIS) : adoptée en 2016, il s'agit du premier texte législatif à l'échelle de l'UE qui traite de la cybersécurité. Comme il s'agit d'une directive, les États membres adoptent une législation nationale qui la suit ou la transpose, ce qui laisse une certaine flexibilité à chaque État de l'UE. La NIS comporte trois parties :
  (1) les États membres doivent disposer d'une certaine capacité nationale en matière de cybersécurité,
  (2) la collaboration transfrontalière entre les États de l'UE est encouragée,
  (3) les pays doivent superviser la cybersécurité des opérateurs de marché critiques sur leur territoire ;
- NIS2 : Proposée fin 2020, cette directive vise à remédier aux lacunes de la directive NIS en élargissant son champ d'application pour classer les secteurs en fonction de leur importance pour l'économie des États et de la société en introduisant un plafond de taille clair. **Elle vise à renforcer les exigences de sécurité pour les entreprises en imposant une approche de gestion des risques et en fournissant des éléments de sécurité de base qui doivent être appliqués.** Cette directive vise également à fournir des dispositions plus spécifiques sur le processus de notification des incidents et à aborder la sécurité de la chaîne d'approvisionnement et des relations avec les fournisseurs en exigeant des entreprises qu'elles abordent les risques de cybersécurité dans ces domaines ;
- Loi sur la cybersécurité de l'UE : Adoptée en 2019, la loi sur la cybersécurité de l'UE mandate l'ENISA en tant qu'agence de régulation permanente et lui attribue plus de ressources. L'ENISA a pour mission d'accroître la coopération au niveau européen, d'aider les États membres dans la gestion de leurs incidents de cybersécurité et de soutenir la coordination de l'UE en cas de cyberattaque ou de crise à grande échelle et transfrontalière. **Elle encadre également la certification de produits, services et processus TIC cybersécurité à l'échelle de l'UE** ;
- ENISA (Agence de l'Union européenne pour la cybersécurité) : **Créée en 2004, il s'agit d'une agence de l'UE qui se consacre à la réalisation d'un niveau élevé de cybersécurité en Europe**. Elle contribue à la cyberpolitique de l'UE, renforce la fiabilité des produits, services et processus TIC grâce à des systèmes de certification de la cybersécurité, et coopère avec les États et les institutions de l'UE sur les questions de cybersécurité.

euratechnologies
EXCELLENCE & INNOVATION

Domaine #4 : Intelligence Artificielle

Intelligence Artificielle

Définition	▪ L'intelligence artificielle désigne les **systèmes capables d'effectuer des tâches qui requièrent généralement l'intelligence humaine ;** ▪ L'IA repose sur trois piliers : **l'algorithmique**, basée sur les mathématiques, la programmation informatique et les neurosciences ; les **données**, qui sont nécessaires pour créer et entraîner les algorithmes et qui sont exploitées par l'IA pour extraire des informations et créer de la valeur sur la base de l'analyse des données par l'IA ; et **la puissance de calcul**, nécessaire pour exécuter les algorithmes, sur une quantité toujours croissante de données, en temps voulu.
Pourquoi ce domaine est-il essentiel ?	▪ L'intelligence artificielle, de plus en plus utilisée dans différents secteurs, est conçue pour aider les humains à prendre des décisions, pour optimiser les activités commerciales et pour automatiser certaines activités ; ▪ La capacité de l'IA à traiter, analyser et apprendre à partir des données disponibles est de loin supérieure à celle de l'humain. **Pourtant, elle peut encore être conçue avec certains défauts (biais, mauvais jeux de données) qui altèrent les résultats ou à des fins nuisibles pour l'être humain et peut constituer une menace pour la souveraineté numérique. Il est donc nécessaire d'établir des règles, notamment éthiques, afin de s'assurer qu'il n'y aucune dérive dans sa conception et ses usages (recrutement, santé, justice, bancaire ou militaire) ;** ▪ L'IA intervient dans de nombreuses activités stratégiques : la gestion de l'énergie, l'amélioration des processus de la supply chain industrielle, l'amélioration des soins de santé, en apprenant à personnaliser finement de chaque patient, dans l'analyse d'images satellitaires ou d'images de vidéosurveillance, ou encore dans le suivi des activités agricoles. ▪ **À l'heure où l'IA se diffuse dans de nombreuses technologies et secteurs d'activités, il est cruciale que l'Europe tire partie de ses savoir-faire d'excellence dans ce domaine, pour se positionner parmi les leaders et ne pas laisser les Big Tech s'emparer des précieuses données, matière indispensable à la construction des IA et par la même, de la valeur ajoutée qu'il en résulte.**

Intelligence Artificielle

Les problématiques existantes liées à la souveraineté numérique européenne dans ce domaine

