FONDATION ROBERT SCHUMAN

POLICY PAPER

**Schuman Paper**
n°816
12 janvier 2026

**Earl WANG**

# La formulation stratégique européenne sur la sécurité technologique : les défis de la Chine

*Cet article est publié dans le cadre de l'Observatoire du multilatéralisme en Indo-Pacifique, un programme de recherche pluriannuel initié et soutenu par la Direction générale des relations internationales et de la stratégie (DGRIS) du ministère français des Armées. Le programme est piloté par la Fondation pour la recherche stratégique (FRS) en coopération avec l'European Council on Foreign Relations (ECFR), l'Institut Montaigne, le Centre de recherches internationales de Sciences Po (CERI-Sciences Po) et l'Institut national des langues et civilisations orientales (Inalco). Cette publication propose une analyse du sujet de 2013 à 2022.*

Les États-Unis, mais aussi l'Union européenne et ses 27 États membres font face à des restrictions chinoises concernant les infrastructures technologiques critiques étrangères. Les entreprises européennes de télécommunications comme *Nokia* et *Ericsson* ont vu leur part de marché en Chine chuter des deux tiers par rapport à 2020. À l'inverse, les fournisseurs chinois « à haut risque » de réseaux de télécommunications, tels que *Huawei* et *ZTE*, n'ont subi qu'un déclin de 5 à 10% en Europe depuis que l'Union européenne a adopté la boîte à outils pour la sécurité des réseaux 5G en 2020.

En matière de cybersécurité, on observe également des menaces directes de la part de la Chine. Les récentes cyberattaques publiques contre la France et la République tchèque nous rappellent – une fois de plus – les défis de cybersécurité posés par la Chine, comme l'a souligné l'Organisation du traité de l'Atlantique Nord (OTAN).

Les technologies critiques, ainsi que les infrastructures cyber et numériques, figurent en tête des préoccupations de l'Union en matière de sécurité technologique vis-à-vis de la Chine.

Cet article propose une analyse de la formulation stratégique des institutions européennes et des États membres sur la sécurité technologique face à la Chine, de 2013 à 2022. Les pays étudiés sont la France, l'Allemagne, la Grèce, les Pays-Bas, la République tchèque et le Royaume-Uni.

## I. LA SÉCURITÉ DES TECHNOLOGIES CRITIQUES

### Made In China 2025 : La politique nationale pour dominer dans le domaine technologique

Lancé en mai 2015, *Made in China 2025* (MIC 2025) est une politique chinoise visant à moderniser les capacités technologiques et industrielles du pays et à en faire une puissance manufacturière haut de gamme d'ici 2049[1]. Le gouvernement chinois identifie des technologies et des industries dans les domaines de l'information, de la robotique/ machines automatisées, de l'aérospatial et des véhicules à nouvelle énergie – parmi d'autres « secteurs clés » – dans la politique *MIC 2025*. L'objectif est de « localiser » les chaînes de valeur des industries high-tech en Chine et de réduire la dépendance du pays aux équipements et savoir-faire étrangers.

*[1] L'année 2049 marquera le centenaire de la fondation de la République populaire de Chine (RPC).*

En tant que « projet phare » du président Xi pour atteindre le progrès technologique, le *MIC 2025* ne semblait pas de nature à susciter autant d'inquiétudes de la part des institutions de l'Union européenne ou des États membres à la fin des années 2010. Les principales raisons de cette prise de conscience résident dans l'augmentation des investissements et acquisitions chinois dans les technologies avancées de l'Union, et les implications de ces mouvements chinois sur la sécurité de l'Europe. Les investissements chinois à l'étranger ont été très ciblés sur les « actifs high-tech et de fabrication avancée ». Ces cibles choisies répondent à des « intérêts clairement définis », qui ne sont pas seulement économiques, mais aussi « stratégiques globaux, incluant les dimensions politiques et sécuritaires ».

