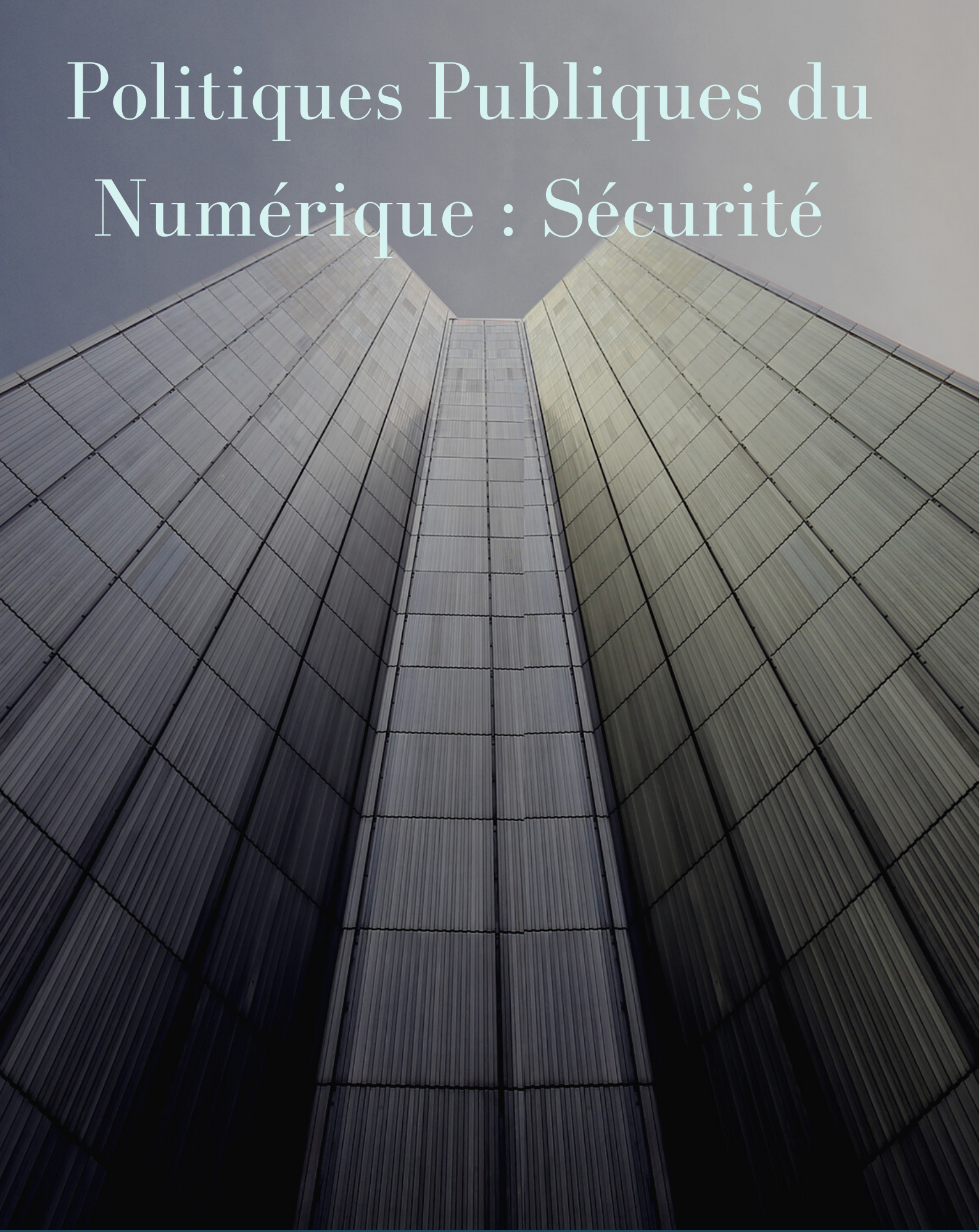
Politiques Publiques du Numérique : Sécurité



Hansen Luc
Lopez Luca
Dupille Arnaud
Julien Grégory
Elie Dit cosaque Arnaud

Master AFPU
IEP de Fontainebleau
77300
France

Qu’est-ce que la souveraineté numérique ? Quels sont les enjeux de souveraineté numérique qui s’imposent aux sociétés contemporaines et quelles solutions peuvent-elles déployer pour y répondre ?

La globalisation de l’usage du numérique dans nos sociétés, aussi bien par les individus au quotidien que par les organisations qui constituent sa gouvernance et son activité, pose depuis plusieurs années l’enjeu de « faire face » à cette révolution numérique.
Parmi les défis posés à nos sociétés et à leurs constituants on trouve celui de l’indépendance, autrement dit de la souveraineté numérique. Si une indépendance individuelle face aux influences des acteurs du World Wide Web (WWW) semble idyllique à notre époque, la question de l’indépendance d’une Nation, de son économie et de son fonctionnement vis-à-vis d’influences extérieures concurrençant sa souveraineté semble être une réflexion plus réaliste et nécessaire à entreprendre.

L’espace numérique ou le cyberespace

Pour comprendre les enjeux de la souveraineté numérique, il est d’abord important de définir schématiquement et simplement le rôle du « cyberespace », ou de « l’espace numérique » dans les activités humaines.
Tout d’abord, pour des individus peu informés sur les enjeux numériques, c’est un sujet dont « l’ontologie profonde » est bien moins complexe qu’un programme informatique. C’est avant tout un milieu stratégique comme les autres, au même titre, par exemple, que les espaces stratégiques militaires, économiques ou politiques . Il constitue un enjeu majeur aussi bien au niveau individuel que collectif (local, national, international) et remet en cause l’anonymat de la vie privée comme l’assurance de l’indépendance du fonctionnement des technologies d’une organisation, d’une infrastructure, etc.