- En matière d'IA, **certains estiment que l'Europe est incapable de rivaliser avec les deux leaders que sont la Chine et les États-Unis,** et qu'elle ne sert que **de champ de bataille pour ces 2 superpuissances et leurs entreprises technologiques et leurs IA. L'Europe pourrait ainsi devenir dépendante de leurs technologies, sans aucun contrôle sur son développement ;**
- Bien que l'Europe ait mené de nombreuses actions dans le cadre réglementaire de l'IA, il a été souligné que « les matchs n'étaient pas gagnés par les arbitres», mettant en avant que la réglementation seule ne permettrait pas à l'Europe d'affirmer sa souveraineté numérique dans ce domaine, mais qu'il était également indispensable de soutenir la recherche et l'innovation, les entreprises européennes (Start-up, PME-ETI) créatrices ou utilisatrices de solutions d'IA pour s'assurer de sa maitrise pour en tirer tous les bénéfices ;
- Les données sont l'une des ressources les plus importantes pour le développement de la technologie faisant usage de l'IA. Les données sont parfois connues sous le nom de « pétrole du 21ième siècle, **car dans le monde de l'intelligence artificielle, les données sont une ressource économique** qui doit être protégée, valorisée et exploitée de manière réglementée ;
- Le manque d'accès à de grandes bases de données freine le développement de l'IA en Europe. Les données publiques pourraient permettre aux start-ups ou aux entreprises du secteur numérique de développer de meilleures solutions pour le bien public (dans le secteur de la santé ou pour lutter contre le réchauffement climatique par exemple). Les acteurs européens ont intérêt à ce que la libre circulation de certains types de données soit fixée dans un cadre réglementaire lui-même défini par l'UE. Par exemple, l'UE pourrait élaborer une réglementation concernant le partage des données non-personnelles sur le sujet de l'environnement, comme elle l'a fait avec le RGPD concernant les données personnelles, et catégoriser les données en fonction de leur sensibilité ;
- **Les révélations du scandale Cambridge Analytica ont démontré les dangers que l'IA pouvait présenter pour la démocratie, en révélant comment des acteurs malveillants pouvaient utiliser l'IA pour influencer le résultat d'élections démocratiques :** l'entreprise a collecté des données d'utilisateurs de Facebook et les a utilisées pour cibler des individus avec des messages politiques personnalisés dans le but de manipuler leurs décisions de vote ;
- L'algorithme de recommandation de vidéos utilisé par YouTube a été critiqué par l'un de ses développeurs dans le podcast "Rabbit Hole" du New York Time : il a été conçu pour retenir l'utilisateur coûte que coûte sur la plateforme afin de générer des revenues publicitaires sans vraiment tenir compte des vidéos déjà visionner, représentant ses goûts et envie. **Certains acteurs et organisations ont compris le pouvoir de ce biais de l'algorithme et l'ont utilisé à leur avantage pour diffuser leurs idées politiques.** La plateforme et son algorithme ont été critiqués par un nombre important de personnes comme jouant un rôle considérable dans la radicalisation politique en ligne.

Cambridge Analytica

Intelligence Artificielle

Initiatives européennes

- **En 2021, la Commission européenne a défini un nouveau cadre réglementaire pour la conception et les usages de l'IA : il interdit toutes solutions dont la destination est la manipulation du comportement humain et la limitation de son libre arbitre; celles "à haut risque", l'utilisant comme élément de sécurité d'un produit ou d'un service, devront satisfaire à certaines exigences avant d'être commercialisées. Les entreprises qui ne respecteront pas ces exigences s'exposeront à une amende pouvant atteindre 30 millions d'euros ou 4 % de leur chiffre d'affaires mondial, le montant le plus élevé étant retenu** ;
- **Le cadre réglementaire européen pourrait renforcer la souveraineté européenne en garantissant la compatibilité des solutions d'IA avec les valeurs de l'UE. Ce cadre pourrait aussi, dans une certaine mesure, bénéficier aux start-ups européennes qui créent des solution d'IA respectant ces valeurs. Cependant, l'élaboration de normes internationales et objectives reste un défi. Une telle initiative nécessiterait d'engager les acteurs Big Tech à développer des normes communes et exigerait la création d'un organisme de réglementation ayant les compétences techniques pour évaluer les solutions d'IA ;**
- **La stratégie de l'UE en matière d'intelligence artificielle est construite pour garantir que cette dernière soit développée dans le respect des règles et des valeurs de l'UE**, pour favoriser la compétitivité en améliorant les compétences, en soutenant la recherche et le développement en favorisant les partenariats entre les États membres et le secteur privé ;
- **Le réexamen du plan coordonné de l'UE en matière d'IA de 2021 a mis en évidence la nécessité d'accélérer les investissements dans les technologies d'IA**, que les états membres mettent en œuvre des stratégies et des plans d'IA notamment pour aligner leur politique en matière d'IA afin de supprimer la fragmentation au niveau européen. Le plan fixe quatre objectifs principaux : créer en Europe les conditions propices au développement et à l'adoption de l'IA, faire de l'UE un lieu où l'excellence prospère du laboratoire au marché, veiller à ce que l'IA soit une force positive pour la société et les citoyens, et créer un leadership stratégique dans les secteurs à fort impact ;
- Le partenariat européen sur l'intelligence artificielle, les données et la robotique **est l'un des partenariats européens d'Horizon Europe. Il a pour objectif de faire profiter l'Europe des avantages de l'IA, des données et de la robotique en favorisant l'innovation, l'acceptation et l'adoption de ces technologies**. Le partenariat est composé de BDVA, CLAIRE, ELLIS, EurAI, euRobotics et Adra, et la Commission européenne a prévu d'y **investir 1,3 milliard d'euros**, un montant identique sera investi par les industriels d'ici 2030.