## La prise de conscience progressive des implications sécuritaires des investissements chinois

Dans l'*EU-China 2020 Strategic Agenda for Cooperation* de 2013, les deux parties encourageaient la coopération en matière de science, de technologie et d'innovation, en complémentarité des forces mutuelles et pour des résultats gagnant-gagnant. Dans le *China's Policy Paper on the EU* de 2014, la Chine promouvait les échanges technologiques et la coopération avec l'Union dans diverses industries stratégiques émergentes, telles que les énergies renouvelables, l'information numérique et la fabrication avancée. Le ministère allemand de l'Éducation et de la Recherche, par exemple, a développé des interactions et une coopération étroite avec la Chine[2]. La Chancellerie et le ministère de l'Économie avaient une opinion plus positive sur l'engagement économique et industriel avec la Chine, tandis que d'autres ministères, comme le ministère des Affaires étrangères et le ministère de la Défense, adoptaient des attitudes plus prudentes[3]. L'ancienne chancelière allemande, Angela Merkel, s'est davantage concentrée sur la coopération dans les relations germano-chinoises[4].

La situation prometteuse a commencé à changer dans le document *Elements for a new EU strategy on China* en 2016. Ce document encourageait la coopération technologique et l'innovation entre l'Union européenne et la Chine, mais il soulignait les difficultés croissantes d'accès au marché rencontrées par les entreprises numériques européennes en Chine après la mise en place de la politique *MIC 2025*, ainsi que les préoccupations concernant le piratage et le vol de propriété intellectuelle technologique par la Chine. De plus, la Chine concurrence aussi l'Europe dans l'établissement de normes technologiques dans des domaines comme la 5G, l'intelligence artificielle et les nouveaux véhicules électriques[5]. L'Union et ses États membres ont progressivement pris conscience des risques liés à la coopération en matière de recherche et de technologie avec la Chine[6]. Du côté chinois, le document *China's Policy Paper on the European Union* de 2018 a maintenu la tonalité de celui de 2014 en promouvant la coopération technologique et l'innovation, sans mentionner sa politique *MIC 2025* ni aborder les préoccupations qui y sont liées.

L'Allemagne, l'une des principales puissances industrielles européennes, a collaboré avec la Chine dans la mesure où cette dernière est un partenaire manufacturier majeur. Les deux parties se sont donc complétées. Cependant, la situation de concurrence entre la Chine et l'Allemagne, ainsi que d'autres États membres, dans les industries à forte intensité technologique s'est intensifiée. Elle est devenue de plus en plus notable depuis le lancement de la politique *MIC 2025*[7]. La Fédération des industries allemandes (BDI) a soulevé ces préoccupations dans un document en janvier 2019 qui mettait clairement en lumière la politique *MIC 2025* et les actions chinoises d'investissements publics dans les technologies avancées, ainsi que les « transferts forcés de technologie et les rachats stratégiques d'entreprises high-tech étrangères » dans le but d'atteindre une « suprématie technologique ». En conséquence, la BDI a qualifié la Chine de « concurrent systémique » en plus d'être un partenaire.

La réflexion et l'indication de la BDI ont fortement influencé la désignation de la Chine comme « concurrente » et « rivale systémique » dans le document *EU-China – A Strategic Outlook* en 2019 qui exprimait de manière encore plus claire que « la Chine ne peut plus être considérée comme un pays en développement. C'est un acteur mondial clé et une puissance technologique de premier plan ». La Chine était ainsi définie comme un « concurrent économique

**[2]** *Entretien avec Friedolin Strack, en ligne, juin 2021. Suite à la prise de conscience progressive des risques de sécurité dans la coopération en matière de recherche, de technologie et d'innovation avec la Chine, le gouvernement fédéral allemand a mis en place en 2018 un mécanisme de coordination interministérielle sur les questions chinoises.*

**[3]** *Entretien avec un expert sur l'Asie d'une fondation politique allemande, en ligne, juin 2021.*

**[4]** *Ibid et entretien avec un fonctionnaire allemand, en ligne, juin 2021.*

**[5]** *Entretien avec un fonctionnaire du SEAE, en ligne, mai 2021.*

**[6]** *Ibid.*

**[7]** *Entretien avec Reinhard Bütikofer, en ligne, février 2021.*

dans la quête de leadership technologique », en plus d'être un partenaire et un rival systémique. L'Union européenne a souligné que la Chine développait ses « secteurs high-tech stratégiques » tout en limitant l'accès au marché et en exigeant des transferts forcés de technologie de la part des entreprises étrangères via la politique *MIC 2025*. De plus, le document indiquait que les investissements étrangers et les acquisitions de technologies critiques de l'Union « peuvent poser des risques pour la sécurité ». On observe que les défis sécuritaires liés aux investissements étrangers et aux acquisitions de technologies critiques sont progressivement devenus un sujet clé dans la politique européenne envers la Chine[8]. La prise de conscience par l'Union et ses États membres du lien entre sécurité et technologie est un phénomène « très récent »[9].

