Euromad 2023- MODÉLISATION DU CONSEIL EUROPÉEN

Conseil des secrétaires d'État des ministres de la Défense et des Armées

"Comment l'UE peut-elle assurer un usage éthique du numérique ? "

Commissaires: Olivia KREISLER STERLING, Miguel ROJO KREISLER, Patricia SUAREZ CARRERA

SOMMAIRE

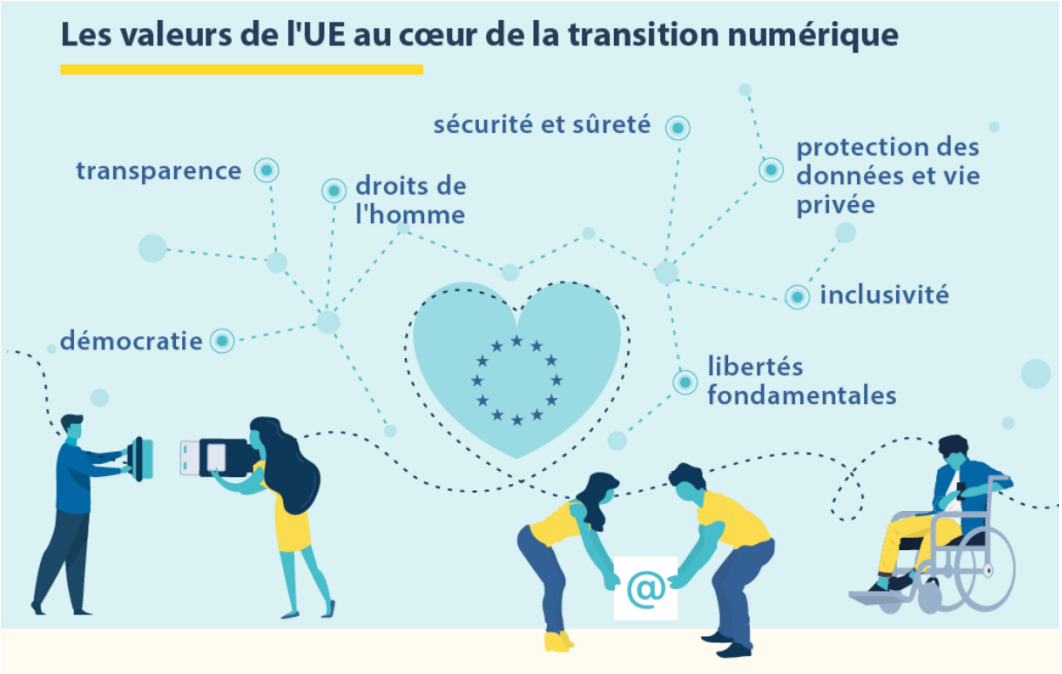
I. Introduction

II. Bilan Historique

III. Contextualisation politique

IV. Sitographie

I. Introduction



Nous vivons actuellement dans un monde où le numérique a une grande importance. Durant la pandémie du Covid-19, source d'isolement, époque de crise et d'incertitude, le numérique et ses utilités se sont présentés comme un véritable outil d'espoir. Néanmoins le numérique est aussi source d' attaques, de cyber menaces qui pèsent sur notre société et qui peuvent avoir des graves conséquences sur l'ensemble de nos citoyens. Par exemple, les hackers volent plus de 10 terabytes de données chaque mois dans l'UE pour après demander une rançon.

Actuellement on dénomme "numérique", des systèmes, dispositifs ou procédés employant ce mode de représentation digital.

Le secteur en question connaît un développement accéléré et touche de nombreux domaines tels que la santé, la banque, l'éducation ou l'industrie. C'est ainsi que le numérique est devenu un des principaux piliers de l'économie Européenne. Parmi les avancées qui occupent une place exceptionnelle se trouve l'intelligence artificielle, concept ambigu qui suscite crainte et espoir. La mise en place de l'Intelligence Artificielle peut modifier les conflits armés, en leur donnant une nouvelle façon de poser des problèmes. D' autre part, l'IA offre un énorme potentiel dans d' autres secteurs tels que le transport, la santé, l'énergie ou l'agriculture. Néanmoins, il faut prendre en compte les attaques qui mettent en danger la sécurité. Cette controverse entre les avantages et les risques est également caractéristique de la monnaie numérique.

Les technologies numériques sont donc à l'origine de conséquences positives au sein de l'Union Européenne. Entre celles-ci, nous pouvons citer l'accessibilité à un réseau de communication à l'échelle mondiale, la création des nouveaux emplois ou la création des nouveaux marchés. Cela entraîne une consolidation de la compétitivité au sein de l'Union Européenne.

Néanmoins, face à l'augmentation progressive de l'usage du numérique, nous devons parallèlement défendre les intérêts de nos citoyens en respectant un code éthique qui correspond avec les valeurs de l'Union Européenne.

C'est ainsi que nous sommes appelés à agir : nous devons assurer la sécurité et le bien-être de nos citoyens, nous devons répondre face aux menaces qui pèsent sur

L'union Européenne. La Commission européenne doit en définitive assurer un usage éthique du numérique en accord avec nos valeurs fondamentales.

II. Bilan Historique de la politique numérique de l'UE

"Depuis 2014, la Commission a mis en place des directives et des règlements afin de favoriser la circulation des informations tout en protégeant les données personnelles. Il faut faire face au difficile équilibre entre développement économique et sécurité."

1) Règlement sur la libre circulation des données à caractère non-personnel (14 novembre 2018)

Le Règlement sur la libre circulation des données à caractère non-personnel, c'est-à-dire les données électroniques qui ne contiennent aucune information qui puisse être utilisée afin d'identifier une personne, vise à établir un cadre applicable au libre flux de ces données dans l'UE.
En effet, les économies dépendent de plus en plus des données informatiques: celles-ci peuvent ajouter de la valeur à des services existants et créer des modèles d'entreprises innovateurs. C'est pourquoi, afin de profiter au maximum des effets bénéfiques des données, la Commission assure à travers ce règlement la libre circulation des données non personnelles et donc permet aux entreprises et administrations publiques de les garder et gérer librement. De plus, ce règlement assure la coopération entre les pays membres en leur permettant d'accéder aux données d'un autre pays.

