Lettre mensuelle – **Février 2021 – Disponible sur omc.ceis.eu**

Table des matières

ANALYSES (1/2)

SEMI-CONDUCTEURS : UN ENJEU STRATÉGIQUE POUR L'INDÉPENDANCE TECHNOLOGIQUE EUROPÉENNE

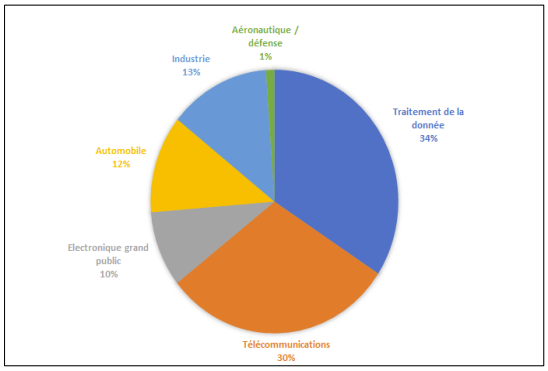
La pénurie de composants à laquelle font face différents secteurs industriels (télécommunication, automobile, consoles vidéo…) met en exergue la forte dépendance européenne en la matière. Une dépendance matérielle, résultat de la stratégie du « *fabless* » qui a prévalu tant aux Etats-Unis qu'en Europe pendant très longtemps, et qui devient **un risque stratégique majeur** dans le contexte actuel de guerre technologique et commerciale entre la Chine et les Etats-Unis.

1. Les raisons d'une pénurie

La pénurie actuelle résulte d'abord du **choc occasionné par la pandémie sur la chaîne d'approvisionnement** en semi-conducteurs : chute brutale des commandes en mars 2020, puis reprise tout aussi soudaine, et non anticipée par les producteurs. Et ce alors même que la chaîne est relativement rigide. Les délais de production (4 à 6 mois) sont en effet incompressibles et l'élasticité de la production par rapport à la demande est faible : il faut des investissements massifs (250 millions $ par machine), et au moins un an, pour développer de nouvelles capacités de production. La réorientation brutale des commandes d'un segment vers l'autre, en particulier vers l'électronique grand public et les télécommunications, lors de la crise, a ainsi accéléré le phénomène en épuisant les stocks disponibles.

Cette pénurie s'explique aussi par la **dépendance croissante de l'industrie aux composants électroniques**, corollaire de la transformation numérique de l'ensemble des secteurs d'activité. Le marché mondial des semi-conducteurs devrait s'élever à 514 milliards $ par an en 2021[1], en progression de 45% par rapport à 2016.

Répartition du marché mondial des semi-conducteurs (source : Gartner/Deloitte)



Cette pénurie a enfin été aggravée par la **concentration des capacités de production et la spécialisation** des acteurs sur la chaîne de valeur. De façon globale, les 3 premiers acteurs mondiaux, l'Américain Intel (65,8 milliards $ CA en 2019), le Sud-Coréen Samsung (52,2 milliards $ CA en 2019) et le Taïwanais TSMC[2] (35,8

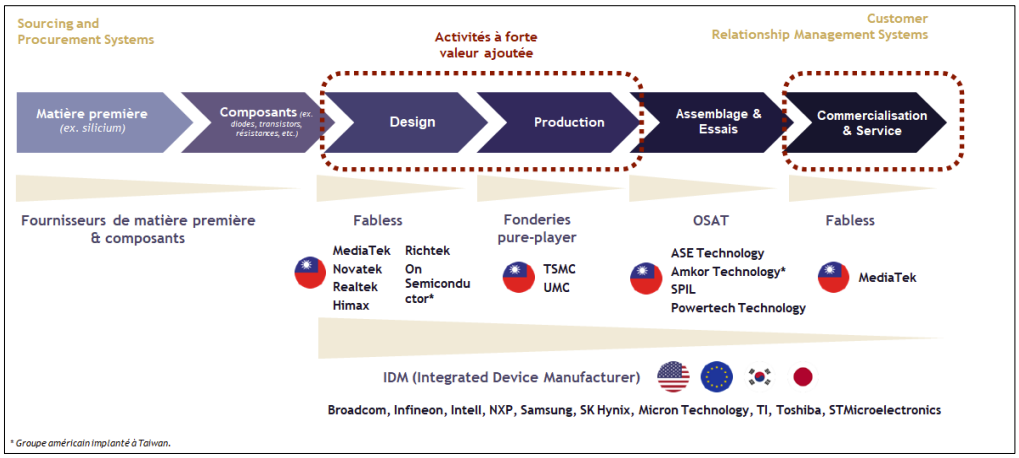
[1] Source : Gartner/Deloitte [en ligne]

[2] Taiwan Semiconductor Manufacturing Company

milliards $ CA en 2019) représentent en effet 30% du marché mondial[3]. Mais une analyse plus précise de la chaîne de valeur montre surtout la **nette domination de Taïwan sur le segment "production" ou "fonderie"** de la chaîne, avec les leaders TSMC, UMC[4] et GlobalFoundries. En 2020, le pays a ainsi capté 75,7% du marché mondial des fonderies (soit 85 milliards $) et, à l'étape suivante de la chaîne de valeur, 56,7% de celui des OSAT (OutSourced Assemblage & Tests)[5].

Une position dominante qui résulte d'une part d'une politique industrielle très volontariste initiée dès la fin des années 50 et largement facilitée par les stratégies « *fabless* » très en vogue aux Etats-Unis et en Europe dans les 1990-2000, et d'autre part de la globalisation des chaînes de valeur. Le secteur taïwanais des semi-conducteurs compte ainsi plus de 300 entreprises et emploie 225 000 personnes, dont 43 000 dans la R&D, pour un budget R&D cumulé de 8,5 milliards de dollars en 2020[6]. Mais surtout, il est le seul en lice pour graver dès 2022 des composants en 3 nanomètres, là où les Chinois SMIC ou Huawei ne gravent pour l'instant qu'à 14 nm, et où Intel se contente de 10 nm.