La souveraineté numérique : action, unification globale et vulnérabilités

Comment peut-on ensuite définir la souveraineté numérique ? Dans le rapport sénatorial de Gérard Longuet de 2019, la souveraineté numérique est définie par « la capacité de l’État à agir dans le cyberespace », à le réguler et à peser sur celui-ci et son autonomie volatile. Il ne s’agit plus de savoir comment l’État et la société civile influent sur les activités du WWW mais, dans des sociétés libérales qui lui permettent d’avoir une influence remarquable et indépendante. Comment l’État et la société civile peuvent réguler les activités et les influences du WWW. Agir dans ce secteur stratégique, qui ne dépend pas que d’eux. C’est un espace « a-régulé mais encadré » et, c’est fondamental, à encadrer.
Il s’agit également d'un espace qui revêt deux caractères intrinsèques, d’une part l’unicité et d’autre part la standardisation.
Unicité par la centralisation du fonctionnement d’internet, si on prend par exemple les GAFAM et leur rôle dans le fonctionnement de l’espace numérique on comprend rapidement ce caractère d’unicité, voire de monopole. Grégoire Germain et Paul Massart font une comparaison judicieuse : « d’un point de vue systémique, la dimension énergétique ne revêt pas ce caractère d’unicité et de standardisation, ce qui rend nos approvisionnements en énergie beaucoup moins vulnérables grâce à la multiplicité et à la diversité des modes de production et de la segmentation du secteur énergétique ».

Standardisation par la pénétration du monde numérique dans la plupart des activités humaines. Aussi bien dans les secteurs les plus sensibles d'une société tels que la défense, la sécurité, la santé, la pérennité du fonctionnement administratif, que dans des activités plus quotidiennes : les transports, le commerce, l'échange d'information. Une majorité des activités humaines contemporaines sont interdépendantes de l'espace numérique. « La numérisation a donc pris un rôle unique qui lui donne une position de surplomb sur toutes les autres ». La cybersécurité est un enjeu stratégique comme les autres, mais il est en réalité un "supra-enjeu" stratégique ou un "milieu" stratégique, puisque tous les autres secteurs des activités humaines tendent à devenir interdépendants de celui-ci.

Ces deux caractéristiques en font un espace vulnérable. Vulnérable par son unicité - comme le montre la comparaison systémique avec l'énergie – et par l'interdépendance des autres activités humaines à cet espace. En temps de guerre comme de paix, une déstabilisation des réseaux numériques, de l'espace numérique, aurait des effets qualifiables du handicap aux habitudes ou au travaux quotidiens à la catastrophe selon l'ampleur de l'impact.

L'espace numérique : un milieu « vulnérable et contesté »

Il est d'autant plus vulnérable puisqu'il est également contesté et enjeu de concurrence, de puissance, voire d'affrontement comme dans la Guerre en Ukraine et son volet de guerre d'information ou en Afrique entre la France et la milice Wagner. Pour de nombreux acteurs dont les États, les entreprises et les individus sont aussi bien émetteurs que récepteurs de ce nouvel ordre numérique. Enjeu de souveraineté nationale, au fonctionnement central et vulnérable, l'espace numérique constitue un « milieu » stratégique pour tous les secteurs d'activité d'une nation ou d'une organisation. Il est devenu « un enjeu décisif dans les rapports de force », entre individus et organisations, entre individus, entre États, entre intérêts d'origines diverses, dont étrangers, etc. « Les acteurs étatiques et industriels qui en maîtrisent les ressorts conserveront l'initiative et l'indépendance et ils pourront préserver leur invulnérabilité. Inversement, ceux qui perdront le contrôle de certains compartiments de ce « terrain » seront réduits à agir en réaction, à dépendre d'autres acteurs hégémoniques et à subir les conséquences de leur vulnérabilité ». Les enjeux de souveraineté numérique impactent à la fois le secteur public mais également le secteur privé.

I- La souveraineté numérique : une imposition de ses enjeux

1- Les enjeux pour le secteur public

Le domaine public est le premier secteur auquel on pense quand on parle de vulnérabilité numérique. Le secteur régalien et militaire évidemment, qui est un des grands sujets de cybersécurité du XXIème siècle. Mais cette menace se ressent dans tous les autres secteurs de l'Etat, administrations pourtant historiquement moins touchées par les risques du numérique que le secteur privé. En effet la tendance s'est inversée avec un taux d'attaque des administrations qui rattrape celui du secteur privé, de par la transition numérique opérée qui rend le secteur public plus vulnérable. Il est donc devenu une cible privilégiée, car hors du domaine de la défense, les administrations sont des cibles plus faciles que le privé qui subit depuis plus longtemps ces attaques et a eu plus de temps pour s'y adapter. Les administrations sont donc devenues une cible privilégiée des cyberattaques ces dernières années, spécialement deux types d'administrations, les collectivités locales et les hôpitaux.