2) Règlement de l'UE sur la cybersécurité (juin 2019, Octobre 2020)

Une croissante accessibilité aux cyber données, assurée par exemple par le règlement précédent, doit être accompagnée par une réglementation de plus en plus solide. En vue de ceci, la loi sur la cybersécurité renforce l'Agence de l'UE pour la cybersécurité (ENISA) et établit un cadre de certification de cybersécurité pour les produits et services.
L'ENISA fut créée en 2004 et travaille près des États membres et autres acteurs afin de conseiller sur les questions de cybersécurité. Elle supporte également le développement d'une réponse coopérative à large échelle pour la cybersécurité à travers les frontières, par exemple face aux cyberattaques de pays étrangers.

Selon la commission européenne, cette loi lui confère un mandat permanent et lui concède davantage de ressources et de nouvelles tâches. Par exemple, mettre en place des systèmes de certification en matière de cybersécurité.
En effet, la loi de l'UE sur la cybersécurité introduit en plus un cadre de certification de cybersécurité à l'échelle de l'UE pour les produits, services et processus TIC[1]. Les entreprises exerçant des activités dans l'UE n'auront à certifier leurs produits, processus et services TIC qu'une seule fois et à voir leurs certificats reconnus dans toute l'Union européenne.
D'un autre côté, en octobre 2020, après la pandémie de 2019 où l'exposition aux cybermenaces à été supérieure il y a eu une "réponse plus ferme" en matière de sécurité de la part de UE et accroître le bien-être des citoyens. Cette renforcé de la cybersécurité s'est basé sur trois points principaux :

1) La protection contre les menaces informatiques.
2) La mise en place d'un environnement sécurisé grâce au chiffrement quantique.
3) L'accès à des données à des fins judiciaires et répressives.

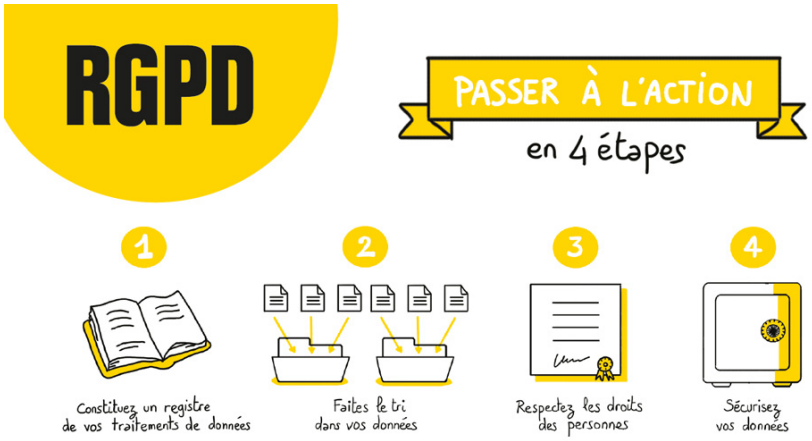
3) Directive de l'UE sur les données ouvertes (16 juillet 2019)

La directive sur les données ouvertes et la réutilisation des informations du secteur public, qui remplace la directive relative aux informations du secteur public (ISP), prévoit des règles communes pour un marché européen des données détenues par les pouvoirs publics. Les données ouvertes sont des données ouvertement accessibles, exploitables, éditables et partageables par n'importe qui et pour n'importe quel but, même commercial.
La directive met l'accent sur les aspects économiques de la réutilisation de l'information plutôt que sur l'accès des citoyens à l'information. Elle encourage les pays de l'UE à mettre à disposition le plus d'informations possibles en vue de leur réutilisation et traite des documents détenus par des organismes du secteur public dans les pays de l'UE, qui comprennent :

- Les documents détenus par les ministères, les organismes publics, les municipalités et les organisations financées principalement par des autorités publiques,
- Les contenus détenus par les musées, les bibliothèques et les archives
- Les textes écrits, les bases de données, les fichiers audio et les fragments de films

4) Règlement Général sur la Protection des Données (RGPD) (2016)

[1] Ensemble d'outils et de ressources technologiques permettant de transmettre, enregistrer, créer, partager ou échanger des informations



Ce règlement, adopté par le Parlement Européen le 26 avril 2016 et remplaçant la directive sur la protection des données personnelles 95/46/CE adoptée en 1995, renforce et unifie la protection des données pour les individus au sein de l'Union européenne.
Il a trois grands objectifs :

- Établir des règles pour protéger les personnes physiques à l'égard du traitement des données à caractère personnel et pour garantir la libre circulation de ces données.
- Protéger les droits fondamentaux et les libertés des personnes physiques, en particulier le droit à la protection des données privées.
- Assurer que la libre circulation des données à caractère personnel au sein de l'Union ne s'oppose pas à la protection des personnes physiques à l'égard de ses données privées.

Ces principes pourront être appliqués grâce à l'augmentation du pouvoir des autorités de contrôle.
À l'échelle mondiale, des auteurs voient le RGPD comme une perte de compétitivité pour les entreprises européennes. En effet, celles-ci devront beaucoup investir dans la protection des données personnelles, pendant qu'il n'existe aucun règlement similaire dans des pays comme les États-Unis.

5) <u>Plan coordonné avec les États membres dans le domaine de l'intelligence artificielle</u> (2018)

Le Plan coordonné dans le domaine de l'intelligence artificielle, proposé par la commission européenne, a pour but de :

- Promouvoir l'innovation et l'utilisation de l'IA

- Profiter au mieux des possibilités offertes par l'IA
- Combattre la concurrence internationale en matière d'IA, notamment face aux grands investissements des É.-U. et de la Chine
- Placer les citoyens au centre du développement de l'IA

Il repose sur 3 piliers :

- accroître les investissements publics et privés dans l'IA :

Les investissements publics et privés dans l'IA réalisés dans l'Union doivent être augmentés pour atteindre l'objectif de 20 milliards d'€ par an au cours de la prochaine décennie.

- se préparer aux changements socioéconomiques :

Selon la commission Européenne, le rythme auquel certains emplois disparaîtront et d'autres seront créés devrait vraisemblablement s'accélérer, tandis que les modèles économiques et la manière dont les tâches et les fonctions sont exécutées changeront. De plus, l'adoption de l'IA pourrait créer ou augmenter les disparités entre différents acteurs économiques (par exemple entre petites et grandes entreprises) de par un différend accès à cette technologie.

- garantir un cadre éthique et juridique approprié :

En effet, l'adoption et l'innovation en IA provoquera sûrement des problèmes éthiques, auxquels l'UE devra répondre de la meilleure manière possible.