L'Allemagne est un exemple marquant de la vigilance croissante face aux tentatives chinoises d'acquérir des technologies avancées en Europe. Le rachat de l'entreprise allemande *KUKA* par l'entreprise chinoise *Midea* en 2016 a souvent été qualifié de « signal d'alarme » ou de « point de non-retour »[10]. *KUKA* était un leader dans le secteur de la robotique industrielle à l'échelle mondiale, tandis que *Midea* est un fabricant d'appareils électriques spécialisé dans les produits comme les machines à laver, les réfrigérateurs et les climatiseurs. Le gouvernement allemand a autorisé l'opération en août 2016, expliquant qu'elle ne « menaçait pas la sécurité » du pays. Des articles de presse ont rapporté que le PDG de *KUKA* avait des stratégies de développement différentes de celles du président du conseil d'administration de la société mère *Midea*, et que *KUKA* a changé de PDG en décembre 2018. Cette opération a suscité des préoccupations et des débats sur les risques liés à l'acquisition de technologies de pointe européennes par des entreprises étrangères, en particulier lorsqu'un pays étranger a développé une politique nationale pour être concurrentiel dans le domaine technologique.

Dans le rachat d'*Aixtron* par le *Fujian Grand Chip Investment Fund*, l'opération a été bloquée par le gouvernement allemand en octobre 2016. *Aixtron* est un fournisseur d'équipements pour semi-conducteurs, tandis que le *Fujian Grand Chip Investment Fund* est un fonds d'acquisition. Le ministère allemand de l'Économie avait initialement approuvé l'opération en septembre 2016, malgré des préoccupations similaires à celles soulevées par l'affaire *KUKA* un mois plus tôt. En octobre, il a réexaminé l'opération à la suite de « nouvelles informations liées à la sécurité », et a finalement retiré son autorisation. Les États-Unis ont joué un rôle dans l'affaire *Aixtron*. Le Comité sur les investissements étrangers aux États-Unis – un comité interministériel du gouvernement américain présidé par le secrétaire au Trésor pour examiner les effets des investissements étrangers sur la sécurité nationale – a examiné *Aixtron* car l'entreprise possède des actifs aux États-Unis. Le Comité a alerté le gouvernement allemand sur les risques sécuritaires. Le *Fujian Grand Chip Investment Fund* a finalement abandonné l'opération en décembre 2016.

Ces deux cas illustrent le lien croissant entre les dimensions économique, sécuritaire et technologique. L'Allemagne avait l'habitude de tenter de séparer l'économie d'un côté, et la politique et la sécurité de l'autre, en raison de son histoire[11]. Depuis le lancement de la politique *MIC 2025*, on observe un changement dans la posture traditionnellement ouverte de l'Allemagne en matière d'investissement en raison des préoccupations sécuritaires liées aux investissements et acquisitions chinois dans les technologies avancées. Les investissements chinois dans les technologies critiques allemandes ont suscité de plus en plus de débats et d'attention publique[12]. L'Allemagne a pris conscience des implications sécuritaires des investissements étrangers dans les technologies critiques.

Pour les Pays-Bas, la Chine et ses investissements dans les technologies avancées n'étaient pas sur l'écran radar sécuritaire[13]. Au début de cette décennie, le pays subissait des réductions du budget de la défense. Les sujets de sécurité étaient concentrés sur le continent européen ou, plus précisément, sur l'Union et le voisinage oriental. En même temps, les Pays-Bas ont suivi de près les politiques et priorités de l'OTAN[14]. L'OTAN a commencé à alerter sur les défis émergents posés par la Chine, et a officiellement reconnu la Chine comme un sujet important de l'Alliance lors de son sommet de Londres en 2019.