Chaîne de valeur industrielle « semi-conducteurs » (source : CEIS)



2. L'Europe face au risque d'une dépendance systémique

Au-delà de la pénurie, c'est le risque de **dépendance systémique** qu'elle a mis en lumière qui mérite l'attention. Cette dépendance concerne en effet la plupart des grands pays consommateurs de semi-conducteurs. La Chine ne produit ainsi que 16% à 30% des puces dont elle a besoin, ce qui l'a contraint à importer pour 350 milliards de semi-conducteurs en 2020[7]. Même chose pour les Etats-Unis, dont la position semble en apparence solide avec 47% des parts de marché mondiales sur l'ensemble du secteur, mais qui a progressivement délaissé la fabrication pour se concentrer sur l'amont ou l'aval de la chaîne. Seuls 12% des semi-conducteurs mondiaux sont ainsi produits aux Etats-Unis, contre plus de 30% en 1990. Le géant américain Intel sous-traite ainsi à TSMC la quasi-totalité de ses besoins. Constat identique, enfin, pour l'Europe, et pour la France dont la balance commerciale avec Taïwan, historiquement négative, s'élevait en 2019 à 3,2 milliards d'importations (dont plus de 2 milliards concernent l'électronique) contre 1,7 milliard

[3] Source : Gartner/Institut Montaigne [en ligne]
[4] United Microelectronics Corp
[5] Source : Bureau Français de Taipei - service économique, Ministère de l'Economie, des Finances et du Trésor [en ligne]
[6] *Ibid*
[7] Source : Banque Nationale du Canada [en ligne]

d'exportations. Ce déficit, qui a explosé depuis 2017, devrait même encore s'accroître en raison de la demande croissante d'équipements de télécommunication et de produits numériques.

Ces dépendances, naturelles dans une économie globalisée, ne seraient finalement pas si graves si elles n'intervenaient pas dans un **contexte géopolitique troublé** marqué par des tensions croissantes entre la Chine et les Etats-Unis. Pour conserver un avantage compétitif sur les technologies numériques, en particulier sur la 5G, les Etats-Unis cherchent en effet par tous les moyens à bloquer les avancées chinoises, et utilisent les semi-conducteurs comme un levier de pression sur l'Empire du milieu. Ils ont ainsi soumis TSMC à de fortes pressions pour qu'ils interrompent leurs relations commerciales avec leurs clients chinois et pour qu'ils implantent une partie de leur production sur le territoire américain. Dans le même temps, les Etats-Unis ont placé SMIC, principal producteur chinois de puces électroniques, sur la liste noire d'exportation, limitant l'accès de l'entreprise aux technologies américaines en raison de ses liens présumés avec l'Armée chinoise.

Cette stratégie de coercition américaine a cependant **de nombreux effets de bord**. A court terme, elle n'a fait qu'amplifier le choc sur la filière semi-conducteur : à l'image de Huawei, nombre d'entreprises chinoises se sont précipitées sur les stocks existants de composants pour se prémunir contre toute rupture d'approvisionnement. Elles devraient d'ailleurs être imitées en cela par des entreprises occidentales. TSMC a en outre relevé ses prix de 10 à 15% à l'automne dernier et envisagerait de les augmenter de nouveau[8]. Au plan géopolitique, elle ne fait qu'aiguiser l'appétit de l'ogre chinois envers Taïwan. Au plan industriel, enfin, elle pousse la Chine à s'autonomiser en matière de semi-conducteurs et à combler son retard technologique en renforçant ses propres capacités. Dans le cadre de son plan "Made in China 2025" (avec un budget de 1 400 milliards $ consacrés aux technologies), le pays redouble ainsi d'efforts pour réduire sa dépendance et investit massivement dans le secteur. Objectif : produire en 2025 70% des puces dont elle a besoin pour son industrie. Outre les pressions exercées sur TSMC pour qu'il augmente sa production sur le continent, la Chine débauche aussi à tour de bras des ingénieurs spécialisés en Corée du Sud et à Taïwan. Fin 2019, plus de 3 000 ingénieurs ont ainsi été débauchés dans les 2 pays[9]. Le chinois SMIC a ainsi un projet d'usine à 12 milliards de dollars pour viser à terme la production de composants de 7 nm et moins, et trouver une alternative à ASML, entreprise néerlandaise qui est aujourd'hui la seule au monde à produire des machines permettant de graver en dessous de 10 nm avec la technologie de lithographie EUV (extreme ultraviolet).

Pour l'Europe et la France, le risque n'est donc pas tant dans ces dépendances que dans l'exploitation de cette dépendance dans le cadre de **stratégies de coercition** susceptibles d'être menées par la Chine ou les Etats-Unis, lesquelles peuvent affecter des secteurs stratégiques, comme l'aéronautique, le spatial ou l'électronique de défense. Dans le domaine militaire, même si l'extrême miniaturisation n'est pour le moment pas nécessaire pour les systèmes d'armes et de control-command, "*la confiance et la spécificité du design de certains circuits intégrés restent des éléments clés*", souligne l'Institut Montaigne[10]. La numérisation des opérations militaires va en outre changer progressivement la donne. Ce serait d'ailleurs en partie la raison pour laquelle l'administration Trump a fait pression pour que TSMC s'installe en Arizona. "*La continuité des activités de fabrication électrique et électronique est essentielle au fonctionnement économique de notre pays, indispensable à l'approvisionnement de secteurs critiques tels que la production d'appareils médicaux, les télécommunications, les infrastructures et services numériques essentiels, l'industrie de défense, la fabrication d'équipements pour les réseaux énergétiques, la logistique, les transports, l'industrie*", écrivaient Bruno Le

[8] Ibid

[9] Source : Asia Nikkei [en ligne].

[10] Source : The weak links in China's drive for semiconductors, Institut Montaigne [en ligne]

Maire, ministre de l'Economie et des Finances, et la secrétaire d'Etat, Agnès Pannier-Runacher, dans une lettre adressée aux syndicats professionnels de la filière, le 27 mars 2020[11].