6) Lignes directrices en matière d'éthique pour une IA digne de confiance (avril 2019)

Le 8 avril 2019, un groupe d'experts de haut niveau sur l'IA (à la demande de la Commission Européenne) a présenté les lignes directrices en matière d'éthique pour une IA digne de confiance. En accord avec ces lignes directrices, l'IA digne de confiance devrait être :

- licite : respectant toutes les lois et régulations
- éthique : respectant tous les principes et valeurs éthiques
- robuste : d'une perspective technique mais aussi en prenant en compte l'environnement social

Ces lignes directrices mettent en avant 7 règles qui doivent être remplies afin d'être un système d'IA digne de confiance :

- Agence et surveillance humaines : Les systèmes d'IA doivent donner du pouvoir aux êtres humains, en leur permettant de prendre des décisions éclairées et en favorisant leurs droits fondamentaux.

- Robustesse technique et sécurité : Les systèmes d'IA doivent être résilients et sûrs. Ils doivent être protégés et avoir un plan en cas de problème. De même, ils doivent être précis, fiables et aussi reproductibles.
- Privacité et gouvernance des données : Il doit y avoir un respect complet de la privacité et la protection des données, une gouvernance des données assurée par des mécanismes adéquats.
- Transparence : Les données, systèmes modèles commerciaux relevant de l'IA devraient être transparents. Des mécanismes de traçabilité peuvent aider à ce but.
- Diversité, non-discrimination et justice : Les systèmes d'IA devraient être accessibles à tous.
- Bien-être sociétal et environnemental : Les systèmes d'IA devraient bénéficier à tous les êtres humains, en incluant les générations futures. Ils doivent donc être durables et respectueux de l'environnement.
- Responsabilité : Des mécanismes devraient être mis en place afin d'assurer une responsabilité quant aux systèmes d'IA et leurs conséquences.

7) Le combat contre les cybermenaces

Les cyberattaques et la cybercriminalité causent des problèmes de plus en plus nombreux et revêtent des formes de plus en plus sophistiquées dans toute l'Europe.

L'UE a donc pour but de mettre en place une réponse plus ferme afin de promouvoir la cyber résilience, combattre la cybercriminalité et stimuler la cyberdiplomatie ainsi que la cyberdéfense. Nous allons nous intéresser aux réponses de l'UE face à ses défis dans les domaines de:

- la cyber-résilience
- la cybercriminalité
- la cyberdiplomatie
- la cyberdéfense

Le but étant de construire un internet mondial stable et sûr, éthique, dans lequel l'état de droit, les droits de l'homme et les valeurs démocratiques seront protégés.

- La cyber résilience:

La cyber résilience désigne la capacité d'un système d'information à résister aux cyberattaques et aux pannes accidentelles, puis à revenir à un état de fonctionnement et de sécurité satisfaisant.

En décembre 2020, la Commission européenne et le Service européen pour l'action extérieure (SEAE) ont présenté une nouvelle stratégie de cybersécurité de l'UE afin de renforcer la résilience de l'Europe face aux cybermenaces.

Selon celle-ci, les quatre cyber communautés - celles qui sont concernées par le marché intérieur, les services répressifs, la diplomatie et la défense - doivent travailler plus étroitement en vue d'une prise de conscience commune des menaces et doivent être prêts à réagir collectivement lorsqu'une attaque se matérialise. De plus, cette stratégie invite

les pays de l'UE à s'unir pour combiner leurs ressources et leur expertise afin d'apporter une réponse collective plus efficace aux cybermenaces.

- La cybercriminalité:

Un centre européen spécialisé dans la lutte contre la cybercriminalité, European Cybercrime Centre (EC3), a été créé en 2013 au sein d'Europol pour aider les pays de l'UE à enquêter sur la criminalité en ligne et à démanteler les réseaux criminels.

De plus, la lutte contre les cyberattaques est une des priorités de la plateforme pluridisciplinaire européenne contre les menaces criminelles (Empact). Afin de poursuivre les criminels, les autorités judiciaires s'appuient donc de plus en plus sur les preuves électroniques telles que des textes, des courriers électroniques ou des applications de messagerie.

Pour cela, l'UE travaille à l'élaboration de nouvelles règles qui faciliteront l'accès transfrontière aux preuves électroniques et négocie actuellement un accord avec les États-Unis, pays où sont établis la plupart des fournisseurs de services.

- La cyberdiplomatie:

En mai 2019, le Conseil a établi un cadre permettant à l'UE d'imposer des sanctions ciblées visant à décourager et contrer les cyberattaques qui constituent une menace extérieure pour l'UE ou ses États membres: la "boîte à outils cyber-diplomatique". Ces sanctions sont applicables aux personnes ou entités responsables directement ou indirectement de cyberattaques. Les mesures restrictives comprennent: l'interdiction de voyager vers l'UE à l'encontre des personnes, le gel des avoirs à l'encontre des personnes et entités. Les toutes premières sanctions à la suite de cyberattaques ont été imposées le 30 juillet 2020.

- La cyberdéfense:

Le cyberespace est considéré comme constituant le cinquième domaine de guerre, qui est aussi critique pour les opérations militaires que les domaines terrestre, maritime, aérien et spatial.

À l'heure actuelle, l'UE coopère en matière de défense dans le cyberespace à travers les activités de l'Agence européenne de défense (AED), en collaboration avec l'Agence de l'UE pour la cybersécurité et Europol.

L'AED aide les États membres à constituer une main-d'œuvre militaire qualifiée dans le domaine de la cyberdéfense et veille à ce que des technologies de cyberdéfense proactives et réactives soient disponibles. De plus, la stratégie de cybersécurité de l'UE adoptée en décembre 2020 par la Commission et le SEAE renforce la coordination et la coopération entre États membres de l'UE en matière de cyberdéfense. Finalement, la politique de l'UE en matière de cyberdéfense, adoptée en novembre 2022 par la Commission et le SEAE, a pour but d'accroître la coopération entre les cyber-communautés militaires et civiles.