Augmentation des attaques sur le secteur public

Ainsi depuis 2020 les organisations publiques ont subi une hausse des intrusions de 37%. Les collectivités locales et les établissements de santé représentent 85% des administrations publiques victimes de ces attaques. Près de 30% des collectivités ont subi une attaque au rançongiciel, soit une augmentation de 50% entre 2019 et 2020. Le nombre d'incidents en sécurité informatique a doublé entre 2020 et 2021 selon l'ANS (agence du numérique en santé).
Dès lors, la sécurité numérique devient un sujet majeur pour les administrations publiques. Si jusqu'alors les organisations privées semblaient de loin les plus touchées par les cyberattaques, la tendance a largement rattrapé cet écart ces dernières années. Ce sujet ne peut plus être ignoré par les autorités publiques tant il pose des enjeux cruciaux et multiples.

Atteintes à l'essence du service public

En plus de la question de la souveraineté numérique, on peut identifier deux enjeux majeurs :

- **Un enjeu de confiance des usagers envers leur administration.** L'augmentation des cyberattaques contre les informations relatives aux citoyens a de lourdes conséquences à la fois réputationnelles et légales (sanctions CNIL), débouchant sur une défiance des citoyens envers des administrations. Les grands événements à venir en France (Coupe du monde du rugby 2023, Jeux Olympiques Paris 2024), catalyseurs d'innovation numérique, et les chantiers de transformation numérique d'envergure portés par l'État (dossier médical partagé, identité numérique, politique de la donnée, dématérialisation accélérée des démarches, …) pourraient ainsi être remis en question par l'émergence de cette société de défiance.

On en a notamment vu l'exemple lors de la mise en place de l'application *TousAntiCovid* durant la pandémie, qui a fait face à des réticences sur ces questions de données personnelles. Alors même que l'ensemble de ces données sont déjà possédées par les grands groupes, remettre nos données à l'Etat semble plus compliqué pour les citoyens.

- **Un enjeu opérationnel de continuité et de délivrance des services publics.** Une perturbation ou une paralysie du fonctionnement du service public recouvre de forts impacts sur la vie quotidienne des citoyens (non-accès à des services essentiels, non-recours aux droits, …), et sur l'attractivité et le développement économique de notre pays.

C'est donc la nature même du service public qui est remise en cause par ces attaques. En atteignant la continuité et l'efficacité du service public, et donc par effet domino la confiance des citoyens envers l'administration, l'ensemble de la structure publique est remise en cause par ces vulnérabilités. Comment faire confiance à un hôpital si nos données de santé peuvent être pillées par rançongiciel pour être revendues par la suite à tout moment ? L'Etat fait face à des enjeux majeurs à la fois sur le plan de la défense de sa souveraineté, sur le plan militaire et sur le plan du service public. Ces enjeux ne concernent pas uniquement le secteur public mais également le secteur privé.

2- Les enjeux pour le secteur privé

Le secteur privé est une cible de prédilection pour les cyberattaques. Il s'agit d'un secteur visé notamment pour l'impact symbolique contre certaines sociétés, ainsi que pour le gain d'informations pouvant être valorisé.

A la suite du COVID, 27% des salariés pratiquent le télétravail. Pour beaucoup d'entreprises, cela signifie donner l'accès de leurs serveurs à des personnes physiquement hors de leur structure. Cela a pour conséquence une augmentation du risque de vulnérabilité. Selon les chiffres communiqués par Guillaume Poupard, le directeur général de l'ANSSI, le nombre de cyberattaques a été multiplié par 16 entre 2019 et 2021. Entre le 1er et le 23 mars 2020, les attaques de phishing signalées ont augmenté de 667%.

Dans un rapport du Sénat de 2021 , la délégation aux entreprises estime quatre motifs de banalisation de la cybercriminalité :

- La numérisation de l'économie, qui a notamment été accélérée depuis le confinement.
- La professionnalisation de la cybercriminalité, qui a été facilité par le développement de la cryptomonnaie.
- La difficulté de la prévention, qui nécessite entre autre une coopération internationale.
- L'intégration du cyberespace comme nouveau lieu de conflit géopolitique, faisant des entreprises des cibles collatérales.

En chiffre, selon le Figaro, les coûts liés à la cybercriminalité constitue une facture de 6 000 milliards de dollars en 2021 au niveau mondiale. Les grosses entreprises ne sont pas les seules impactées, 43% des attaques en 2020 étaient dirigées contre des PME. Pour 50% des PME, l'attaque est fatale, contre 16% de faillite en moyenne .

Pour le président de la Réserve Fédérale des Etats-Unis, M. Jerome POWELL, les cyberattaques contre les entreprises représentent un risque supérieur pour l'économie que la crise de 2008.

Prévention et Formation

La France manque de compétences. D'une part, le secteur de l'informatique est en pleine expansion. Dans le rapport « Métier 2030 » de France Stratégie , environ 75 000 postes seront à pourvoir d'ici 2030. Déjà qu'aujourd'hui, la pénurie de main d'œuvre produit un effet de bord avec la hausse du salaire moyen d'un ingénieur en cybersécurité. Cela a pour conséquence de rendre la compétence inaccessible pour une PME / TPE. Pour 60% des PME européennes, les ressources ne sont pas suffisantes pour accéder à une protection . Ainsi, quand les grands groupes sont visés, c'est davantage leurs sous-traitants, ainsi que les petites entreprises, ayant des sécurités plus faibles ou datées qui subissent les attaques.