euratechnologies
EXCELLENCE & INNOVATION

Domaine #5 : Informatique quantique

Informatique quantique

Définition

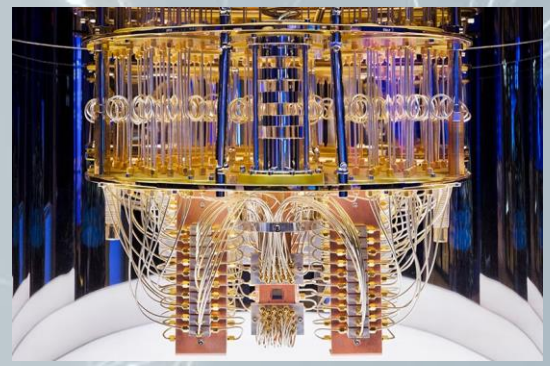
- Un ordinateur quantique est basé **sur les lois de la physique quantique**, en utilisant notamment la **superposition** et **l'intrication quantique** ;
  - **Superposition** : **un qubit ou un bit quantique** (atome, ion, molécule, électron, photon) **peut avoir simultanément la valeur 1 et 0**, alors que dans un ordinateur ordinaire, qui utilise le binaire, un bit (transistor) ne peut avoir que la valeur 1 ou 0, mais pas les deux ;
  - **L'intrication quantique** : **les qubits ont la capacité d'interagir les uns avec les autres**, leur état physique peut s'enchevêtrer, si bien qu'on ne peut pas les décrire comme étant indépendants - ils sont enchevêtrés. **Cet enchevêtrement est utilisé comme un multiplicateur de calcul pour les qubits, plus il y a de qubits enchevêtrés, plus un système est capable de faire des calculs** ;
- C'est ce qui permet, en théorie, à un ordinateur quantique d'être capable de trouver la totalité des résultats possibles d'un problème en utilisant un seul cycle d'opération. Un ordinateur binaire traite les informations de manière séquentielle, en trouvant le résultat des problèmes les uns après les autres. **Cela rend les ordinateurs quantiques plus efficaces, car ils peuvent traiter plus de données qu'un ordinateur binaire, traiter ces données plus rapidement, tout en utilisant moins de puissance de calcul**.

Pourquoi ce domaine est-il essentiel ?

- Cette technologie serait particulièrement **utile pour améliorer l'efficacité** tout le long de la **chaîne d'approvisionnement**, pour traiter la quantité toujours croissante de données afin d'aider les entreprises et les organisations à rationaliser leurs opérations. L'informatique quantique pourrait être utilisée pour **améliorer la circulation et l'efficacité des transports publics**, **la production agricole et la production de biens**, ainsi que le fonctionnement du secteur de la santé ;
- **D'un point de vue économique et stratégique, il y a donc un intérêt à développer cette technologie avant tout le monde. Elle permettrait à l'Europe et aux acteurs européens, grâce aux bénéfices attendus des usages de l'informatique quantique, d'accroître significativement leur compétitivité et leur position sur l'échiquier mondial.**

Informatique quantique

Les problématiques existantes liées à la souveraineté numérique européenne dans ce domaine