III. Contextualisation générale

1) Classement 2020 des pays européens

L'indice relatif à l'économie et à la société numérique (DESI) de la Commission européenne mesure la performance des Etats membres ainsi que de l'UE dans son ensemble en matière de numérique. Cinq dimensions sont mises en évidence par ce classement :

a. l'état de la connectivité,

b. le capital humain,

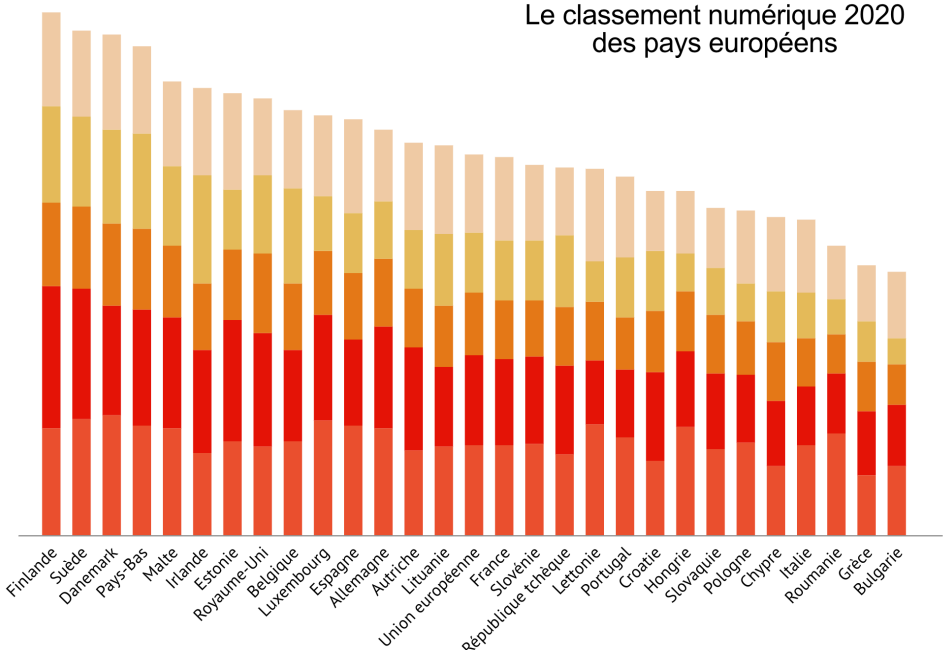
c. l'utilisation d'internet par les citoyens,

d. le degré de numérisation des entreprises

e. les services publics en ligne

On observe cependant que la sécurité numérique, une dimension indispensable pour la stabilité du secteur, n'est pas prise en compte dans ce classement, ce qui nous fait douter de la véracité de celui-ci, et de l'état réel du secteur numérique au sein de l'Union Européenne.

Note de 0 à 100 par domaine numérique au sein du rapport DESI (indice relatif à l'économie et à la société numérique) 2020

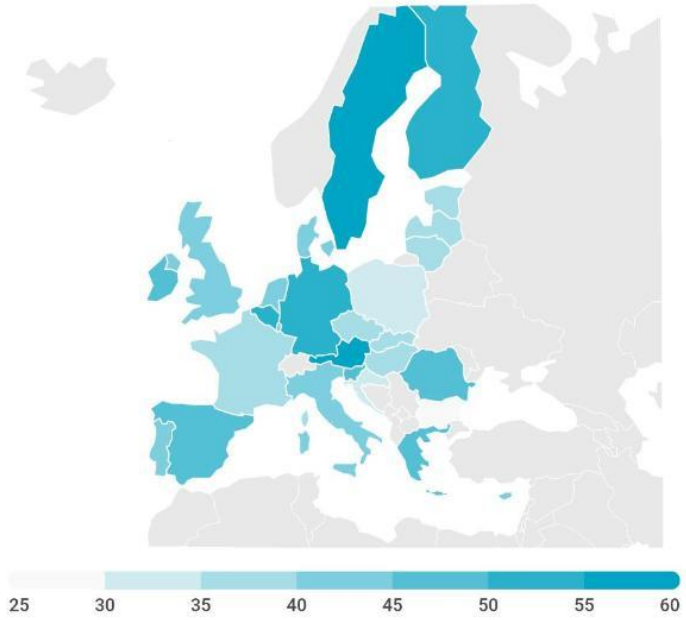


2) Rapport 2021-2022 sur le numérique en Europe

L'enquête annuelle du Groupe BEI sur l'investissement et le financement de l'investissement (EIBIS) est une étude à l'échelle de l'UE qui permet de recueillir des informations qualitatives et quantitatives sur les activités d'investissement des entreprises européennes sur leurs besoins de financement et sur les difficultés auxquelles elles sont confrontées.

- Pays les plus performants de l'UE

En 2021, la Finlande et Malte arrivaient en tête dans le domaine du numérique, suivies par le Danemark, l'Autriche, les Pays-Bas et la Suède.



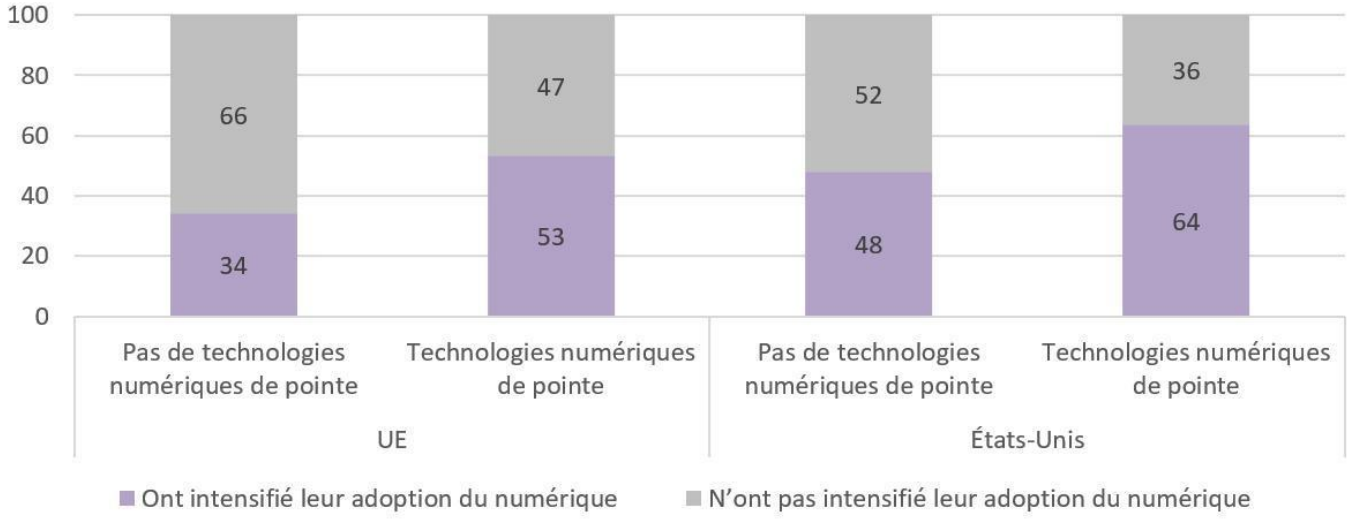
Entreprises ayant investi pour intensifier leur adoption du numérique en réponse à la crise due au COVID-19 (en %), par pays