Lorsqu'il s'agit de société en partenariat avec l'Etat, celles-ci sont encouragées à s'entraider : à l'instar du cybercampus du site de La Défense. Il permet aux entreprises de partager leurs expériences et de se maintenir à jour sur les nouvelles techniques de cybersécurité.

Un enjeux d'image, de confiance et de responsabilité

Les entreprises sont très scrutées par le législateur notamment français et européen sur leur gestion des attaques. En effet, avec les crises comme Cambridge Analytica, les consommateurs et les États sont devenus particulièrement sensibles sur le traitement réservé à leur donnée. Chaque attaque incrémente la défiance de la population envers l'entreprise victime.
Et l'image de marque n'est pas le seul risque des entreprises.

Économiquement, une attaque informatique coûte en moyenne entre 15 000 et 4 millions d'euros.
Au vu du risque sur les comptes de la société, les agences de notation boursières (ESG) prennent en compte le risque cyber dans leurs critères d'évaluation. Après une attaque, les investisseurs seront moins susceptibles de placer leurs économies dans la société.

Lors de la fuite de données provoquée par une attaque contre Facebook, le groupe s'est effondré de 20% en bourse et a perdu quelques millions d'utilisateurs. Face à ces nouveaux enjeux de souveraineté numérique l'État a décidé de mener différent type d'action tant dans le secteur public que privé.

II- Préserver la souveraineté numérique : les actions étatiques

1- La stratégie étatique de protection du secteur public

Quelles réponses peut alors apporter l'État à ces nouvelles menaces ? Pour pallier ses vulnérabilités, l'État a mis en place toute une batterie de mesures depuis ce qu'on peut appeler le début de la prise en compte de ces enjeux de sécurité, symbolisé par la publication du rapport Lasbordes "la sécurité des systèmes d'information, un enjeu majeur pour la France" en 2006.

La régulation française a beaucoup évolué ces dernières années, et l'ensemble de la stratégie de l'État pour la sécurité numérique est dirigée par un grand organisme, l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Sa création s'appuie sur un postulat très simple, la sécurité informatique est un domaine à part, une discipline purement scientifique. Cette discipline s'appuie sur la science des systèmes d'informations en s'attelant à leur sécurisation. Ainsi, cette discipline a toujours un temps de retard car suivant chronologiquement l'évolution de la première. Compte tenu de ce postulat, il est donc impératif pour la puissance publique d'assurer une vulgarisation ainsi qu'une application de cette science. C'est dans ces objectifs que fut créée l'ANSSI.

Présentation de l'ANSSI

L'Agence nationale de la sécurité des systèmes d'information est un service du Premier Ministre français créé par décret en juillet 2009, remplaçant ainsi la DCSSI. Il est intégré au secrétariat général de la Défense et de la Sécurité nationale (SGDSN), autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale ainsi que de la coordination des ministères intéressés. Dotée d'un budget de 136 millions d'euros, elle représente les deux tiers du millier d'effectifs du SGDSN. Depuis 2014, son directeur est M. Guillaume Poupard (auteur de l'intervention retranscrite ci-après). L'ANSSI a une compétence nationale témoignant d'une centralisation des politiques publiques en matière de protection numérique mais dont l'application demeure déconcentrée.

Le rôle de l'ANSSI

Il s'agit d'une autorité de sécurité et de défense. En ce sens, elle possède une double casquette.
En tant qu'autorité de sécurité, elle établit une réglementation contraignante, qualifie des produits et prestataires, prodigue conseils et assistance, effectue un travail de recherche, fournit une expertise technique et se charge d'un contrôle. En ce sens, elle agit tant sur les secteurs publics que privés, mais plus particulièrement sur certains acteurs juridiquement qualifiés Ex : OIV.
En tant qu'autorité de défense, elle veille et détecte les attaques malveillantes et y répond si nécessaire. Elle surveille en temps réel les infrastructures critiques. Contrairement à ses homologues étrangers, l'ANSSI n'effectue aucune attaque et ne fait pas de renseignement (NSA). Dans ce cadre, l'ANSSI s'intéresse aux Institutions, aux ministères, OSE et OIV dans ce cadre.

Typologie de la cybersécurité

Selon ses critères de définition, l'ANSSI classifie les données selon qu'elles soient sensibles ou non (classification similaire à celle du RCPD). Par définition, une donnée est dite sensible lorsqu'elle touche aux intérêts essentiels de celui auquel elle se rapporte.
Quoiqu'il en soit, quatre critères de protection des données seront retenus pour déterminer si celles-ci sont effectivement protégées.

- **Disponibilité/Accessibilité** : accès réservé aux concernés.
- **Intégrité** : réalité et exactitude des données et réelle.
- **Confidentialité** : accéder au moment où c'est nécessaire.
- **Traçabilité** : On va déterminer d'où viennent les données et leur parcours.

En outre, les attaques informatiques peuvent provenir de différentes entités :

- Services étatiques.
- Société de renseignements privées.
- Activistes.
- Criminalité organisée.
- Terroristes.

Mais les victimes se retrouvent dans tous les secteurs. Évidemment, chaque entité malveillante ciblera une victime l'intéressant. Ainsi, un service étatique ne s'en prendra vraisemblablement pas à un particulier pour une finalité financière.