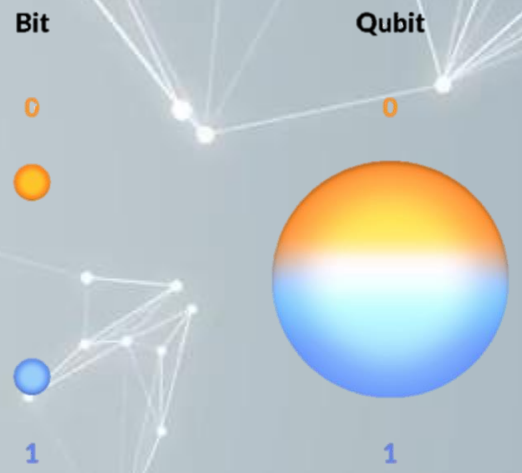


- Au cours des derniers mois, le développement de l'informatique quantique est devenue une "course" stratégique pour l'ensemble des états. **L'une des conséquences est qu'en mars 2021, l'UE a annoncé que le Royaume-Uni, Israël et la Suisse ne pourraient plus participer à son programme scientifique Horizon Europe dans des domaines qui pourraient s'avérer sensibles pour la sécurité nationale, dont l'informatique quantique**;
- L'informatique quantique pourrait être utile aux **opérations militaires,** pour preuve, les investissements réalisés par les acteurs militaires pour créer et gérer l'usage d'armes sur le champ de bataille dont run exemple serait d'assurer la coordination et le contrôle en temps réel de grandes flottes de drones;
- L'OTAN a également mis en évidence l'importante cybermenace que les ordinateurs quantiques pourraient représenter pour la société et l'armée, par sa capacité à décrypter les informations chiffrées, grâce à des algorithmes du type de l'algorithme de Shor ; **cette crainte explique en partie la course aux développements des technologies quantiques et leur mise sous couvert du secret .**

Informatique quantique

Initiatives européennes

- **Dans son discours sur l'état de l'Union de 2020, la présidente de la Commission européenne, Ursula von der Leyen, a promis un investissement de 8 milliards d'euros pour développer la prochaine génération de superordinateurs**, considérés comme nécessaire pour assurer la compétitivité de l'Europe dans les technologies du cloud, de l'IA et de la cybersécurité ;
- Le programme phare des technologies quantiques est une initiative qui a été lancée en 2018 et **qui vise à consolider et à étendre le leadership et l'excellence scientifiques européens dans les technologies quantiques**. Elle soutient le travail de centaines de chercheurs sur 10 ans, avec un budget d'un milliard d'euros de l'UE. L'initiative rassemble des institutions de recherche, des entreprises et des financeurs publics, avec l'objectif de favoriser le transfert des technologies quantiques européennes vers les marchés ;
- Annoncé en janvier 2021 par le gouvernement français, **le "Plan Quantique" est la stratégie française de développement des technologies quantiques, avec un investissement de 1,8 milliard d'euros sur une période de 5 ans. La France devient ainsi le troisième pays en terme de dépenses pour le développement de ces technologies, derrière les États-Unis et la Chine**. La moitié de cet investissement proviendra du Programme d'investissement d'Avenir, tandis que l'autre moitié proviendra des budgets de divers établissements de recherche œuvrant sur les technologies quantiques. Ce plan comporte un volet destiné à la formation de plus de 150 jeunes chercheurs par an.



euratechnologies
EXCELLENCE & INNOVATION

Domaine #6 : Blockchain

Blockchain

Définition	▪ **Une blockchain est une base de données décentralisée ou distribuée aussi connue sous technologies de registres distribués ;** ▪ Dans une base de données blockchain, il n'y a pas de serveur ou d'autorité centrale qui gère l'approbation, l'archivage ou la suppression des données, tous les ordinateurs qui utilisent cette base de données ont une copie de la base de données, ce qui en fait un systèmes peer-to-peer; toute modification de la base de données est validée par un processus, connu sous le nom de mécanisme de consensus ; ▪ **Ce type de base de données est inaltérable, car aucun bloc ne peut être supprimé et ne peut être approuvé unilatéralement . Toutes les transactions sur une blockchain sont cryptées.**
Pourquoi ce domaine est-il essentiel ?	▪ La blockchain a un impact direct sur la souveraineté des états en raison de sa nature même - pas d'autorité centrale, anonymat garanti, échappe aux législations nationales ou aux frontières – rendant sa réglementation et son contrôle complexes. En outre, la création de crypto-monnaies sans aucun contrôle étatique, constitue une atteinte à la souveraineté des états, battre monnaie étant une de leurs prérogatives ; ▪ **En même temps, la sécurité qu'offre la blockchain par son inaltérabilité et son cryptage, ainsi que le fait qu'elle soit décentralisée et permette l'anonymat en font une solution qui respecte la confidentialité des données et d'une certaine manière, redonne plus de contrôle à l'utilisateur sur l'usage fait de ses données ;** ▪ Si, de prime abord, la blockchain et le RGPD semblent incompatibles, la CNIL a proposé un guide de bonnes pratiques qui permet dans le cadre d'un projet blockchain de respecter cette réglementation; ▪ Les technologies de registres distribués sont considérées comme une innovation susceptible d'impacter fortement l'ensemble des secteurs d'activité, en servant d'enregistrement inaltérable des informations, par l'utilisation des contrats intelligents qui permettent de réduire le nombre d'intermédiaires dans les chaînes d'approvisionnement, améliorant ainsi l'efficacité opérationnelle et économique de bon nombre d'activités.