Source : Enquête 2021 de la BEI sur l'investissement

- Creusement de l'écart entre les entreprises numériques et non numériques

La pandémie de coronavirus a d'une part stimulé la transition numérique à tous les niveaux, mais elle a également creusé, dans une certaine mesure, le fossé numérique entre les entreprises. Quelque 26 % des entreprises de l'UE n'ont pas investi dans cette transformation. Ces entreprises sont susceptibles de nécessiter un soutien public plus fort ou spécifique pour maintenir leur compétitivité et éviter de prendre du retard lors de la relance économique. D'un autre point de vue, 61 % des entreprises de l'UE ont déjà adopté des technologies numériques de pointe.

La taille de l'entreprise est un facteur clé pour expliquer le fossé numérique entre les entreprises. En effet, les grandes entreprises sont beaucoup plus susceptibles d'être du "bon côté" de ce fossé.



Entreprises utilisant des technologies numériques de pointe et ayant investi pour intensifier leur adoption du numérique en réponse à la crise due au COVID-19 (en %)

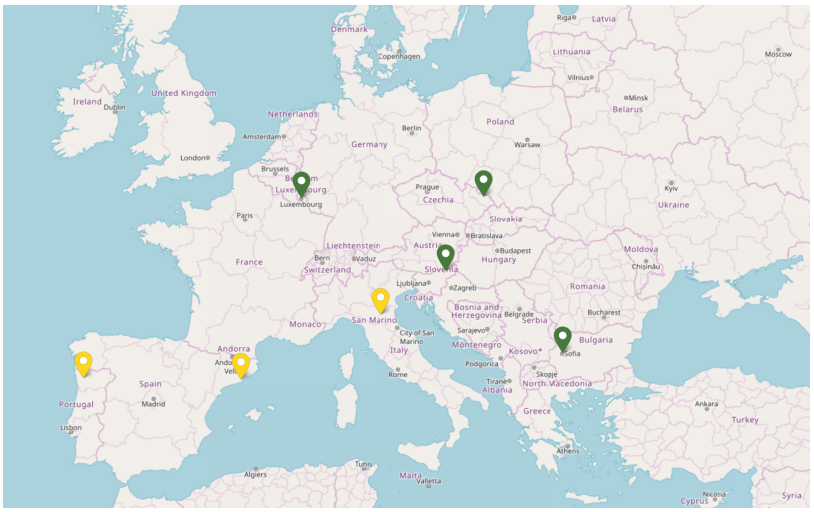
Source : Enquête 2021 de la BEI sur l'investissement

3) Innovations dans le secteur numérique

Il faut également prendre en compte les innovations dans le secteur numérique.

L'entreprise commune européenne de calcul à haute performance (Euro HPC JU) est une entité juridique et de financement, créée en 2018 et située au Luxembourg pour ouvrir la voie au supercalculateur européen. Celle-ci a sélectionné 8 sites dans l'Union européenne (UE) pour accueillir et exploiter les premiers ordinateurs quantiques EuroHPC : la Finlande, l'Italie, l' Espagne, la Slovénie, le Luxembourg, la République Tchèque, la Bulgarie et le Portugal .

Membres: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden and Turkey.



EuroHPC supercomputers under deployment

En somme, l'Union Européenne fait preuve d'une croissante adoption et innovation du numérique, qui, intégré dans le secteur public comme dans le privé, vise à améliorer et faciliter la vie de nos citoyens et stimuler l'économie.

Cependant, cette croissante adoption et même dépendance du numérique pose des menaces jusqu'alors inexistantes contre la sécurité des États, entreprises et citoyens de l' Union Européenne. Ces menaces, inexplicablement pas prises en compte dans certains rapports ou classements concernant ce secteur, sont de plus en plus graves.

Ainsi, le coût annuel de la cybercriminalité pour l'économie mondiale est estimé à 5 500 milliards d'euros à la fin de 2020 (doublant celui de 2015). De plus, selon un Eurobaromètre, 28 % des PME (Petites Moyennes Entreprises) européennes ont été victimes de cyberattaques en 2021.

Il est donc indispensable de mettre en place un système de protection contre ces cybermenaces pour assurer un usage éthique du numérique.

4) Cybersécurité: comment l'UE lutte contre les cybermenaces

a) Quelles sont les cybermenaces?

En effet, l'avènement du numérique a provoqué l'apparition de nouvelles menaces numériques contre l'UE. Elles ciblent non seulement des ordinateurs personnels, mais aussi des réseaux d'entreprises ou des organes gouvernementaux, et elles peuvent être menées par des pirates informatiques seuls, des groupes de pirates ou même des pays.

Celles-ci sont illustrées annuellement par le rapport du paysages des menaces de l' ENISA (ENISA threat landscape), qui analyse les principales cybermenaces et son évolution, et décrit des mesures de défense contre celles-ci.

Selon l' itération de 2022, les principales menaces identifiées sont:

- Attaques par *ransomware*:

Ce terme désigne les cyberattaques où un cybercriminel prend le contrôle d'un actif de la victime (généralement des institutions publiques, des compagnies privées et la presse), et demande une rançon pour rétablir sa disponibilité et/ou garantir sa privacité.

Ce type d'attaque est de plus en plus utilisé et effectif. Selon l'ENISA, entre mai 2021 et juin 2022, plus de 10 terabytes d'information ont été volés chaque mois . De plus, le rapport compte plus de 600 attaques durant l'année. Cependant, le nombre est probablement beaucoup plus important, vu qu' un grand nombre des organisations victimes décident de ne pas les reporter aux autorités.

- Malware

Un malware est un logiciel ou un micrologiciel destiné à exécuter un processus non autorisé qui aura un impact négatif sur la confidentialité, l'intégrité ou la disponibilité d'un système. C'est le cas par exemple des trojans, des vers informatiques ou des spywares.

Les deux formes de malware les plus présentes aujourd'hui sont le *crypto-jacking*, qui utilise un ordinateur pour miner des crypto-monnaies sans l'autorisation du propriétaire, et *IoT (Internet of Things) malware*, qui s'attaque aux dispositifs connectés à Internet (caméras, micros, assistants virtuels (Alexa, Siri…) ect.)