***[8]*** *Op. cit. 5.*

***[9]*** *Entretien avec François Godement, Paris, juillet 2021.*

***[10]*** *Entretiens avec trois fonctionnaires allemands, en ligne, juin 2021.*

***[11]*** *Op. cit. 3.*

***[12]*** *Op. cit. 3 et entretien avec un fonctionnaire allemand, en ligne, juin 2021.*

***[13]*** *Entretiens avec deux fonctionnaires néerlandais, en ligne, mars et mai 2021.*

***[14]*** *Entretiens avec un fonctionnaire néerlandais, en ligne, mars 2021.*

Les Pays-Bas ont progressivement prêté attention aux investissements et acquisitions chinois – voire aux vols – de technologies avancées[15].

L'Université de Leiden a mis fin à son accord de partenariat avec l'Institut Confucius en août 2019, invoquant le fait que « les activités de cet Institut ne s'alignaient plus sur la stratégie de l'Université vis-à-vis de la Chine ». La décision de l'université était un exemple de la prise de conscience progressive des risques et défis de la coopération scientifique avec la Chine – en plus des opportunités[16]. Ils incluent, par exemple, le vol potentiel de données et de propriété intellectuelle, la « censure et l'atteinte à la liberté académique », et le fait que la recherche scientifique chinoise s'aligne de plus en plus sur les « besoins de sécurité et la vision stratégique » du gouvernement chinois. De plus, sur le plan sécuritaire de la coopération scientifique, les services néerlandais de sécurité et des affaires étrangères ont travaillé à sensibiliser d'autres institutions gouvernementales et non gouvernementales, qui considéraient la Chine comme une opportunité, aux risques et défis liés à la collaboration. Ces institutions incluent, par exemple, les entreprises, les établissements académiques, les gouvernements non centraux (provinces et municipalités), ainsi que les ministères de l'Économie et de l'Éducation, de la Culture et des Sciences.

En mai 2019, les Pays-Bas ont publié le document *The Netherlands and China: A New Balance*, qui peut être vu comme un tournant dans la politique néerlandaise envers la Chine. Dans ce document, la Chine était décrite comme un « concurrent fort » en matière de technologie, visant à devenir une « superpuissance technologique » grâce à sa politique *MIC 2025*. Parmi d'autres actions menées par le gouvernement, la Chine a imposé des transferts forcés de technologie aux entreprises étrangères, investi et acquis des entreprises étrangères, et mobilisé des « tactiques numériques agressives » pour accéder aux technologies avancées.

Le rapport annuel 2022 du Service général de renseignement et de sécurité des Pays-Bas indiquait que la Chine représentait la « plus grande menace » pour la « sécurité économique » et les « intérêts de sécurité nationale » – outre la Russie. La raison en est que la Chine cherche à acquérir stratégiquement des technologies avancées néerlandaises et européennes, tant par des moyens légaux (investissements, fusions et acquisitions, projets de recherche conjoints) qu'illégaux (espionnage, investissements clandestins, exportations illégales).

La France a également vu croître ses préoccupations concernant le lien entre sécurité et technologie dans ses relations avec la Chine[17]. D'abord, la préoccupation est sérieuse vis-à-vis de l'ambition et des activités chinoises d'acquisition de propriété intellectuelle liée aux technologies avancées de la France et d'autres États membres. Ensuite, sont en cause les mesures connexes prises par la Chine pour établir des restrictions empêchant l'accès étranger à ses capacités technologiques. Sur le plan technologique et sécuritaire, la mobilisation de l'Union est l'approche la plus adaptée pour la France afin d'avoir un levier suffisant dans les négociations avec la Chine et d'éviter les menaces chinoises envers les États membres individuels[18].

On observe la prise de conscience progressive de la dimension sécuritaire des technologies critiques, à travers les cas de l'Allemagne, des Pays-Bas et de la France. Cette évolution est liée à la fois à la politique *MIC 2025* de la Chine et à l'augmentation des préoccupations concernant les investissements et acquisitions chinois de technologies avancées des États membres. Ces préoccupations concernant les risques et défis posés par la Chine ont également été renforcées par le changement de perception de l'Union et de ses États membres vis-à-vis de la Chine, considérée comme un « concurrent économique dans la quête de leadership technologique ».

## II. LA SÉCURITÉ DES INFRASTRUCTURES NUMÉRIQUES

Des chercheurs estiment que les infrastructures critiques comme les ports, aéroports, chemins de fer et réseaux électriques sur le sol européen sont généralement « trop ouverts » à l'acquisition ou, même, à la propriété étrangère par le biais d'investissements.