3. Une stratégie industrielle dédiée pour sortir de l'impasse ?

Pour réduire cette dépendance stratégique et ne pas être freinée dans le développement d'usages liés à la 5G, aux voitures connectées ou au calcul haute performance, l'Europe doit donc rapidement adopter des mesures volontaristes **combinant diversification des approvisionnements, aide à l'installation d'industriels étrangers sur son territoire, soutien au développement de la filière locale et contrôle des investissements étrangers**. Comme le note l'entrepreneur et chercheur autrichien Hermann Hauser dans le Monde[12] à propos du projet de rachat du spécialiste britannique du design des puces électronique ARM par l'Américain Nvidia, *"tout pays ou groupe de pays doit désormais se poser trois questions : Possédons-nous les technologies essentielles ? Si ce n'est pas le cas, avons-nous accès à ces technologies par l'intermédiaire de pays indépendants ? Si là encore ce n'est pas le cas, disposons-nous d'un accès garanti, libre et à long terme (plus de cinq ans) à ces technologies par l'intermédiaire de fournisseurs monopolistiques ou oligopolistiques d'un pays particulier (généralement les Etats-Unis ou la Chine) ? Si la réponse à ces trois questions est négative, nous nous exposons à une coercition technologique non moins rigoureuse que la coercition militaire d'antan."*

Sur le front de la diversification, des alternatives aux fournisseurs taïwanais existent en Asie du Sud-Est (Malaisie et Corée du Sud) ou aux Etats-Unis, en particulier sur les produits finis que sont les circuits programmables (FGPA). **La réglementation ITAR,** qui permet aux Etats-Unis de bloquer les exportations de produits intégrant des technologies américaines, **reste cependant un obstacle majeur**, en particulier en matière de défense. Le développement sur son territoire d'activités non seulement de conception et d'intégration mais aussi de fabrication des composants, à l'opposé du modèle « *fabless* » qui a longtemps prévalu en Occident, est donc indispensable. Ce qui suppose des **investissements massifs en R&D**, surtout pour développer des chaînes de fabrication sur les composants de dernière génération (taille inférieure à 7 nm). A titre de comparaison, TSMC et Samsung envisagent d'investir respectivement 21 et 26 milliards d'euros en R&D en 2021[13]. Restent enfin les mesures incitant des industriels étrangers à s'installer sur le territoire européen, à l'image des projets de TSMC (12 milliards de dollars) ou de Samsung (15 milliards de dollars) aux Etats-Unis, où le projet de loi baptisé CHIPS for America Act, présenté en 2020 et toujours en cours de discussion, prévoit de distribuer 25 milliards $ de fonds fédéraux pour soutenir le mouvement[14].

Consciente des enjeux, l'Union européenne s'est de son côté engagée en décembre 2020 dans le cadre du plan de relance, à soutenir l'industrie européenne des semiconducteurs. Objectif : **produire à terme au moins 20% des circuits intégrés dans le monde**. Un plan d'investissement ambitieux, qui pourrait atteindre 30 milliards d'euros, devrait ainsi être annoncé d'ici la fin du premier trimestre 2021. "*Sans une capacité européenne autonome en matière de microélectronique, il n'y aura pas de souveraineté numérique européenne",* souligne Thierry Breton, commissaire européen[15]. Des contacts auraient déjà été pris pour nouer des partenariats avec les fonderies taïwanaises et sud-coréennes, dans le but de doter le Vieux continent de capacités inférieures à 10 nm, voire de 2 nm. Côté français, le plan Nano 2022, initié par Bruno Le Maire en

[11] Source : L'Usine Nouvelle [en ligne]
[12] Source : Le Monde, 23 février 2021 [en ligne]
[13] Source : l'Usine Nouvelle [en ligne]
[14] Source : [en ligne]
[15] Source : Siècle digital [en ligne]

2018, a permis d'investir plus de 1 milliard d'euros dans des capacités industrielles nouvelles. Un plan dont bénéficie notamment le champion franco-italien STMicroElectronics et une dizaine d'autres projets portant non seulement sur la conception des puces, mais aussi la fonderie.

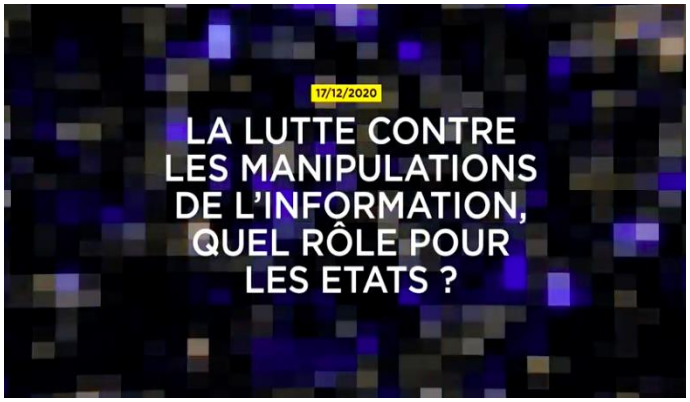
Face au duopole stratégique Chine-Etats-Unis, Hermann Hauser[16] rappelle que l'Europe devrait en effet « *aider la Chine à développer sa propre industrie des semi-conducteurs en nous fondant sur le principe de réciprocité. En échange d'une cession de propriété intellectuelle et de la fourniture d'une assistance technique, la Chine pourrait s'engager à construire des usines en Europe pour répondre aux besoins des marchés européens et partager la propriété intellectuelle qui sera générée de manière conjointe. Cette stratégie a très bien fonctionné avec l'industrie automobile japonaise* ». De fait, la Chine aligne aujourd'hui des moyens supérieurs à ceux des Etats-Unis, tant au plan financier qu'en termes de compétences, et pourrait bien à terme s'affranchir rapidement de sa dépendance aux Etats-Unis en matière de propriété intellectuelle sur les semi-conducteurs. L'indépendance européenne pourrait donc d'abord passer par un **"équilibrage de sa dépendance"** pour lui éviter d'être prise en otage dans la guerre technologique sino-américaine. Dans ces conditions, il n'est pas certain que le partenariat transatlantique renforcé dans le domaine des semiconducteurs auquel appelle l'Institut Montaigne dans un récent rapport[17] ne suffise à rétablir la confiance de l'industrie européenne après les années Trump...