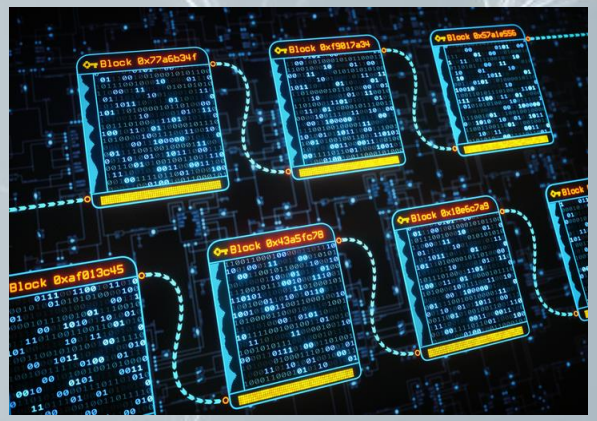
Les problématiques existantes liées à la souveraineté numérique européenne dans ce domaine

- **La Chine a interdit le minage et l'utilisation de crypto-monnaies sur son territoire en 2021 considérant les crypto-monnaies comme une atteinte à sa souveraineté nationale ;**
- Les tentatives de Facebook de créer une monnaie numérique stable appelée Lira, puis Diem, se sont heurtées à une large opposition des gouvernements. Le projet, bien que modifié de manière à ce que la crypto-monnaie soit rattachée à la valeur des monnaies fiduciaires nationales, le fait que ce soit Facebook qui en ait le contrôle, a été perçu comme une menace pour la souveraineté monétaire des États et a suscité la crainte que **Facebook n'accroisse son influence en devenant une banque fantôme** ;
- **Monnaies numériques officielles - La Chine a lancé un renminbi numérique en 2020, d'autres gouvernements et banques centrales, dont la BCE, envisagent d'émettre des monnaies numériques officielles**. L'intérêt suscité par les stablecoins, vient du fait qu'elles sont adossées à un actif de réserve, offrant une stabilité de valorisation, contrairement aux crypto-monnaies comme le Bitcoin ou l'Ethereum qui sont spéculatives et dont la valeur ne dépend que de l'offre et de la demande. Les Stablecoins offrent à la fois la sécurité et la confidentialité, ainsi que la rapidité de traitement des transactions que permettent les crypto-monnaies, sans la volatilité de celles-ci. Les états considèrent également que les monnaies numériques sont en train de prendre une place importante dans le concert international du commerce et de la finance. **Les banques européennes ont demandé à leur gouvernement respectif de veiller à ce que l'UE tienne sa place dans le développement des monnaies numériques et des jetons des secteurs privés et publics. Selon l'ancien conseiller à la sécurité nationale britannique Mark Lyall Grant, le renminbi numérique donnerait à la Chine la "capacité de contourner les systèmes bancaires traditionnels du monde, puis de contester la position prééminente du dollar", remettant en cause le système monétaire international .**

Blockchain

Initiatives européennes

- Fonds pour l'intelligence artificielle et la technologie blockchain : propose **des financements via six fonds différents aux start-up et aux PME** en phase de démarrage et de croissance dont les activités sont liées à l'intelligence artificielle ou à la technologie blockchain. **Le FEI dispose d'environ 700 millions d'euros** grâce à des accords conclus avec des fonds d'actions technologiques en Autriche, en Finlande, au Luxembourg, en Allemagne et aux Pays-Bas ;
- Observatoire et forum de l'UE sur la blockchain : Il s'agit d'une initiative sous le contrôle de la Commission européenne qui **accélère le développement des écosystèmes blockchain au sein de l'UE et contribue à faire de l'Europe un leader mondial**. Cet organisme suit les initiatives en matière de blockchain en Europe, sert de source de connaissances, fait office de forum pour le partage d'informations et d'opinions, et formule des recommandations à l'UE sur le rôle qu'elle pourrait jouer dans la blockchain ;
- **Dés 2012, l'Estonie a développé une plateforme basée sur les technologies des registres distribués,** appelée KSI Blockchain. Elle sert de registre officiel pour les entreprises, pour la propriété foncière ou les décisions de justice. Les Estoniens peuvent également l'utiliser pour voter et payer leurs impôts ;
- Infrastructure européenne de services blockchain : **conduit la stratégie blockchain de l'Europe**. L'UE entend utiliser les technologies des registres distribués pour la notarisation des actes, la certification des diplômes, l'identité numérique européenne et le partage des données. L'EBSI est la première infrastructure blockchain à l'échelle de l'UE, pilotée par le secteur public. Elle compte actuellement 25 nœuds actifs et 11 nœuds blockchain en phase d'installation. **4 millions d'euros ont été investis sur la période 2019-2020 dans cette infrastructure.**