*[15]* Ibid.

*[16]* Ibid.

*[17]* Entretiens avec deux fonctionnaires français, Paris, juin et août 2021.

*[18]* Ibid.

Ce phénomène contribue au risque d'ingérence politique et stratégique des acteurs étrangers – publics et privés – dans l'Union européenne. Les chercheurs ont également souligné le fait que le commerce et les investissements sont de plus en plus liés à la sécurité technologique, en particulier dans le domaine des infrastructures numériques[19].

Les infrastructures numériques désignent « un ensemble de composants technologiques de l'information et de la communication qui constituent le fondement des services de technologies de l'information et de la communication. Ceux-ci incluent généralement des composants physiques – matériel informatique et de réseau, ainsi que des installations – mais aussi divers composants logiciels et réseau ».

Le sujet des infrastructures numériques n'apparaissait ni dans l'*EU-China 2020 Strategic Agenda for Cooperation* de 2013, ni dans le *China's Policy Paper on the European Union* de 2014. Les préoccupations européennes ont commencé à émerger dans le document *Elements for a new EU strategy on China* en 2016. L'Union européenne a exprimé son mécontentement face aux contrôles de sécurité chinois des investissements européens en Chine, allant au-delà des « préoccupations légitimes de sécurité nationale ». À l'inverse, elle a souligné la nécessité de définir le domaine des infrastructures critiques parmi les États membres face aux investissements étrangers chinois en Europe. Le *China's Policy Paper on the European Union* de 2018 n'a pas abordé cette question. Cependant, sous la rubrique du commerce et des investissements, le document chinois aspire à ce que « l'Union maintienne son marché des investissements ouverts ».

Les préoccupations européennes concernant la sécurité des infrastructures numériques critiques sont devenues concrètes et sérieuses dans le document *EU-China – A Strategic Outlook* de 2019. Ce document consacre deux plans d'action (Neuf et Dix) à ce sujet, dont l'un se concentre sur les infrastructures numériques critiques. Le document indique explicitement que les investissements étrangers et les acquisitions d'infrastructures critiques peuvent mettre en danger la sécurité de l'Union. L'action Neuf concerne principalement la nécessité de sauvegarder la sécurité des infrastructures numériques, en mettant l'accent sur l'importance des réseaux 5G. De plus, dans l'action Dix, le document politique souligne la nécessité de détecter et de sensibiliser aux menaces sécuritaires provenant des investissements étrangers et des acquisitions d'infrastructures critiques de l'Union.

Au niveau européen, les infrastructures numériques, en particulier les réseaux 5G, sont l'un des principaux sujets sur lesquels l'Union a travaillé pour augmenter son effet de levier quand elle fait face à la Chine[20]. Elle a déployé beaucoup d'efforts pour coordonner les évaluations des risques nationaux et élaborer des mesures communes pour atténuer les risques sécuritaires des réseaux 5G. La boîte à outils pour la sécurité des réseaux 5G comprend, par exemple, la mise en place de mesures pour répondre aux risques sécuritaires posés par les fournisseurs de 5G (y compris la réduction des dépendances, les restrictions et même les exclusions des opérateurs à haut risque), la diversification de la chaîne d'approvisionnement des réseaux 5G, la coordination entre les États membres pour une certification de sécurité européenne sur les infrastructures 5G, et la mise à jour des examens de l'Union et de ses États membres sur les risques sécuritaires des infrastructures 5G par le biais du groupe de coopération NIS.

Ainsi, bien qu'il n'existe pas encore de politique 5G commune, des progrès concrets ont été réalisés dans l'établissement des politiques 5G des États membres et dans l'augmentation de la cohérence entre les politiques nationales sur la sécurité des infrastructures 5G. De plus, bien que les États membres restent les décideurs finaux des politiques nationales 5G, un mécanisme de coordination et de coopération à l'échelle de l'Union exerce une « pression positive » sur les États membres pour qu'ils introduisent des mesures visant à renforcer collectivement la sécurité des réseaux 5G européens[21]. En ce qui concerne les institutions communes, l'ENISA et la DG CONNECT ont formé des groupes de travail pour suivre et répondre aux risques de sécurité 5G en collaboration avec les autorités des États membres[22].