- L'Ingénierie sociale

Ce terme désigne les activités qui visent à profiter des comportements humains avec l'objectif de gagner l'accès à des services ou des informations.

La forme la plus commune d'ingénierie sociale est l' hameçonnage ou *phishing,* qui consiste à obtenir des renseignements personnels (souvent des données bancaires) des individus à travers des liens ou des messages frauduleux.

Selon le rapport de l'ENISA, la Chine a constamment ciblé les diplomates européens depuis août 2020. L' activité la plus récente impliquant des appâts rafraîchis pour coïncider avec l'invasion russe de l'Ukraine.

- Menaces contre les données

Les menaces contre les données forment l'ensemble des menaces qui visent les sources de données avec l'objectif d'en gagner accès non autorisé ou de les manipuler pour interférer avec le fonctionnement des systèmes.

La croissante valorisation des données fait de ces menaces des problèmes de plus en plus importants et fréquents.

En 2022, l'application COVID de Belgique a été attaquée, ce qui a entraîné que les données personnelles de 39 000 personnes soient exposées.

- Déni de service distribué (DDoS)

Ces attaques empêchent les utilisateurs d'un réseau ou d'un système d'accéder à des informations, des services ou d'autres ressources pertinentes en saturant et surchargeant l'objectif d'information.

En septembre 2022 eut lieu la plus grande attaque DDoS contre une compagnie européenne (anonyme) jusqu'alors . Elle fut partiellement mitigée grâce à un logiciel de protection développé par Akamai Technologies.

- Menaces contre l'Internet

Ce terme regroupe toutes les possibles menaces et attaques contre la disponibilité de l'Internet. Nous soulignons la prise en charge et destruction d'infrastructures Internet en détournant le trafic vers d'autres réseaux et la censure active des pages web ou réseaux d'information.

Ce type de menace a été très utilisé dans la guerre Russo-Ukrainienne pour influencer l'opinion publique, prévenir des fuites d'information et réaliser des activités de surveillance.

En 2022, les sites web italiens du Sénat, du ministère de la Défense et de l'Institut national de la santé ont été la cible d'une attaque DDoS lancée par des pirates russes dans l'intention de cibler les pays de l'OTAN.

- Désinformation/mésinformation

Comme son nom l'indique, cette menace consiste en créer ou partager information fausse ou trompeuse afin d'influencer l'opinion publique.

Celle-ci est probablement la menace la plus fréquente et une des plus dangereuses, puisqu'elle est facile de créer et permet d'influencer et manipuler l'opinion et les croyances publiques. Ceci, appliqué par exemple à des élections, constitue un véritable danger contre la démocratie.

- Attaques contre les chaînes d'approvisionnement (*supply chain attacks)*

Une attaque de la chaîne d'approvisionnement est un type de cyberattaque qui cible les organisations en se concentrant sur les maillons faibles de la chaîne d'approvisionnement de celle-ci. En ciblant un point faible de la chaîne d'approvisionnement, une cyberattaque peut avoir plus de chances de réussir.

→ Finalement, selon l'ENISA:

" Les attaques de cyber sécurité ont continué à augmenter au cours du second semestre 2021 et 2022, non seulement en termes de vecteurs et de nombre, mais aussi en termes d'impact.

La crise russo-ukrainienne a défini une nouvelle ère pour la cyberguerre et l'hacktivisme, son rôle et son impact sur les conflits.

En raison de l'instabilité de la situation internationale, nous nous attendons à observer davantage de cyber opérations motivées par la géopolitique dans un avenir proche ou à moyen terme. "

b) Cas d'espionnage numérique

Comme dans les entreprises, l'UE dispose également d'un CERT (Computer emergency response team), une équipe d'experts informatique prête à intervenir lorsqu'une attaque a été repérée. Selon cette agence la principale motivation des attaques serait le cyberespionnage et la méthode utilisée le *phishing*, afin de récupérer facilement des données sur des individus. Cependant, les principaux organes chargés de la promotion de la cybersécurité, à savoir l'Agence de l'Union européenne pour la cybersécurité (ENISA) et le CERT-UE, seraient en sous-effectif et ont besoin de financement. Parmi les attaques répertoriées en 2021, l'une d'elles – le piratage des services de messagerie de Microsoft – est officiellement attribuée à un groupe de hackers chinois. Des pays membres comme la Grèce ou Chypre ont également été victimes de cyber-espionnage depuis la Chine. De même, le réseau de satellites KA-SAT a subi une attaque et les pays membres ont accusé conjointement la Russie. Quels sont donc les enjeux auxquels les pays de l'UE doivent faire face dans le domaine du cyberespionnage ?

- <u>Le scandale Pegasus: un cas d' espionnage de certaines personnalités par des gouvernements</u>

Pegasus est un logiciel espion destiné à attaquer les smartphones commercialisé dès 2013 par l'entreprise israélienne NSO Group. Il accède aux fichiers, messages, photos et mots de passe, écoute les appels, et peut déclencher l'enregistrement audio, la caméra ou la géolocalisation. Pegasus est officiellement vendu uniquement à des organisations étatiques pour la surveillance des personnes soupçonnées de terrorisme ou autres crimes graves. Dans la pratique, il se révèle être aussi utilisé par des régimes démocratiques et des régimes autoritaires pour surveiller des journalistes, des opposants politiques et des militants des droits humains.

Le projet Pegasus est une enquête journalistique collaborative internationale. Le projet révèle en juillet 2021 que onze États ont espionné des journalistes, opposants politiques, militants des droits de l'homme, chefs d'État… au moyen du logiciel espion Pegasus édité par l'entreprise israélienne NSO Group.

Sophie In' t Veld, responsable du rapport

Le 8 novembre 2022 est présenté le premier rapport de la commission PEGA, chargée, suite aux révélations du Projet Pegasus, d'enquêter sur l'abus des logiciels espions, sur ses conclusions et l'eurodéputée Sophie In' t Veld a accusé la

Commission européenne de ne pas défendre la démocratie. Elle dénonce le fait que l'UE pointe du doigt les menaces quand elles viennent de l'extérieur mais reste silencieuse quand elles viennent de l'intérieur. L'enquête s'est principalement concentrée sur le rôle des autorités nationales, et le rapport présente plusieurs profils de pays examinant les spécificités du déploiement de la technologie. Figurent parmi les solutions proposées des définitions plus précises et harmonisées de la sécurité nationale, une application vigoureuse des lois sur l'exportation et une réglementation des logiciels espions conforme à la jurisprudence existante. Le rapport met également en évidence certains États membres dans lesquels la technologie des logiciels espions a été jugée particulièrement manifeste ou répandue, tels que la Pologne, l'Hongrie, l'Espagne, Chypre et la Grèce avec Predator, un autre logiciel espion.