euratechnologies
EXCELLENCE & INNOVATION

Domaine #7 : Semi-conducteurs

Semi-conducteurs

Définition

- **Les semi-conducteurs sont des matériaux dont le comportement physique se situent entre un conducteur et un isolant; ses propriété lui permettent de gérer et contrôler le flux de courant dans l'électronique et constitue la base de tous les composants ou puces électronique;**
- **Les puces électroniques se trouvent dans les smartphones, les appareils photo, les ordinateurs, mais aussi dans des produits tels que les machines à laver, les automobiles, les réfrigérateurs et les ampoules LED ;**
- Les matériaux tels que le silicium, le germanium, l'arséniure de gallium sont couramment utilisés dans la production de puces électroniques ;
- La miniaturisation des puces électronique est un enjeu sur le plan de la consommation électrique, du rapport taille / puissance de calcul / coût et de réduction des coûts de production. Les technologies pour les produire sont complexes et font appel à des procédés de gravure de 7 nanomètres, avec des perspectives de descendre à 2 ou 3 nanomètres.

Pourquoi ce domaine est-il essentiel ?

- **L'utilisation de plus en plus importante de puces électroniques dans l'ensemble des secteurs d'activité leur confère une position stratégique pour l'économie d'un état, et plus largement de l'UE ;**
- De part cette position stratégique , la maitrise technologique et opérationnelle de la production des puces électroniques constitue une composante essentielle pour atteindre la souveraineté technologique et numérique;
- L'industrie des semi-conducteurs est une industrie mondiale complexe, avec une très longue chaîne de valeur et un degré élevé d'interdépendance entre les acteurs. Toute perturbation de cette chaîne de valeur a un impact important et imprévisible ;
- **Avec la loi sur les puces électroniques récemment annoncée, l'UE a montré l'importance qu'elle accordait à cette technologie et son importance dans l'atteinte de la souveraineté numérique européenne.**

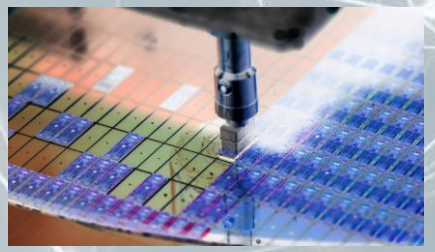
Semi-conducteurs

Les problématiques existantes liées à la souveraineté numérique européenne dans ce domaine

- **L'Europe représente actuellement moins de 10 % du marché des semi-conducteurs. Plus de la moitié des ventes de semi-conducteurs est destinée à la région Asie-Pacifique, la Chine représentant le plus grand marché de semi-conducteurs. Un plan réaliste pour le développement de la fabrication européenne de semi-conducteurs doit donc tenir compte du marché chinois. Cela signifie également que le marché européen dépend énormément de la production dans d'autres pays de cette technologie pour développer et produire des appareils électroniques ;**
- **L'augmentation de la part de marché de l'Europe dans la fabrication de semi-conducteurs nécessitera d'importants investissements publics ou privés, ainsi qu'un plan rationnel de retour sur investissement ;**
- **A la pénurie créée par la pandémie est venu s'ajouter des sanctions américaines à l'encontre de Semiconductor Manufacturing International Corporation (SMIC), le plus grand fabricant de puces chinois**; ces sanctions ont conduit **les entreprises américaines ou commerçant avec les Etats-Unis** à se tourner vers des fabricants tels que TSMC et Samsung, **déjà au maximum de leurs capacités de production**. Les **impondérables météorologiques**, inondations au Texas et sécheresse à Taïwan, n'ont fait qu'amplifier et augmenter les délais de fabrication et de livraison. L'Europe, dont les exportations de produits de haute technologie représentaient environ 20 % des exportations totales de l'UE en valeur, et connaissait un taux de croissance annuel de 10 % avant la pénurie, a connu un ralentissement conséquent de cette production alors que la demande continuait à croître, **entrainant une augmentation des prix**.