ANALYSES (2/2)

LA LUTTE CONTRE LES MANIPULATIONS DE L'INFORMATION : QUEL RÔLE POUR L'ÉTAT ?

*Cet article est une synthèse du troisième module de l'évènement Cyberdéfense et Stratégie, organisé entre les 15 et 17 décembre 2020 par CEIS au profit du Commandement de la cyberdéfense du ministère des Armées. Consacré à la thématique « **Fake news et manipulations de l'information : la démocratie en péril ?** », cet atelier a eu lieu dans un format webinar dont le replay est disponible ici.*

*Les échanges ont réuni les participants suivants (par ordre alphabétique) : **Sébastien Bombal** (chef du pôle Stratégie du Commandement de la cyberdéfense), **Nicolas Cellupica** (avocat au barreau de Paris), **Jean-Louis Gergorin** (co-auteur de « Cyber la guerre permanente »), **Bruno Studer** (député du Bas-Rhin), le **général de division aérienne Didier Tisseyre** (Commandant de la cyberdéfense).*



[16] Ibid

[17] The weak links in China's Drive for Semiconductors, Institut Montaigne [en ligne]

Les « fake news » et les manipulations de l'information inondent désormais nos réseaux et déstabilisent nos démocraties : elles sapent la confiance des lecteurs, donc des citoyens, elles renforcent la polarisation des opinions, et elles attisent les divisions de la société. S'il ne s'agit pas d'un phénomène récent, son regain s'explique par plusieurs facteurs :

- L'explosion des réseaux sociaux et les phénomènes de rétrécissement de l'information qui génèrent des bulles filtrantes ;
- La crise des médias traditionnels et le développement d'une économie de l'attention qui favorisent une culture de la « fast news » ;
- La crise de la connaissance et l'avènement de l'ère de la post-vérité qui se base désormais sur des interprétations et non des faits ;
- Les stratégies de guerre hybride qui s'appuient sur des capacités militaires mais aussi sur des milices ou des proxys, qui utilisent des moyens d'action plus ou moins légaux et qui jouent avec les seuils.

Le contexte géopolitique actuel constitue également un terreau favorable au développement des manipulations de l'information. Chaque acteur, tant au niveau local que régional ou international, essaie ainsi de se positionner dans l'espace informationnel et d'y faire passer des messages, d'agir et d'influencer les auditoires. En France, des réflexions sont aujourd'hui menées au niveau interministériel pour :

- Identifier la nature de la menace informationnelle ;
- Identifier la manière dont elle se manifeste ;
- Identifier les acteurs et auteurs des attaques informationnelles ;
- Concevoir la réponse la plus adéquate.

Ces réflexions doivent prendre en compte le droit international, que la France s'engage à respecter dans son action, mais aussi un certain nombre de grands principes de comportement des États dans le cyberespace auxquels elle adhère. Ces exigences rendent peut-être encore plus complexe la réponse qu'elle peut apporter à des menaces grandissantes et à des attaquants de plus en plus audacieux.

Comment dans ce contexte, l'État peut-il appréhender les manipulations de l'information ? Quel rôle peut-il jouer et quelles réponses peut-il apporter ? Peut-il et doit-il agir seul ? De quel partenaire s'entourer sur les plans national et international, public et privé ?

1. La lutte contre les manipulations d'information : quelles priorités politiques ?

Les manipulations de l'information sont devenues une priorité politique à tous les niveaux. Que ce soit au niveau national, européen ou international, des mesures ou des initiatives se multiplient et se sont accélérées depuis les campagnes de fake news qui ont marquées les diverses échéances électorales de 2016, et plus encore depuis le début de la pandémie Covid-19. En France, la loi contre la manipulation de l'information, dite "loi anti-fake news", a été validée par le Conseil constitutionnel dès décembre 2018. Cette dernière vise à lutter contre la diffusion massive et rapide de « fausses nouvelles » ou « fake news » via les outils numériques, en période électorale. Aux États-Unis, Joe Biden a déclaré lors de son discours d'investiture : « *Nous sommes confrontés à une attaque contre la démocratie et la vérité*[18] ». De son côté, la Commission européenne s'est également saisie de ces sujets depuis le début de la présidence d'Ursula von der Leyen. Le numérique, avec la cybersécurité et la lutte contre les « fake news », font aujourd'hui partie des piliers stratégiques de la

[18] « Inaugural Address by President Joseph R. Biden, Jr. », White House [En ligne], 20 janvier 2021.

Commission. Quant à l'ONU, elle a lancé l'opération Verified, qui vise à lutter contre la désinformation sur le Covid-19 en permettant le partage d'informations entre les parties prenantes[19]. L'OCDE a également publié une série de grandes mesures que les pouvoirs publics et les plateformes peuvent appliquer pour contrer la désinformation sur le Covid-19[20].

La lutte contre les manipulations de l'information s'est donc ouverte sur plusieurs fronts, qu'il s'agisse de combattre la fabrique des « fake news », leur diffusion ou leur propagation.

Reprendre l'initiative face aux plateformes

Dans la lutte contre la désinformation, les plateformes telles que Facebook, Google, Instagram, Twitter, YouTube ou encore Wikipédia, sont régulièrement accusées au mieux de ne pas mettre en œuvre tous les moyens possibles pour lutter contre les fausses informations, au pire de contribuer à leur fabrique et à leur diffusion.