S'il fallait dresser un bilan de la cybersécurité pour l'ANSSI, et a fortiori pour l'ensemble des sécurités des systèmes d'information, il faudrait différencier au sein de la cybersécurité :

- La **cyberprotection** garantissant la protection effective des données, couverte par les deux autres. C'est donc la résultante de la cyberdéfense et de la cyber-résilience.
- La **cyberdéfense** soit la lutte contre les cyberattaques, que constitue la lutte informatique défensive localisée à Paris.
- La **cyber-résilience**, soit la capacité d'un système à renaître après un dysfonctionnement dû à un sinistre accidentel. Ce service est assuré, pour les Armées par exemple, par la DIRISI.

Les ressources juridiques

Outre les textes mentionnant sa création, plusieurs normes juridiques viennent compléter l'action de l'ANSSI ou la contraindre.

En premier lieu, le Livre blanc de la Défense de 2013 , plus haute norme relative à la Défense, où les menaces y sont hiérarchisées. Il peut être observé que le volet informatique est considéré comme l'une des plus grandes menaces contemporaines. Voici le classement du livre blanc de la défense de 2013 :

1. Menaces terroristes
2. Attaques informatiques
3. Menaces balistiques
4. Pandémies
5. Catastrophes naturelles ou industrielles
6. Criminalité organisée

De surcroît, les attaques informatiques recouvrent une réalité très large : espionnage, agitation, propagande, destruction, fraude, neutralisation, pré positionnement pour une invasion….
Mais en plus de ce Livre Blanc, la réglementation autour de l'ANSSI s'étoffe au fil des années :

- Le dispositif de protection du potentiel scientifique et technique de 2011.
- Loi de programmation militaire de 2013, Article 22 définissant les "opérateurs d'importance vitale" (OIV).
- RGDP de 2016.
- Directive euro Network and information security (NIS) de 2016.
- Loi du 26 février 2018 définissant les "opérateurs de services essentiels", transposition de la NIS.
- SO/CEI 27000 comprenant les normes de sécurité de l'information publiées conjointement par l'Organisation internationale de normalisation et la Commission électrotechnique internationale.
- Aide aux dispositifs PPST pour le patrimoine (promouvoir le dispositif local de PPST et sensibiliser le secteur de la recherche aux enjeux de la SSI. En collaboration avec le SGDSN/AIST)

Les missions de l'ANSSI couvrent donc un secteur très large, allant des Institutions aux particuliers. Il convient de préciser que, de manière générale, les actions de l'ANSSI seront parallèles entre le secteur public et le secteur privé. Plus précisément, les réglementations qu'émettra l'ANSSI à l'endroit des personnes publiques seront également des recommandations pour le secteur privé. Seule la nature des actes varie.

En la matière, l'une des règles d'hygiène informatique de l'ANSSI constitue la mise en place d'une politique de sécurité des systèmes d'informations. En d'autres termes, chaque entité, qu'elle soit publique ou privée, se doit d'avoir une réglementation interne afin d'assurer la protection de ses données.

Le cas des Armées (PSSI-A)

Les armées ont donc mis en place leur propre PSSI-A afin d'assurer la sécurité des systèmes d'informations de la Défense Nationale. Cette mise en place résonne avec la mise en avant des enjeux numériques et leur apparition dans le Livre Blanc de 2013. En la matière, la cyberprotection s'opère par trois biais : la sécurité informatique, la sécurité des communications et la sécurité du personnel. Ces trois biais ayant pour finalité de garantir une confidentialité, disponibilité, accessibilité et traçabilité des données.

A noter qu'un système d'informations n'est pas nécessairement numérique. Théoriquement, les données physiques obéissent à la même logique : un ensemble structuré de données organisées. Lorsque que les nouvelles technologies sont en cause, c'est à dire les systèmes SIC, la réglementation en question s'applique.

Le PSSI-A est ainsi issu d'une instruction ministérielle (IM2003) et s'intéresse donc à la politique de sécurité des systèmes d'informations. Constitué de 57 règles (allant des règles d'accès, des périphériques USB, à l'utilisation de stations blanche), il faut remarquer son aspect très concret mais également très similaire à l'ensemble des autres secteurs. En effet, une chaîne de cybersécurité est aussi forte que le maillon le plus faible. Ladite chaîne obéit donc à la même logique quel que soit le réseau en cause. La seule différence sera donc la résistance de chacun des maillons exigés selon l'importance des données en jeu.

A noter que ce dispositif évolue. Ainsi, le projet Spartacus mené par la DIRISI a pour but de mettre en place des meilleures stations blanches en réseau ou encore d'assurer la désactivation automatique des clés hors du système.

L'ANSSI a pour vocation de protéger les institutions des menaces mais son secteur d'activité concerne l'ensemble de notre société y compris le secteur privé.

2- La stratégie étatique de protection des citoyens et du secteur privé

L'ANSSI mène donc également une action pour l'ensemble des citoyens.

L'ANSSI et les citoyens

De manière courante, elle est accessible via son site internet. De même, certains guides sont développés à l'usage des décideurs privés pour une bonne gouvernance de la cybersécurité et à l'usage des responsables SSI, par définition beaucoup plus techniques. De même des guides des bonnes pratiques pour tout un chacun est publié. En somme, un grand nombre de guides constituant une forte politique de prévention considérant la grande pluralité des types d'attaques :

- Rançon logiciels (ordinateur pris en otage) : Possibilité de rançonner et en plus de récupérer les données.
- Compromission et latéralisation : On s'attaque à des petites victimes afin d'avoir accès à de plus grosses cibles.
- Point d'eau : création d'un faux site.
- Homme du milieu : infiltrer la connexion de l'intéressé et se substituer à sa banque.
- Botnet : participe à miner du Bitcoin en utilisant une partie des capacités de l'infecté.
- Typosquatting : Faux site avec un nom très similaire.