Semi-conducteurs

Initiatives européennes



- **La Commission européenne a déclaré qu'elle souhaitait doubler la part de marché de l'Europe dans le domaine des semi-conducteurs d'ici 2030**. Margrethe Vestager, responsable de la concurrence au sein de l'UE, a reconnu la nécessité d'augmenter la capacité de production en Europe, mais a mis en garde contre des attentes irréalistes quant à l'autosuffisance de l'Europe en matière de production de semi-conducteurs ;
- **Les technologies des semi-conducteurs sont l'un des sept domaines pour lesquels des plans coordonnés d'États membres sont encouragés dans le cadre du plan de relance NextGenerationEU**, adopté en décembre 2020 ;
- **L'Alliance sur les technologies des processeurs et des semi-conducteurs, lancée par la Commission européenne en juillet 2021, va identifier les lacunes dans la production de composants électroniques, les développements technologiques dont les entreprises et les organisations ont besoin, améliorer la coordinations entre les initiatives actuelles et futures de l'UE, pour répondre aux besoins technologiques et marché de l'UE.** L'alliance rassemble des acteurs de la conception et de la production de puces électroniques ;
- L'initiative européenne sur les technologies des processeurs et des semi-conducteurs est une déclaration commune signée par 22 États membres pour réduire la dépendance de l'UE à l'égard de l'Asie et dans une moindre mesure des Etats-Unis sur l'approvisionnement en processeurs et puces électroniques en augmentant les investissements sur l'ensemble de la chaîne de valeur des semi-conducteurs et en renforçant les capacités de production de l'Europe ;
- L'engagement commun Key Digital Technologies (KDT-JU), dont l'ancienne appellation était **Electronic Components and Systems for European Leadership (ECSEL)**, est un partenariat public-privé pour améliorer les capacités de l'Europe en matière de semi-conducteurs grâce à la recherche, le développement et l'innovation et par l'octroi de fonds à des projets apportant une expertise ou innovation dans ce domaine ;
- **La Commission européenne a présenté le EU Chips Act en février 2022**. Ce texte propose d'améliorer la capacité de recherche et d'innovation de l'Europe, d'à assurer le leadership européen en matière de conception et de fabrication, de fournir un soutien aux PME innovantes, d'adapter les règles relatives aux aides d'État pour permettre un soutien public aux installations de site de production en Europe et d'améliorer la capacité de l'Europe à anticiper et à répondre aux pénuries dans ce secteur. La Commission européenne a lancé un plan d'investissement pluriannuel pour l'industrie des semi-conducteurs, prévoyant d'allouer 11 milliards d'euros de fonds publics à la recherche, la conception et la fabrication de semi-conducteurs, ellet a déclaré que son objectif était de mobiliser un total de 43 milliards d'euros d'investissements publics et privés dans ce domaine jusqu'en 2030. Cette annonce est intervenue quelques jours après l'adoption par la Chambre des représentants des États-Unis d'un paquet législatif comprenant 52 milliards de dollars de subventions et d'aides pour stimuler la production américaine de semi-conducteurs.

euratechnologies
EXCELLENCE & INNOVATION

Domaine #8 : SpaceTech

SpaceTech

Définition	▪ **Ce domaine concerne les technologies utilisées pour voyager ou pour des activités menées dans l'espace. Elle concerne notamment l'industrie satellitaire, qui fournit des infrastructures civiles et militaires (satellites, lanceurs et bases terrestres) pour la fourniture des services de communication, des services voyages spatiaux, de GPS, d'observation du climat et des effets du changement climatique.**
Pourquoi ce domaine est-il essentiel ?	▪ Les **satellites** sont utilisés pour les **communications**, pour les **missions de défense** (surveillance des mouvements des forces armées, détection des lancements de missiles, armement spatial) et de **collecte de renseignements**, pour **soutenir les infrastructures ou les activités critiques** et pour mener des **recherches** ; ▪ Les **voyages spatiaux commerciaux ou touristiques se développent** grâce aux avancées technologiques et de la recherche des lanceurs : développement de lanceurs réutilisable, augmentation de la charge, baisse des coûts de lancement,..; ▪ **L'espace est à nouveau considéré comme une sphère de la politique internationale, mais aussi comme un domaine offrant de nombreuses opportunités économiques.** Les États-Unis et la France ont créé des forces armées dédiées à l'espace, l'OTAN est en train de créer un centre spatial, le Royaume-Uni a développé un commandement spatial, la Chine a posé des astromobiles ou rovers sur la Lune, des acteurs privés ont lancé des centaines de satellites pour fournir des services Internet ou ont envoyé des personnes dans l'espace ; ▪ **L'espace est stratégique pour l'UE dans les domaines de la sécurité maritime, des services d'urgence, de la gestion des frontières, des télécommunications, de la surveillance de l'environnement et de la terre, de l'agriculture durable et de la sécurité des transports**; ▪ **Les recherches et technologies développées par le secteur spatial ou celles développées dans l'espace contribuent au développement de technologies de pointe pour l'amélioration des conditions de vie sur Terre**. L'imagerie satellitaire par exemple, est utilisée pour aider les agriculteurs à optimiser l'arrosage, la fertilisation ou la récolte de leurs terres. Elle peut également être utilisée pour surveiller les niveaux d'eau des réservoirs et alerter en cas de pénurie, suivre la déforestation ou encore surveiller les zones de pêche pour arrêter la pêche illégale.