***[19]*** *Entretien avec Gudrun Wacker, en ligne, juin 2021.*

***[20]*** *Entretien avec Zaki Laïdi, en ligne, février 2021.*

***[21]*** *Ibid.*

***[22]*** *Op. cit. 5.*

Le Parlement européen a été actif dans la sensibilisation aux menaces sécuritaires posées par l'engagement de la Chine dans les infrastructures numériques, telles que les réseaux 5G. Pour certains députés européens, les fournisseurs chinois de télécommunications à haut risque sont systématiquement sensibles à la sécurité numérique de l'Union et de ses États membres[23]. En mars 2019, le Parlement européen a adopté une résolution sur ce sujet qui exprimait des préoccupations concernant les vulnérabilités des infrastructures 5G européennes construites par des entreprises à haut risque. Elle appelait à intégrer les risques sécuritaires dans les analyses des réseaux d'infrastructures critiques, ainsi qu'à renforcer la coordination entre les États membres et entre les niveaux européen et national. La principale demande de la résolution se retrouve plus tard dans le *Rapport sur l'évaluation coordonnée des risques liés à la cybersécurité des réseaux 5G* de l'ENISA en octobre 2019 et dans la boîte à outils pour la sécurité des réseaux 5G en janvier 2020.

Cependant, la sécurité des infrastructures numériques relève de la compétence des États membres, en particulier lorsqu'elle est liée à la sécurité nationale. Le Parlement européen est en mesure de susciter des débats, de sensibiliser et d'appeler le Conseil, la Commission et les États membres à faire des progrès plus concrets dans cette perspective. Cependant, il n'est pas en mesure de « forcer » les autres acteurs dans le processus décisionnel concernant ce sujet[24].

Au niveau national, la France, les Pays-Bas et la République tchèque ont été des contributeurs majeurs à la boîte à outils de sécurité 5G. La France a pris très au sérieux la sécurité des réseaux 5G, y compris la nécessité de réduire la dépendance à l'égard de la chaîne d'approvisionnement des infrastructures 5G chinoises[25]. Elle est de plus en plus consciente des intérêts stratégiques à protéger et des menaces sécuritaires posées par les investissements étrangers en matière d'infrastructures numériques[26]. En réponse à ces défis sécuritaires, la France insiste sur la nécessité pour l'Europe de mettre en place et de mobiliser les outils à leur disposition[27], tels que le mécanisme de contrôle des investissements étrangers directs (IDE). De plus, le Parlement français a adopté une loi sur la sécurisation des intérêts de défense et de sécurité nationale dans le domaine des réseaux mobiles (communément appelée « loi 5G ») en août 2019. Cette loi exige que l'exploitation de certains équipements électroniques soit autorisée par les services françaises compétentes, et que les opérateurs se conforment aux exigences administratives prévues par la loi. En juillet 2020, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a informé les opérateurs de télécommunications que l'agence ne renouvellerait pas les licences d'autorisation pour les équipements 5G de *Huawei*, dont l'échéance est prévue entre trois (2023) et huit ans (2028).

L'Allemagne, en réponse aux risques sécuritaires liés aux télécommunications, a travaillé à renforcer la résilience de ses infrastructures numériques[28]. Avec sa *IT Security Act 1.0*, entrée en vigueur en juillet 2015, elle vise à sécuriser son système informatique et ses infrastructures numériques. La *IT Security Act 2.0* est entrée en vigueur en mai 2021. Les lois allemandes sur la sécurité informatique exigent que les opérateurs de télécommunications respectent des « exigences de sécurité de haut niveau » et que les « composants critiques » obtiennent une certification de sécurité. Les entreprises allemandes dans des secteurs sensibles et d'une « importance économique particulièrement élevée » sont tenues de mettre en œuvre des mesures de sécurité informatique. En septembre 2023, le ministère de l'Intérieur a annoncé une proposition visant à restreindre l'utilisation par les opérateurs de télécommunications d'équipements 5G de *Huawei* et *ZTE* d'ici 2026.

Les responsables tchèques ont remarqué que certaines entreprises chinoises de télécommunications, comme *Huawei* et *ZTE*, sont liées aux activités et aux intérêts du gouvernement chinois[29]. Les discussions sur l'engagement de la Chine dans les infrastructures 5G se sont intensifiées avec l'augmentation des préoccupations sécuritaires en République tchèque. L'Agence pour la cybersécurité et la sécurité de l'information (NÚKIB) a émis un avertissement selon lequel les logiciels et matériels de *Huawei* et *ZTE* représentent une menace pour la cybersécurité.