En vue de répondre à tous ces types d'attaques, les règles d'hygiène informatique se présentent en plusieurs idées :

- Approche méthodologique, (ISO 27002, 114 mesures organisationnelles et techniques), Mise en place d'un système de management de la sécurité et de l'information (Préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information)
- La roue de Diming : Mise en place qu'un processus qualitatif pour la protection de l'information. Pour cela, il peut être fondamental de désigner un RSSI, responsable ou référent.
- Cartographier le système d'informations et les informations sensibles. En d'autres termes, assurer un véritable management de l'information (notamment sensible). Pour cela il s'agit de donner l'accès à ceux qui ont besoin de la connaître seulement. Cloisonner et filtrer les flux (cloisonnement réseau, cloisonnement système, cloisonnement cryptographique. Concrètement, il convient ainsi de dresser des firewalls entre Internet, l'Intranet et le DMZ.
- Contrôler les accès physiques et logiques, le mot de passe correspond à 80% du travail.
- Le principe du moindre privilège, par principe chacun a un compte utilisateur et pas un administrateur. En somme, sans besoin impérieux, le moins de droits possible doit être accordé. Dans un autre sens, il faut supprimer les comptes des anciens employés et mettre à jour les logiciels sans en télécharger d'autres suspects. Enfin, séparer les usages (entre personnel et professionnel).
- Instaurer un antivirus et des stations blanches. De surcroît, ne pas utiliser les clés USB offertes. Chiffrer les informations sensibles sans oublier les disques durs. Sauvegarder les données. Sensibiliser, contrôler, détecter une attaque, anticiper et, le cas échéant, mettre en place une cellule de crise.

Les principaux textes pour la protections des entreprises en France

Depuis plusieurs années, la question de la cybersécurité est devenue un enjeu majeur pour la France. Dès 2005, un chantier sur la lutte contre la cybercriminalité avait été lancé. En 2006, le rapport Lasbordes insistait sur l'importance de la sécurité des systèmes d'information. En 2008, l'ANSSI publiait un Livre blanc sur la sécurité et la défense nationale, tandis que le rapport Romani de la Commission des Affaires étrangères, de la Défense et des Forces armées du Sénat était rédigé à la suite de l'attaque informatique de l'Estonie.

En 2011, le Ministère de la Défense a intégré le risque cyber à son organigramme et nommé un officier général chargé de la cyberdéfense pour coordonner les actions et gérer les crises. Deux ans plus tard, en 2013, le Livre blanc "Menace cyber" a été publié. En 2014, le Ministère de l'Intérieur a nommé un préfet chargé de la lutte contre les cybermenaces.

En 2015, la Stratégie nationale pour la sécurité du numérique a été lancée, tandis qu'un décret renforçait les obligations en matière de cybersécurité des Opérateurs d'Importance Vitale (OIV)[1]. L'année suivante, en 2016, la réserve opérationnelle de Cyberdéfense a été lancée, venant s'ajouter à la Réserve citoyenne de cyberdéfense (RCC) pour mobiliser un grand nombre de "cyber combattants" en cas d'attaque.

En 2018, le Règlement général européen de Protection des Données (RGPD) est entré en vigueur, contraignant toutes les entreprises exerçant sur le territoire européen à respecter un certain nombre de dispositions protectrices des données personnelles des utilisateurs.

En 2020, le Conseil national de l'Industrie a lancé le Contrat Stratégique de la filière "Industrie de Sécurité" [2], appelant à positionner l'industrie française comme leader mondial de la cybersécurité de l'IoT. En 2021, le Sénat a publié un rapport sur la cybersécurité des entreprises, soulignant l'importance de prévenir et guérir les cyber-attaques.

Enfin, en 2021, le ministère de l'Economie a lancé une Stratégie nationale pour le Cloud, rejoignant l'initiative Gaia-X. Avec l'échec du projet Andromède[3] , la France rejoint cette initiative allemande, abandonnant l'idée de créer ex-nihilo une nouvelle entreprise. L'objectif est de créer un organisme de gouvernance chargé de réguler et standardiser les technologies de données. Ce rapport acte l'avance non rattrapable du secteur privé américain. L'objectif est désormais de maîtriser la dépendance dans la durée, à l'instar du nucléaire, dont l'autonomie de la France a pu se développer malgré une technologie sous licence américaine.

Les OIV

L'ANSSI apporte son assistance aux sociétés OIV ou « Opérateurs d'Importance Vitale ». L'objectif est d'éviter des situations de crises où des infrastructures d'importance critique sont inaccessibles. Les États-Unis ont vécu une attaque cyber sur leurs oléoducs . 45% des carburants normalement consommés par la côte Est des États-Unis ont été bloqués. Si le FBI est intervenu, une rançon de 5 millions de dollars aurait été versée aux groupes de pirates.