Alors que l'on pourrait imaginer des cas d'utilisation légitimes de logiciels espions - comme le ciblage de fonctionnaires étrangers à des fins d'espionnage traditionnel, soigneusement contrôlé et supervisé, l'enquête sur des menaces d'attaques extrémistes violentes ou la poursuite des infractions pénales réelles - les activités détaillées dans le rapport du Parlement européen mettent en évidence une surveillance antidémocratique conçue pour réprimer l'expression et la concurrence politique. Le rapport se voit donc dans l'obligation de rappeler que la sécurité nationale n'est pas un domaine sans lois et les États ne peuvent donc pas atteindre aux droits humains pour la garantir. Bien sûr, l'espionnage est légitime pour contrer les menaces contre la sécurité de l'État. Il faut donc que les États membres se dotent d'une définition commune de la sécurité nationale ou, au moins, que chaque État membre rende public ce qu'est la sécurité nationale à ses yeux. Elle appelle les dirigeants européens à consacrer un Conseil européen dédié à ces questions de surveillance généralisée qui fragilise les démocraties en Europe.

Il est cependant extrêmement difficile de contrôler cette technologie, car les contrôles à l'exportation que les gouvernements appliquent aux biens matériels, ne s'appliquent pas de la même manière aux logiciels. C'est pourquoi un moratoire sur l'utilisation de logiciels espions a été mis en place et ne sera levé que sous le remplissage de certains critères et conditions: disposer d'un cadre légal pour un usage responsable des écoutes, se conformer à la jurisprudence de la Cour européenne des droits de l'homme et de la Commission de Venise, élucider les allégations d'espionnage, permettre à Europol d'investiguer sur les abus, annuler les licences d'exportation aux États qui ne répondent pas aux critères démocratiques requis.

- <u>Le cas d'Edward Snowden et PRISM</u>

Edward Snowden, un consultant informatique travaillant pour la CIA et la NSA américaine, révéla, en 2013, l'existance de plusieurs programmes de surveillances en masse américains et britanniques.

En effet, Snowden rend publiques, par l'intermédiaire des médias, des informations classées top-secrètes de la NSA concernant la captation des données de connexion des appels téléphoniques aux États-Unis, ainsi que les systèmes d'écoute sur Internet des programmes de surveillance *PRISM*, *XKeyscore,*

Boundless Informant et *Bullrun* du gouvernement américain, mais aussi les programmes de surveillance *Tempora*, *Muscular* et *Optic Nerve* du gouvernement britannique.

Ces programmes, contrôlés par la NSA, prévoient le ciblage de toute personne vivant hors des États-Unis, y compris les citoyens européens.

Parmi ces personnes, on retrouve des personnalités politiques comme Angela Merkel et les Chanceliers allemands prédécesseurs, dont, selon WikiLeaks, les communications furent mises sous écoute pendant des années.

Les réactions publiques et politiques furent énormes. Viviane Reding, commissaire européenne à la justice, affirmait : « On ne peut pas négocier sur un grand marché transatlantique s'il y a le moindre doute que nos partenaires ciblent des écoutes vers les bureaux des négociateurs européens ».

Tout ceci démontre l'importance et l'impact que le secteur numérique peut avoir dans les relations internationales, la politique, et la sécurité des démocraties, et pousse l'UE à développer dans les plus brefs délais un système fiable de sécurité numérique.

- Comment faire face au cyberespionnage

L'UE n'a pas de front européen uni quand il s'agit de surveillance numérique, comme le montrèrent les révélations faites par une enquête de presse associant plusieurs pays européens en mai 2021. En effet, le NSA aurait écouté des conversations privées et espionné des dirigeants européens, entre 2012 et 2014, à travers des câbles danois et aurait été aidée par les services de renseignements du pays. Dans le domaine du numérique, les frontières ne posent plus d'obstacles, les alliés n'existent plus, chaque pays se retrouve à espionner un autre directement ou bien indirectement. Le chacun pour soi prévaut et ce sera le cas tant que les pays ne seront pas d'accord pour partager pleinement leurs outils. D'ailleurs, la NSA proposait des accords à certains pays et leur fournissait des technologies d'écoute avancées, puis ils partageaient leur usage. C'est pourquoi il est essentiel que les pays de l'UE mettent en commun leurs capacités numériques et fassent face au cyberespionnage ensemble, afin de garantir un usage éthique et digne de confiance du numérique.

c) Indépendance numérique pour l'Europe

La pandémie du Covid-19 a été un révélateur des dépendances industrielles stratégiques de l'UE. Le recours massif aux services numériques proposés par les géants américains a exacerbé la faiblesse relative de l'Europe sur un secteur éminent stratégique, bien au-delà du contexte pandémique. Sur les terrains matériel (puces, câbles, data centers), logiciel (y compris IA) et sémantique (contenus), l'Europe est dépendante de matériaux et technologies dont les chaînes de valeur sont dominées par les Etats-Unis, la Chine, Taïwan et la Corée du Sud.

L'Europe ne peut techniquement pas se passer des entreprises non européennes. C'est pourquoi la stratégie industrielle de l'Europe dans le numérique entend reconquérir des capacités, sans s'isoler. Elle se distingue surtout par la défense des valeurs européennes (respect des droits fondamentaux, équité, recherche du progrès social et environnemental…), ce qui ne garantit pourtant pas l'indépendance technologique. Cependant, de nouvelles alliances et collaborations se mettent en place, telles que le financement du futur drone MALE européen (eurodrone) offrant à l'Allemagne, la France, l'Italie et l'Espagne de se passer du Reaper américain. Si les industriels réussissent à travailler ensemble, autour de programmes désormais trop complexes pour être tenus par un pays seul, il est permis de croire à des alliances industrielles stratégiques renouvelées dotant l'Europe d'authentiques capacités d'indépendances.