Pour tenter de lutter contre ce phénomène en dehors des périodes électorales, la loi française de 2018 contre la manipulation de l'information crée un devoir de coopération des plateformes, et confère au Conseil supérieur de l'audiovisuel (CSA) de nouvelles compétences qui étendent son champ d'action de la télévision à l'Internet. Ainsi, le CSA peut désormais adresser aux plateformes des « recommandations » qui ont pour objectif d'améliorer la lutte contre la diffusion de « fake news ». Il peut aussi contrôler les mesures mises en œuvre par les plateformes, qui doivent par conséquent mettre en place un dispositif facilement accessible et visible afin que les utilisateurs puissent signaler des informations douteuses. Elles sont également invitées à mettre en œuvre des mesures complémentaires et disposent d'une certaine liberté en la matière, sur des sujets dont le législateur a toutefois donné quelques exemples : transparence des algorithmes, lutte contre les comptes propageant des « fake news », éducation aux médias etc. Enfin, le CSA peut également empêcher, suspendre ou interrompre la diffusion de services de télévision contrôlés par un État étranger ou sous l'influence de cet État, et portant atteinte aux intérêts fondamentaux de la nation[21].

Quant à la Commission européenne, elle appelle aussi de ses vœux, depuis quelques mois déjà, à des plateformes plus responsables et transparentes. Les commissaires européens Margrethe Vestager et Thierry Breton ont dans ce contexte présenté le Digital Services Act et le Digital Market Act, deux textes très attendus, notamment par la France car ils permettront de limiter la puissance des plateformes telles que Google, Facebook ou Amazon. Ces textes s'appliqueront aux services numériques y compris les médias sociaux et les places de marché en ligne. Ils doteront l'UE d'un cadre de responsabilité des plateformes du numérique :

- Dimension sociétale : lutte contre la dissémination des contenus illicites ou préjudiciables ;
- Dimension économique et concurrentielle : garantir que les marchés numériques restent innovants et ouverts à la concurrence, et que les relations commerciales entre les grands acteurs et leurs partenaires commerciaux y demeurent équilibrées et loyales[22].

Bruno Studer rappelle que les textes européens permettent déjà d'infliger des amendes à hauteur de 6% du chiffre d'affaires global des plateformes, si puissantes que plusieurs sont même dotés d'« ambassadeurs » auprès de certains États.

---

[19] « L'ONU lance l'initiative « Vérifié » pour lutter contre la désinformation sur la Covid-19 », ONU [En ligne], 21 mai 2020
[20] « Combattre la désinformation sur le COVID-19 sur les plateformes en ligne », OCDE [En ligne], 3 juillet 2020
[21] « Contre la manipulation de l'information », Gouvernement [En ligne], 10 septembre 2020
[22] « Grandes plateformes du numérique : vers le Digital Services Act et Digital Markets Act », Ministère de l'Économie, des Finances et de la Relance [En ligne], 16 décembre 2020

Soutenir le journalisme et promouvoir une information de qualité

Face à des plateformes difficiles à contrôler, qui diffusent des contenus dont la véracité et la fiabilité ne sont pas systématiquement établies, il est essentiel de permettre aux médias professionnels de continuer d'exister et de diffuser une information de qualité. L'État a donc un rôle essentiel à jouer pour soutenir la profession et le secteur du journalisme, que ce soit par la contribution à l'audiovisuel public, les aides à la presse prévues par le plan de relance, les aides au portage, ou encore du crédit d'impôt pour l'abonnement, destinées à fidéliser les lecteurs à des médias fiables et qualitatifs.

Soutenir le journalisme français doit aussi permettre à la France de protéger ses intérêts dans des régions ou des pays ou sa présence et son influence sont concurrencées par les narratifs diffusés par des médias soutenus par des puissances étrangères, comme Russia Today ou Chine Nouvelle. Lutter contre la déstabilisation informationnelle passe donc aussi par le soutien à journalisme fiable et qualitatif.

Retrouvez ici et ici les interventions de Bruno Studer :

« *La meilleure porte d'entrée dans une culture c'est la langue et si les gens aujourd'hui n'ont plus les moyens de maîtriser la langue française, ils ne maîtriseront pas l'information qui est derrière et se contenteront du son et de l'image* » – Bruno Studer

Développer et professionnaliser l'éducation aux fake news

Au cœur des critiques contre les plateformes : leurs algorithmes dits « de recommandations », qui enferment les utilisateurs dans des « bulles » informationnelles et intellectuelles, et propagent sans les vérifier des contenus dont la véracité est rarement établie. Pour lutter contre ce phénomène qui touche d'abord les plus jeunes, plus exposés et moins armés donc plus vulnérables, tout l'enjeu consiste à leur donner les outils permettant d'analyser les informations auxquelles ils sont confrontés. Un rôle de choix pour les professionnels de l'Éducation nationale, qui doivent donc d'abord monter en connaissance sur l'environnement numérique dans lequel évolue la jeunesse, à l'heure où les médias sociaux ont fait exploser le triptyque famille-école-réseaux de sociabilité. Les professionnels de l'Éducation nationale doivent ensuite monter en compétences sur les mécanismes et les outils de déconstruction de ces contenus imposés par les algorithmes.

Les sciences cognitives sont à ce titre essentielles, d'abord pour comprendre le fonctionnement du cerveau et l'impact de l'enfermement algorithmique chez les utilisateurs, en particulier chez les plus jeunes, et ensuite par conséquent, pour aider à concevoir les outils permettant d'y faire face. L'objectif est bien de développer, chez tous les utilisateurs, des réflexes de vérification et une méfiance raisonnée et constructive à l'endroit de

certains narratifs. « *Il faut arriver à faire du premier avril un jour de tous les jours* » résume Bruno Studer. L'éducation aux médias et à l'information doit ainsi être intégrée aux cursus scolaires.

Si l'école a un rôle central à jouer dans la lutte contre les manipulations de l'information, il demeure que les *fake news* et autres théories du complot touchent toutes les générations, et se diffusent également auprès de personnes éduquées. Des efforts constants de sensibilisation doivent être menés, tant auprès du grand public que dans les milieux professionnels.