Les problématiques existantes liées à la souveraineté numérique européenne dans ce domaine

- La constante appropriation de l'espace par des entreprises privées est un sujet d'inquiétude pour les Etats et leurs populations. Si les acteurs du secteur privé y voient des opportunités commerciales dans le tourisme spatial, le déploiement de constellations de satellites ou l'extraction de matériaux de l'espace, **certains s'inquiètent de savoir qui est en droit de revendiquer la propriété de cet espace et de ces matériaux ;**
- **Le traité de l'espace de 1967 stipule que toutes les nations ont le droit d'utiliser et d'explorer la Lune et les autres corps célestes, mais interdit toute revendication de souveraineté sur ces derniers et exige des nations qu'elles surveillent les activités des entreprises spatiales privées ;**
- Des problèmes ont déjà été rencontrés avec les entreprises spatiales privées : la constellation de satellites en orbite basse Starlink de SpaceX, utilisée pour fournir des services Internet, a fait l'objet de plaintes de la part d'astronomes parce qu'elle perturbait l'observation des étoiles et l'espace. Les autorités chinoises ont demandé au gouvernement américain d'exercer une plus grande surveillance sur les entreprises privées après des collisions évitées de justesse impliquant ces satellites et la station spatiale chinoise.

Initiatives européennes

- L'UE a sélectionné un groupe de fabricants, opérateurs, fournisseurs de services et de lanceurs de satellites européens, ainsi qu'une société de télécommunications terrestres pour étudier la faisabilité d'un système européen de communications spatiales identique à OneWeb ou StarLink, afin de fournir des services de communications à hauts débits sécurisés aux régions rurales et aux zones dépourvues de services adéquats. Ce consortium est composé d'Airbus, Arianespace, Eutelsat, Hispasat, OHB, Orange, SES, Telespazio et Thales Alenia Space ;
- Le directeur général de l'Agence spatiale européenne, Josef Aschbacher, a déclaré **qu'il craignait que l'Europe ne prenne du retard avec la Chine et les Etats-Unis dans la course à l'espace, si elle n'investissait pas dans le développement de lanceurs de fusées réutilisables, de constellation de satellites de communication et même dans de missions vers la Lune et Mars. M. Aschbacher estime que l'industrie spatiale générera des revenus de plus de 800 milliards d'euros d'ici 2040 et que l'Europe doit agir maintenant si elle veut garder et développer sa place sur ce marché ;**
- L'Agence spatiale européenne (ESA) est l'un des leaders à l'avant-garde de la R&D le domaine spatial. L'ESA a contribué à la mission Webb, lancée en décembre 2021, en fournissant et en finançant plusieurs composants clés de l'instrument MIRI (Mid-InfraRed Instrument) du télescope spatial James Webb; il produit des images et des spectres dans l'infrarouge moyen qui permettront aux scientifiques de pénétrer les épaisses couches de poussière qui masquent les régions de naissance d'étoiles intenses. L'ESA a également fourni le spectrographe proche infrarouge qui équipe le télescope et qui étudiera les objets enfouis dans des nuages de gaz et de poussière pour mieux comprendre la formation et l'évolution des galaxies. Le télescope a également été lancé depuis la base spatiale européenne de Kourou en Guyane française par un lanceur Ariane 5 ;
- Le programme Copernicus est le programme d'observation de la Terre de l'UE. Il est utilisé pour surveiller la planète et son environnement; les services d'information fournis sont gratuits et librement accessibles aux utilisateurs. Il agrège des informations des données d'observation satellitaire de la Terre et des données provenant de systèmes de mesure terrestres, aériens et maritimes ;
- Depuis 2016, Galileo est le système mondial de navigation par satellite de l'Europe, composé de 26 satellites et d'une infrastructure terrestre de soutien. Il fournit des informations très précises sur la position et le temps, utilisées par les voitures autonomes et connectées, les chemins de fer, l'aviation et d'autres secteurs. **Aujourd'hui, environ 7 % de l'économie de l'UE dépend de la disponibilité des signaux de satellites de navigation. Des études démontrent que le système apportera environ 90 milliards d'euros à l'économie de l'UE au cours de ses 20 premières années de fonctionnement.**

EURATECHNOLOGIES

Plus d'informations sur notre organisation sur
https://www.euratechnologies.com/

euratechnologies.com