Un enjeu d'image, de confiance et de responsabilité

Enfin, après une attaque, les États sanctionnent. La CNIL en France se base sur l'article 29 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : « toute personne ordonnant ou effectuant un traitement d'informations nominatives, s'engage de ce fait, vis-à-vis des personnes concernées, à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées, ou communiquées à des tiers non autorisés ». Le non-respect de cet article est sanctionné pénalement par l'article 226-17 du code pénal (cinq ans d'emprisonnement et 300 000 euros d'amende). L'article 17 de la directive du 24 octobre 1995 vient compléter cette obligation de sécurité qui pèse sur le responsable du traitement. Celui-ci « doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que toute autre forme de traitement illicite. Ces mesures doivent assurer, compte-tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des risques à protéger ».

Au niveau européen, la RGPD impose les mêmes responsabilités notamment à son article 32, dont le G29 (regroupement de CNIL européennes) à la compétence de contrôle.

Au vu des conséquences, les sociétés peuvent être tentées de cacher les assauts qu'elles subissent.
La société UBER a vécu une attaque en 2016, au bilan de 57 millions de comptes d'utilisateurs piratés. Afin de dissimuler cette attaque, le dirigeant de l'époque a payé les pirates 100 000$ contre leur silence. En 2017, l'affaire est exposée, l'entreprise sera sanctionnée d'une amende de 400 000€ en France. La CNIL française a estimé que l'attaque « n'aurait pu aboutir si certaines mesures élémentaires en matière de sécurité avaient été mises en place ». Cette sanction sera imitée dans d'autres pays européens, 430 000€ en Grande Bretagne et 600 000€ par les Pays-Bas.

Depuis la mise en application du RGPD, les entreprises risquent jusqu'à 2% de leur chiffre d'affaires mondial et le fait de dissimuler les attaques est un élément aggravant.

Ainsi, si les grosses structures sont les plus aptes à répondre aux attaques, il est recommandé pour les PME de se tourner vers des plateformes comme cyber malveillance.gouv.fr, qui comporte un service d'urgence. Dans ses propositions, la délégation aux entreprises du Sénat appelle à une facilitation des dépôts de plainte anonyme, et des "équipes de réponses aux incidents informations" (CSIRT : Computer Security Incident Response Team) a échelle régionale.

L'ANSSI a d'ores et déjà démarré des simulations d'attaque de grande d'ampleur, dernièrement avec 200 participants et 100 organisations. La France mise notamment sur la mise en place de certification, garantissant la résistance des systèmes d'informations.

La délégation appelle également à une revalorisation du rôle des assurances :

- Par une meilleure compréhension du risque, en ayant la connaissance la plus exhaustive possible des sinistres.
- Par l'utilisation de logiciels et d'experts en cybersécurité certifiés, afin de promouvoir le label Expert Cyber.
- Par la création d'une agence de cyber notation européenne, utilisant les référentiels de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), ou française, utilisant ceux de l'ANSSI.

Conclusion

En somme, la souveraineté numérique est un enjeu qui ne cesse de croître en importance, de pair avec la cybercriminalité. Occasionnant des coûts de 6.000 milliards au niveau mondial par ses attaques en 2021, représentant la deuxième menace de sécurité en France selon le livre blanc de la Défense de 2013, derrière les attaques terroristes, elle s'affirme comme une puissance remettant en cause la souveraineté des Etats.

Les enjeux régaliens de protection des administrations, des entreprises et des citoyens représente un véritable défi pour les États et une véritable menace pour les sociétés. Cibles privilégiées des attaques numériques, les entreprises sont en passe d'être dépassées par les administrations, moins préparées à ces assauts. Ces attaques ne touchent plus seulement en majorité le fonctionnement ou le capital d'une entreprise, mais les services publics, remettant en cause leur nature même, basés sur un principe de pérennité essentiel à la confiance des citoyens. On ne choisit pas le jour de son arrêt cardiaque.

Néanmoins, si ces attaques sont plus anciennes dans le secteur privé, les entreprises font face à une évolution de leurs enjeux de cybersécurité. Le télétravail constitue une nouvelle faille de vulnérabilité pour leurs données. Les normes juridiques internationales sur la protection des données personnelles peuvent inciter certaines entreprises à cacher les cyberattaques qu'elles subissent. Enfin, la menace est devenue assez importante pour que les agences de notations boursières prennent en compte le risque de cybersécurité qu'encours une entreprise dans leurs évaluations.

Pour répondre à ces enjeux de souveraineté numérique l'État français base sa stratégie sur deux points essentiels : la constitution d'un organisme centralisé sous l'autorité du premier ministre - l'ANSSI - et la mobilisation du droit.

L'ANSSI tient un rôle central d'édiction des règles de sécurité numérique à appliquer et de surveillance de leur application, de veille des données sensibles et de formation et de prévention des citoyens, des entreprises et des administrations. Elle assure également une surveillance poussée des OIV, enjeu stratégique d'ampleur. Elle constitue une organisme stratégique d'avenir dans un monde où la standardisation numérique ne cesse de s'accroître.
Le droit, en France et à l'international a vu défiler, depuis le début des années 2000, un enchaînement de normes juridiques visant à favoriser la sécurité numérique des entreprises et du secteur public. Symptôme d'une prise de conscience mondial, ce sursaut, au-delà d'une adaptation à la transition numérique, représente essentiellement une réaction à l'ampleur que prend la cyber insécurité au niveau mondial.

Malgré ces réponses, le manque de compétences et de main d'œuvre dans le secteur numérique et de la sécurité numérique constitue une faille de vulnérabilité pour la protection de nos données et la stratégie de l'État français.