Retrouvez ici et ici les interventions de Sébastien Bombal :

2. La lutte contre les manipulations d'information : une réponse qui ne peut être que collective

Le champ informationnel, dans lequel naissent et se propagent les manipulations de l'information, ne connaît pas de frontières. Et les infosphères, c'est-à-dire les environnements numériques dans lesquels les informations transitent, sont poreuses. Sur Internet, les contenus et les narratifs, manipulés ou pas, se diffusent de façon naturelle et spontanée en passant de compte en compte, de page en page, et de site de mésinformation en site de mésinformation. Les communautés linguistiques, comme la « francophonie », contribuent à accélérer ce phénomène : elles favorisent la diffusion de contenus entre des audiences partageant la même langue mais pas la même localisation géographique. La lutte contre les manipulations de l'information doit faire l'objet d'une réponse globale, concertée, collaborative, tant sur le plan national qu'international, et associer les acteurs privés.

L'action interministérielle ou la complémentarité

« La réponse que peut apporter la France ne peut-être qu'interministérielle, et ne peut être que globale » – Général de division aérienne Didier Tisseyre (Commandant de la cyberdéfense)

En matière de lutte contre les *fake news* comme dans beaucoup d'autres domaines, "l'union fait la force". Combattre un phénomène protéiforme tel que les manipulations de l'information nécessite des compétences, des ressources et des capacités aussi variées que les formes qu'elles peuvent prendre. Les armées, dont les activités sont strictement encadrées par des règles d'engagement, ne peuvent agir seules. Elles n'en n'ont ni les prérogatives, ni les moyens, à la fois en termes de compréhension et de caractérisation du phénomène, qu'en termes d'actions et de réponses concrètes. Le ministère des Armées, avec le Commandement de la cyberdéfense plus particulièrement, travaille ainsi en étroite collaboration avec tous les acteurs publics concernés (ANSSI, ministère de l'Intérieur et ministère de l'Europe et des Affaires étrangères) pour apporter

une réponse globale et collective qui lui permette de parler d'une seule voix face à ses interlocuteurs, privés comme internationaux. Tout l'enjeu est alors de coordonner, au niveau interministériel, les responsabilités et les capacités respectives des parties prenantes pour que la réponse soit aussi efficace et rapide que l'exige ce phénomène qui ne cesse de croître.

Une coopération internationale sur mesure

Avec les partenaires internationaux, la coopération bilatérale en matière de lutte contre les manipulations de l'information ne peut être envisagée qu'au cas par cas : elle dépend à la fois de nos relations avec le(s) pays concerné(s), du contexte dans lequel elles interviennent, et du niveau et du type de l'information considérée. Car la première difficulté est en effet celle de la définition et de l'interprétation des narratifs concernés. Si certains comme la pédopornographie font aisément l'objet d'une qualification commune, d'autres en revanche sont plus ambigus. C'est le cas par exemple de la « subversion » et de la « diffamation » dont la définition, la perception et les réponses à y apporter varient d'un pays à l'autre. La compréhension de l'infosphère locale et de ses caisses de résonance est donc à la fois l'enjeu et le pré-requis de toute coopération internationale dans la lutte contre les manipulations de l'information. C'est cette compréhension commune du phénomène, de l'impact qu'il peut avoir et des enjeux qu'ils représentent, qui permet de concevoir collectivement une réponse efficace.

L'indispensable coopération public/privé

Si les plateformes sont à bien des égards le nœud du problème, elles font aussi partie de la solution. Une partie de la réponse aux manipulations de l'information passe en effet aussi par le contrôle de ces contenus sur les réseaux sociaux, dont le législateur peut, sous certaines conditions, exiger le retrait ou la suppression voire la fermeture du compte associé. Une coopération publique/privée, à la fois avec les plateformes, les médias sociaux, les hébergeurs et les fournisseurs d'accès internet est donc indispensable.

Mais cette nécessaire coopération - ou du moins, dialogue, avec les plateformes, ne peut être mené qu'au niveau national. La France, ni aucun autre pays, ne peut s'imposer seul face à elles. L'action menée à l'échelle européenne contre ces plateformes qui diffusent les manipulations de l'information, est sans doute à ce jour, la plus proactive.

Le dispositif législatif français

« Dès lors qu'un avocat intervient, c'est que le mal est fait et que la « fake news » a circulé » – Maître Nicolas Cellupica

En France, la réponse judiciaire aux manipulations de l'information est particulièrement lente, et n'est jamais à la hauteur du dommage causé. Elle repose de fait sur assez peu d'outils législatifs, qui sont plus ou moins efficaces :

- La Loi de 1881, qui pose la liberté de la presse et sanctionne tout ce qui vient la réduire, à commencer par la « diffamation » : c'est sur ce terrain que le Laboratoire Pasteur a fait condamner l'internaute ayant diffusé la « fake news » concernant la propagation du Covid-19. C'est donc sur le terrain d'une loi du 19ème siècle. L'infraction d'« injure » peut aussi être invoquée dans le cadre de cette loi.
- La Loi de 2018 sur la manipulation de l'information portée par le Député Studer, qui ne s'applique toutefois qu'en période électorale pour des élections nationales. Cette loi permet notamment d'introduire une procédure en urgence permettant d'exiger des hébergeurs, dans certaines conditions très restrictives, la suppression de certains contenus.
- La loi du 21/06/2004 pour la confiance en l'économie numérique, qui permet d'introduire très rapidement des procédures permettant de lever l'anonymat sur certaines publications, en contraignant les hébergeurs à fournir les renseignements sur les comptes litigieux et dans certains cas, à supprimer les contenus concernés avant toute procédure contentieuse. Ce dispositif est aujourd'hui relativement efficace, les hébergeurs coopérant beaucoup plus facilement et spontanément que ce n'était le cas auparavant – mais surtout cependant si les hébergeurs sont Européens. Les hébergeurs américains se sont montrés plus réticents, et exigent pour beaucoup une américaine pour s'exécuter. Un argument supplémentaire en faveur du renforcement du dispositif législatif et règlementaire dédié au niveau européen.

Retrouvez ici l'intervention de Me Nicolas Cellupica :

L'échelon européen : stronger together ?