D'autre part, l'UE a créé le programme pour une Europe numérique (DIGITAL), un nouveau programme de financement axé sur l'apport des technologies numériques aux entreprises, aux citoyens et aux administrations publiques. Il souligne à quel point il est important que l'Europe ne dépende pas des systèmes et des solutions provenant d'autres régions du monde. Le programme DIGITAL ouvre la voie à cet objectif. Le programme pour une Europe numérique fournira un financement stratégique pour relever ces défis, en soutenant des projets dans cinq domaines clés de capacité: dans les domaines du supercalcul, de l'intelligence artificielle, de la cybersécurité, des compétences numériques avancées et de la garantie d'une large utilisation des technologies numériques dans l'ensemble de l'économie et de la société. Avec un budget global prévu de 7,5 milliards d'euros, il vise à accélérer la reprise économique et à façonner la transformation numérique, en apportant des avantages à tous, mais en particulier aux petites et moyennes entreprises. Le programme s'inscrit dans le cadre d'autres initiatives européennes telles que Horizon Europe pour la recherche et l'innovation et le mécanisme pour l'interconnexion en Europe pour les infrastructures numériques, la facilité pour la reprise et la résilience et les fonds structurels. De même, en décembre 2020, le Conseil et le Parlement européen sont parvenus à un accord informel sur la proposition établissant le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité, soutenu par un réseau de centres nationaux de coordination.

Ainsi, les pays de l'UE cherchent à s'unir et s'allier, en créant des programmes européens, mettant en œuvre des innovations européennes et des fonds européens, afin de créer un environnement numérique qui respecte les droits humains.

IV. Sitographie

INTRODUCTION

https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_fr

https://www.consilium.europa.eu/fr/topics/digital-europe/

https://www.touteleurope.eu/economie-et-social/le-numerique-dans-l-union-europeenne/

https://www.larousse.fr/dictionnaires/francais/num%C3%A9rique/55253

https://www.youtube.com/watch?v=Ry2UQL9fVzw

https://www.thpanorama.com/blog/cultura-general/las-9-actividades-econmicas-de-europa-principales.html

https://presidence-francaise.consilium.europa.eu/media/zp2jt3up/european-ethical-principles-for-digital-health_fr_eng.pdf

BILAN HISTORIQUE

Commission Européenne: libre circulation des données non personnelles
https://digital-strategy.ec.europa.eu/en/policies/non-personal-data

Règlement de l'UE sur la cybersécurité
https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
https://www.consilium.europa.eu/fr/policies/cybersecurity/#

Directive de l'UE sur les données ouvertes
https://digital-strategy.ec.europa.eu/en/policies/legislation-open-data

RGPD
https://www.cnil.fr/fr/reglement-europeen-protection-donnees
https://fr.wikipedia.org/wiki/R%C3%A8glement_g%C3%A9n%C3%A9ral_sur_la_protection_des_donn%C3%A9es#cite_note-2

Stratégie sur l'IA
https://www.senat.fr/europe/textes_europeens/ue0144.pdf

Lignes directrices en matière d'éthique pour une IA digne de confiance
https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Commission Européenne: Une Europe adaptée à l'ère du numérique -> sur l'Intelligence artificielle
https://ec.europa.eu/commission/presscorner/detail/fr/IP_21_1682

Cybermenaces:
https://www.eset.com/fr/cybermenaces/#:~:text=Les%20cybermenaces%20sont%20des%20tentatives,les%20particuliers%20que%20les%20entreprises

https://www.touteleurope.eu/economie-et-social/cybersecurite-que-fait-l-union-europeenne/

Cyberrésilience:
https://www.consilium.europa.eu/fr/policies/cybersecurity/#:~:text=En%20octobre%202020%2C%20les%20dirigeants,des%20fins%20judiciaires%20et%20r%C3%A9pressives

https://digital-strategy.ec.europa.eu/fr/policies/cybersecurity

Cyberespionnage:
https://www.numerama.com/cyberguerre/969411-cyberattaques-ciblant-lunion-europeenne-cest-essentiellement-de-lespionnage.html

CONTEXTUALISATION POLITIQUE

https://eurohpc-ju.europa.eu/index_en

Rapport 2021-2022 sur le numérique en Europe

https://www.touteleurope.eu/societe/numerique-le-classement-2020-des-pays-europeens/

Pegasus
https://fr.wikipedia.org/wiki/Projet_Pegasus_(journalisme)
https://www.euractiv.fr/section/economie/news/lutilisation-systematique-de-logiciels-espions-par-certains-gouvernements-de-lue-denoncee-par-des-eurodeputes/
https://securite.developpez.com/actu/338561/De-multiples-Etats-membres-de-l-union-europeenne-font-usage-L'utilisation « systématique » de logiciels espions par certains gouvernements de l'UE dénoncée par des eurodéputés – EURACTIV.frde-logiciels-espions-sur-leurs-citoyens-a-des-fins-politiques-et-meme-des-systemes-embarques-espions-concus-pour-des-regimes-autoritaires/
https://www.politico.eu/wp-content/uploads/2022/11/08/PEGA-draft-report-final-8-1117473.pdf
https://www.lepoint.fr/politique/emmanuel-berretta/logiciel-espion-cinq-etats-europeens-sur-le-gril-10-11-2022-2497246_1897.php#11

Europe espionnée par NSA
https://www.la-croix.com/Monde/Europeens-espionnes-NSA-lunivers-numerise-notion-dallie-nexiste-pas-2021-06-04-1201159403
https://www.touteleurope.eu/l-ue-dans-le-monde/renseignement-le-danemark-accuse-davoir-facilite-lespionnage-de-dirigeants-europeens-par-la-nsa/

Indépendance numérique:
https://incyber.org/quelle-independance-numerique-pour-leurope/
https://digital-strategy.ec.europa.eu/fr/activities/digital-programme

https://www.consilium.europa.eu/fr/policies/cybersecurity/#:~:text=En%20octobre%202020%2C%20les%20dirigeants,des%20fins%20judiciaires%20et%20r%C3%A9pressives

Cybermenaces:

https://digital-strategy.ec.europa.eu/fr/policies/cybersecurity

https://www.consilium.europa.eu/en/infographics/cyber-threats-eu/

https://www.eset.com/fr/cybermenaces/#:~:text=Les%20cybermenaces%20sont%20des%20tentatives,les%20particuliers%20que%20les%20entreprises

https://www.techtarget.com/searchsecurity/definition/supply-chain-attack

https://www.enisa.europa.eu/news/ransomware-publicly-reported-incidents-are-only-the-tip-of-the-iceberg

DDoS record:
https://www.bitdefender.com/blog/hotforsecurity/new-ddos-attack-in-europe-breaks-previous-record-set-only-two-months-ago/

ENISA threat landscape:
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (il faut le télécharger)