Ouverture : vers un numérique intelligent, quantique et dépendant

L'une des principales problématiques pour le secteur du privé est d'adopter une position de réaction. Les entreprises anticipent déjà l'impact de l'IA, qui a déjà en outre la capacité d'évaluer des failles de sécurité de système, et l'apparition de l'ordinateur quantique, qui peut rendre obsolète l'utilisation des mots de passe.

Les pouvoirs publics ont augmenté le budget en 2023 en faveur de la cybersécurité, appelant à la création de 1 500 « cyber patrouilleurs » et créant une nouvelle agence et augmentant les moyens des agences existantes.

Malgré ces prises de position, il demeure une problématique essentielle : le retard de la France, mais plus généralement de l'Europe dans la production de technologies numériques. D'une part l'Union européenne n'affiche à ce jour aucune cohésion sur le sujet de cyberdéfense. Les États ne se coordonnent pas pleinement dans la fabrication et la planification d'une défense commune de leurs entreprises. D'autre part, la France et l'Union européenne accusent un retard de développement de leur capacité cyber et d'outil numérique stratégique face aux autres pôles de puissances puissances. Les leaders dans le domaine sont les Etats Unis, avec le populaire ChatGPT. En 2021, un rapport britannique évaluait l'avance des États-Unis sur la Chine d'au moins 10 ans. Si les Etats-Unis sont nos alliés, il demeure que leurs pratiques de négociation useront de nos dépendances, non seulement sur les technologies que nous leur empruntons (cloud, IA pour ne citer que les plus critiques), mais également des ressources stratégiques dont ils ont le contrôle comme les microprocesseurs, éléments essentiels pour nos entreprises. Quand bien même nous trouvons les matières premières pour produire à grande échelle ces composants (principalement issu de Taiwan, allié stratégique des US), il nous faudrait des années et des milliards d'euros pour atteindre leur technologie logiciel d'aujourd'hui . Les politiques publiques semblent contraintes à adopter une posture de régulation, faute d'être en capacité de combler ce retard et sortir de cette dépendance.

Communication gouvernementale

- Contrat Stratégique de la Filière : Industries de sécurité 2020 - 2022, Conseil National de l'Industrie, Consulté le 21 mars 2023
- La cybersécurité des entreprises : Prévenir et guérir : quels remèdes contre les cyber virus ? Sénat (n° 678 (2020-2021)), Délégation aux Entreprises du Sénat, Consulté le 21 mars 2023
- Métiers en 2030 : Quels métiers en 2030 ?, France Stratégie, Consulté le 21 mars 2023

Normes juridiques

- Règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE
- Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union
- Livre blanc sur la défense et la sécurité nationale du 29 avril 2013
- Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.
- Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité
- Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information »
- Décret n° 2011-1425 du 2 novembre 2011 portant application de l'article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation
- Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation
- Circulaire interministérielle du 7 novembre 2012 de mise en œuvre du dispositif de protection du potentiel scientifique et technique de la nation.

Bibliographie

Articles scientifiques

- Quelle responsabilité en matière de sécurité informatique ?, 8 avril 2002, Avocat Lille, jurisexpert.
- La stratégie française de cybersécurité : une complémentarité Public/Privé essentielle., 29 janvier 2019, Auteurs J, Opérationnels – Soutien, Logistique, Défense, Sécurité.
- Leveraging machine learning to find security vulnerabilities, 15 mars 2022 The GitHub Blog, Gazit, T.
- Budget 2023 : la France augmente ses investissements en cybersécurité, 27 septembre 2022, Siècle Digital, Crimino V.
- Choking off China's Access to the Future of AI., 20 décembre 2022 Center For Strategic & International Studies, Allen, G. C.
- GERMAIN Grégoire et MASSART Paul (2017), "Souveraineté numérique", Etudes, vol.10, France, p.45-58.

Articles de presse

- Du renfort sur le front de la sécurité informatique, 15 novembre 2006, LeMondeInformatique.
- Piratage de données : Uber mise à l'amende en France par la Cnil, 20 décembre 2018, Les Echos
- Comment hacker le plus grand oléoduc des Etats-Unis., 23 mai 2021, France Culture.
- Cyber puissance : une étude britannique montre que les Chinois ont un retard de 10 ans sur les Etats-Unis. Quid de l'Europe ? 4 juillet 2021, Atlantico, DeCloquement F.
- « En matière de cyberdéfense, la communauté européenne n'existe pas », 11 novembre 2022, LEFIGARO, Planchon R.
- Simulations de crise et cyberdéfense se multiplient en France. (S. d.). LeMondeInformatique. https://www.lemondeinformatique.fr/actualites/lire-simulations-de-crise-et-cyberdefense-se-multiplient-en-france-88778.html

Sitographie

- Vox. (2023, 7 février). Why China is losing the microchip war [Vidéo]. YouTube. https://www.youtube.com/watch?v=Uh4QGey2zTk

- Contributeurs aux projets Wikimedia. (2022, 27 septembre). Andromède (cloud). https://fr.wikipedia.org/wiki/Androm%C3%A8de_(cloud)

- Retour sur les grandes cyberattaques en France en 2022 : quelles résolutions pour 2023 ? (S. d.). Portail de l'IE. https://portail-ie.fr/analysis/4247/retour-sur-les-grandes-cyberattaques-en-france-en-2022-quelles-resolutions-pour-2023

Conférences

- Intervention de M. Guillaume Poupard, 7 octobre 2022, Université de Nancy