« Nous avons besoin de nos partenaires européens pour être efficaces, la France seule ne peut rien faire ».

Bruno Studer, Député du Bas-Rhin, Rapporteur de la loi contre la manipulation de l'information

Comme évoqué précédemment, l'UE est à ce jour la plus proactive dans la lutte globale contre les manipulations de l'information. La Présidente Ursula von der Leyen, et avant elle la commissaire Westager, ont entamé un véritable bras de fer contre les plateformes que ni la France, ni aucun État n'aurait pu soutenir seul. Face à ces géants numériques à la puissance de feu considérable, seule une réponse concertée et collective peut permettre de récréer les conditions d'une souveraineté non seulement nationale, mais aussi et surtout européenne, comme l'appelle de ses vœux le Président de la République française depuis 2017. Le prochain combat à mener à l'échelle européenne est celui de la remise en cause du statut d'hébergeur, qui exempt les plateformes de toute responsabilité quant aux contenus publiés sur leurs pages. Car comme le rappelle le Député **Bruno Studer**, *« c'est l'essence même de la démocratie qui est en jeu »*.

Conclusion : la démocratie en danger ?

Face aux manipulations de l'information, les démocraties sont en danger. Elles le sont inévitablement car c'est le propre des démocraties que de permettre à leurs adversaires et opposants de s'exprimer – et potentiellement donc les remettre en cause. Mais ces derniers disposent aujourd'hui de moyens sans précédent pour formuler et diffuser des opinions contestataires ou des contenus extravagants, à la fois en termes de volume et de vitesse de propagation : les plateformes des réseaux sociaux, dont la rapide montée en puissance semble de plus en plus susceptible de déstabiliser et de fragiliser durablement les modèles démocratiques. Leurs adversaires ou concurrents, acteurs privés comme étatiques, ont bien compris qu'ils pouvaient exploiter ces faiblesses, transformant ainsi l'espace informationnel en un véritable théâtre d'affrontement.

Face aux velléités des acteurs privés et aux ingérences étrangères, c'est aussi la souveraineté des États concernés qui est en cause. Et puisqu'aucun État ne peut y résister seul, c'est collectivement qu'ils doivent répondre aux manipulations de l'information et aux tentatives de déstabilisation informationnelle, que ce soit à l'échelon bilatéral, multilatéral, ou régional. Un dialogue constant et étroit avec les parties prenantes, notamment les plateformes numériques, s'impose aussi. Enfin, au-delà des États et des entreprises, les institutions que sont l'école et le journalisme professionnel, doivent activement prendre part à la lutte contre les manipulations de l'information.

FOCUS INNOVATION

CryptoNext Security : prévoir une sécurité de long terme par la cryptographie résistante au quantique

Entretien avec Ludovic Perret (co-fondateur).

Présentation

CryptoNext Security est une startup née en 2019 d'un *spin-off* de l'INRIA et de Sorbonne Université. Les fondateurs de cet éditeur de logiciels sont Ludovic Perret (CEO) et Jean-Charles Faugère (CTO), chercheurs-entrepreneurs, spécialisés dans l'analyse de sécurité de la cryptographie (« du côté de l'attaquant ») par des techniques algébriques.

En 2016, le National Institute of Standards and Technologies (NIST) a initié un renouvellement inédit des standards de cryptographie et a appelé la communauté scientifique mondiale à lui soumettre ses meilleurs algorithmes. La bonne représentation de la France dans le dernier tour de sélection consacré à la cryptographie résistante au quantique, avec un académique français impliqué dans plus de la moitié des algorithmes retenus, est l'un des facteurs qui a motivé Ludovic Perret et Jean-Charles Faugère, candidats toujours en lice, à créer CryptoNext Security. Leur startup a en effet pour objectif de capitaliser et de traduire cette excellence de la recherche nationale en opportunités technologique et commerciale.

Face aux menaces que les progrès quantiques font peser sur la protection des communications, CryptoNext Security accompagne de manière proactive ses clients – entreprises comme ministères – dans la migration vers des solutions de cryptographie résistante au quantique, que la startup développe et aide à mettre en place.

Solution

La solution de CryptoNext Security s'appuie sur une cryptographie dite « résistante au quantique ». Elle s'inscrit dans le contexte de montée en puissance de l'ordinateur quantique dont le potentiel est susceptible d'affecter à terme la sécurité de la cryptographie à clé publique.

Cette cryptographie à clé publique est un pilier fondamental du développement de l'Internet. Elle intervient dans la majorité des communications sécurisées, qu'il s'agisse des réseaux web (SSL, VPN…), des messageries instantanées ou de la *blockchain*. Elle permet de partager une clé secrète pour garantir la confidentialité des communications entre des parties ou de les authentifier au moyen d'une signature. La sécurité des algorithmes à clé publique repose sur des problèmes mathématiques de théorie des nombres, complexes à résoudre pour des ordinateurs classiques mais simples pour des ordinateurs quantiques.

La perspective de voir émerger un ordinateur quantique suffisamment puissant (avec assez de qubits) pour résoudre ces algorithmes, et donc casser la cryptographie à clé publique, est de plus en plus plausible. Bien que cette échéance soit incertaine, le fait que la Chine et les États-Unis aient massivement investi dans le quantique pose un potentiel enjeu de souveraineté à venir, sur lequel CryptoNext Security mise. La startup

souhaite en effet aider les entités à chiffrer dès maintenant leurs données stockées à haute valeur ajoutée (défense, banque, etc.), en les prémunissant contre toute cybermenace quantique (*harvest now*, *decrypt later*).

La loi de programmation militaire (2019-2025) fait par ailleurs de la cryptographie et de l'informatique quantique des « innovations de rupture et de supériorité opérationnelle », pour lesquelles elle prévoit davantage d'investissements. Une ambition dans ce domaine qui a été confortée par l'annonce du Président de la République, en janvier 2021, d'un plan d'investissement national dans le quantique et la cryptographie résistante au quantique. Celui-ci vise à placer la France dans le trio de tête mondial des technologies quantiques.