**[23]** *Entretien avec Michael Gahler, en ligne, juin 2021.*

**[24]** *Ibid.*

**[25]** *Entretiens avec un fonctionnaire français, Paris, juin 2021.*

**[26]** *Op. cit. 9.*

**[27]** *Op. cit. 25.*

**[28]** *Entretien avec deux fonctionnaires allemands, en ligne, juin 2021.*

**[29]** *Entretien avec un fonctionnaire tchèque, en ligne, mai 2021.*

Classée au niveau de menace le plus élevé (niveau 4), la participation de *Huawei* aux réseaux 5G tchèques est restreinte. Les activités d'espionnage chinoises intensifiées en République tchèque sont également devenues un sujet que les services de renseignement surveillent de près[30].

Le Royaume-Uni a implanté le premier bureau de *Huawei* dès 2001, avant les autres pays européens. Huawei a accru son implication dans les infrastructures numériques britanniques depuis 2005, année où l'entreprise a obtenu des contrats de *British Telecom* pour en moderniser les réseaux de télécommunications, en particulier les « routeurs et autres équipements de transmission ». Les préoccupations sécuritaires britanniques concernant l'engagement croissant de *Huawei* dans les infrastructures numériques du pays ont commencé en 2010[31]. Ces préoccupations se sont encore aggravées depuis juin 2013, lorsque le Comité mixte du Parlement sur le renseignement et la sécurité – une commission commune de la Chambre des communes et de la Chambre des lords – a publié un rapport sur les risques pour la sécurité nationale posés par l'engagement de *Huawei* dans les infrastructures numériques critiques. En réponse, le gouvernement a reconnu que les procédures d'évaluation de la dimension sécuritaire des contrats de *British Telecom* avec *Huawei* étaient « insuffisamment robustes », il a été convenu que le Conseiller à la Sécurité Nationale examinerait le fonctionnement du Centre d'évaluation de la cybersécurité de *Huawei*[32], et il a reconnu la nécessité d'adopter une « approche fondée sur les risques » pour examiner les investissements étrangers dans les infrastructures critiques du pays. Après l'apogée des relations entre le Royaume-Uni et la Chine sous le mandat de David Cameron, le Centre britannique de cybersécurité a été créé en octobre 2016 et a surveillé de près les risques sécuritaires liés aux équipements et technologies de *Huawei* dans les infrastructures numériques[33]. En juillet 2020, le Royaume-Uni a annoncé l'interdiction de *Huawei* et d'autres entreprises chinoises à haut risque sécuritaire des réseaux 5G d'ici la fin de l'année 2027.

En ce qui concerne la Grèce, il est intéressant de noter la présence relativement limitée de la Chine dans les réseaux de 5G du pays. La raison en est que la Chine s'était fortement engagée dans les réseaux 4G grecs depuis l'investissement de *Huawei* dans la modernisation des réseaux 4G de l'entreprise de télécommunications *Wind Hellas*, en pleine crise financière. *Huawei* représenterait plus de 50% du réseau d'accès radio de la Grèce, qui est le composant de télécommunication reliant les appareils individuels aux autres parties des réseaux de télécommunication. Le réseau d'accès radio de *Wind Hellas* est presque exclusivement fourni par *Huawei*. Cependant, en passant progressivement aux infrastructures 5G, à la fin des années 2010 et encore plus depuis 2020, la Grèce a connu un moment où les États-Unis et d'autres États membres de l'Union européenne ont commencé à discuter ou à interdire la participation de *Huawei* et *ZTE* dans les infrastructures 5G sur leur sol. En juin 2020, la Grèce a rejoint l'initiative Clean Network, promouvant l'interdiction des équipements et services numériques provenant de gouvernements autoritaires. Bien que la Grèce n'ait pas décidé d'interdire à *Huawei* de participer aux infrastructures 5G, le pays s'est distancié de l'entreprise.