Dans ce cadre, la solution de CryptoNext Security utilise des algorithmes à clé publique qui reposent sur des problèmes très difficiles à résoudre, même pour un ordinateur quantique. Il s'agit d'une bibliothèque logicielle permettant d'effectuer les deux fonctions principales de la cryptographie à clé publique : l'échanges de clés et la signature électronique. Elle intègre tous les algorithmes finalistes de la sélection du NIST dans des environnements techniques variés pour optimiser les performances.

Applications

Concrètement, la solution est un logiciel qui ne cherche pas à remplacer la cryptographie initiale d'une application mais à la complémenter par une couche résistante au quantique. Ce caractère hybride, recommandée par l'ANSSI, offre la garantie de ne pas dégrader le système existant et de pouvoir s'intégrer à tout type de protocoles de sécurité, en se « greffant » par-dessus, qu'importe le support (processeur puissant, ordinateur, *smartphone*, IoT, etc.). En d'autres termes, la solution apporte une double-protection par le biais d'un double-jeu de clés.

Elle peut ainsi s'appliquer par extension à tous les cas d'usage. Ci-dessous, deux exemples publics :

- L'intégration d'une surcouche de cryptographie résistante au quantique à une application de messagerie instantanée au profit de l'OTAN ;
- l'intégration d'une option de cryptographie résistante quantique dans les *hardware security modules* (HSM) Luna de Thales, avec qui CryptoNext Security a d'ailleurs récemment noué un partenariat.

La solution a été conçue de sorte à ne pas entraîner de modification pour l'utilisateur final des applications à sécuriser – elle peut même augmenter la confiance envers ces dernières. Elle permet aussi d'assurer une transition douce en faveur de la potentielle migration générale vers la cryptographie résistante au quantique.

Actualité

En 2020, CryptoNext Security a été retenue dans l'étape finale de la sélection du NIST pour son algorithme dédié à la signature numérique. Aujourd'hui, les demandes des clients s'accélèrent et la startup prévoit prochainement une seconde levée de fonds. CryptoNext Security est lauréat du grand Prix du concours d'innovation i-Lab 2020.

CALENDRIER

25/03/2021 : CYBERSECURITÉ ET ESPACE NUMÉRIQUE : QUELLES PRIORITÉS POUR LA PROCHAINE PRÉSIDENCE FRANÇAISE DE L'UNION EUROPÉENNE ?

Le Forum International de la Cybersécurité (FIC) organise le jeudi 25 mars 2021 une matinée de webinar-débat visant à contribuer à la **préparation de la Présidence française de l'Union Européenne (PFUE)** qui doit débuter le 1er janvier 2022.

Souhaitant incarner et défendre les valeurs d'une Europe « plus solidaire et plus souveraine », la future Présidence française fera du triptyque « Relance, puissance, appartenance » le fil rouge de son action. Le numérique, à la fois outil de relance, vecteur de puissance et élément constitutif du sentiment d'appartenance européenne que la France entend développer, sera donc au cœur des priorités.

La rencontre réunira décideurs privés, chercheurs, acteurs politiques et institutionnels pour débattre des grandes orientations qui seront données à la PFUE sur toutes les questions de sécurité et de confiance numérique. Elle s'articulera autour de trois sessions :

- Session 1 : Un bouclier cyber européen au service de la "relance"
- Session 2 : Le modèle numérique européen, "clé de l'appartenance"
- Session 3 : "L'Europe puissance" à l'épreuve du numérique

Un groupe d'experts se réunira ensuite dans le cadre de l'Agora pour travailler à la définition d'une feuille de route publiée lors du FIC (8, 9 et 10 juin 2021).

Retrouvez plus d'informations sur le site de l'Agora du FIC.

Inscrivez-vous directement par courriel à paul.azibert@avisa-partners.com

ACTUALITÉ

PRÉSENTATION DE LA STRATÉGIE NATIONALE POUR LA CYBERSÉCURITÉ

Le Président de la République a présenté le 18 février les objectifs de la stratégie nationale d'accélération pour la cybersécurité. Dans le contexte des cyberattaques qui ont touché ce mois les hôpitaux de Dax et de Villefranche-sur-Saône, Emmanuel Macron a rappelé l'ambition du gouvernement de soutenir la filière nationale de la cybersécurité et de renforcer la souveraineté et l'innovation française dans ce domaine.

L'objectif principal de cette stratégie nationale est de tripler le chiffre d'affaires actuel de la cybersécurité en atteignant les 25 Md€. Elle vise également à doubler le nombre d'emplois de la filière, en passant de 37 000 à 75 000 postes, et à faire émerger trois licornes françaises (startup valorisée à plus de 1Md€).

Grâce à un investissement de 1Md€, plusieurs mesures concrètes sont prévues pour 2021/2022 dont :

- Le soutien à des projets de R&D de nouvelles technologies souveraines et consacrées à des thématiques spécifiques qui seront dévoilées progressivement ;
- le lancement de programmes et équipements prioritaires de recherche (PEPR) ;
- la mise en place d'un « Observatoire des métiers et des qualification de la sécurité du numérique » ;
- l'ouverture à l'automne d'un Campus Cyber qui fédèrera l'écosystème de la cybersécurité.

En outre, les structures de santé bénéficieront désormais d'un soutien renforcé de l'Agence du numérique en santé et de l'ANSSI en matière de détection de vulnérabilités. Elles devront également consacrer 5 à 10% de leur budget informatique à la cybersécurité, notamment pour le maintien en condition de sécurité des SI.

Retrouvez plus d'information sur le site de la Direction générale des entreprises en cliquant ici.

La **Direction générale des relations internationales et de la stratégie (DGRIS)** propose des analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et les organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

À ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique (OMC)**, qui s'inscrit dans le contrat-cadre n°2018-02. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère des Armées
Direction générale des relations internationales et de la stratégie
60 boulevard du général Martial Valin | 75015 Paris

CEIS
Tour Montparnasse | 33 avenue du Maine | 75015 Paris
E-mail : omc@ceis.eu