Une tendance similaire s'observe au sujet de la cybersécurité. L'Union européenne et ses États membres sont de plus en plus conscients et réagissent aux préoccupations de sécurité posées par l'engagement chinois dans les infrastructures numériques – en commençant par la 5G – sur le sol européen. L'Union a poussé ses États membres à progresser dans l'établissement de politiques nationales de sécurité 5G. Ils sont progressivement éveillés des risques sécuritaires posés par les entreprises chinoises fournissant des équipements et services 5G. Dans une mesure différente, les États membres ont ajusté leurs réglementations 5G concernant les entreprises chinoises à haut risque, en particulier dans le cas de *Huawei* et *ZTE*.

## III. LE CADRE EUROPÉEN POUR LE FILTRAGE DES INVESTISSEMENTS DIRECTS ÉTRANGERS (IDE)

Le nouvel outil européen pour répondre aux préoccupations de sécurité liées aux investissements étrangers et des acquisitions d'infrastructures et de

***[30]*** *Ibid.*

***[31]*** *Entretien avec deux fonctionnaires britanniques, en ligne, mars 2022.*

***[32]*** *Il a été créé en 2010 pour examiner les risques de sécurité liés à la présence croissante de Huawei dans l'infrastructure numérique critique du Royaume-Uni.*

***[33]*** *Op. cit. 31.*

technologies critiques est le mécanisme de filtrage des IDE. Il a établi un cadre, d'une part, pour que les États membres examinent les IDE sur la base de la sécurité ou de l'ordre public, et d'autre part, pour la coordination et la coopération entre les États membres et entre les niveaux européen et national.

La Commission a présenté la proposition du cadre européen de filtrage des IDE en septembre 2017. Le Conseil et le Parlement européen sont parvenus à un accord politique sur ce mécanisme en novembre 2018. En mars 2019, le mécanisme de filtrage des IDE a été adopté. En fait, ce mécanisme était fondé sur l'initiative de la France, de l'Allemagne et de l'Italie en février 2017[34]. Dès mai 2012, le Parlement européen avait déjà adopté une résolution appelant à la mise en place d'un « nouveau cadre institutionnel » pour traiter les implications sécuritaires des investissements stratégiques étrangers, en référence au modèle du Comité américain sur les investissements étrangers.

Le cadre européen de filtrage des IDE a été considéré comme une étape importante pour deux raisons principales[35]. Premièrement, le mécanisme a été mis en place en dix-huit mois, ce qui est un délai très efficace pour la prise de décision européenne. Un consensus a été trouvé en un laps de temps relativement court, malgré le caractère novateur du concept. Le consensus sur la nécessité de ce nouvel outil a été trouvé dans l'écosystème européen sur le fondement de travaux analytiques menés par les États membres et les institutions communes. Deuxièmement, l'Union a pu mobiliser sa compétence en matière de commerce et d'investissement, et la lier à des questions de sécurité, ce qui a ouvert de nouvelles dimensions dans le domaine de la sécurité.

Il est important de souligner que les révisions et les décisions finales concernant les cas d'investissements étrangers sont réalisés par les États membres sur la base de leurs mécanismes nationaux de contrôle, avec des variations dans leur portée et leurs critères. Cela dit, le cadre européen de filtrage des IDE permet une coordination de ces révisions au niveau européen. Par exemple, la Commission européenne peut émettre des avis sur les cas d'investissements étrangers, les États membres ont l'obligation de notifier à la Commission les cas d'IDE contrôlés, les États membres sont appelés à mettre à jour et à mettre en place des mécanismes nationaux de filtrage, et des points de contact de la Commission et des États membres ont été établis pour échanger des informations. Les IDE relèvent d'une compétence exclusive de l'Union, tandis que la question de la sécurité relève de la compétence des États membres. Par conséquent, l'efficacité du cadre européen de contrôle des IDE dépend largement de la coordination et de la coopération entre le niveau européen et le niveau national.

Les chercheurs et décideurs politiques ont loué ce cadre européen de filtrage des IDE, considéré comme un outil concret et utile de l'Union face aux défis de sécurité liés aux investissements étrangers et à l'acquisition des technologies et infrastructures critiques[36]. Grâce à cet outil, l'Union a accru son effet de levier dans ses interactions avec la Chine. Le mécanisme repose sur la conviction centrale que l'Europe reste ouverte aux investissements étrangers, mais qu'elle doit protéger ses technologies critiques et ses infrastructures si des implications sécuritaires existent.

## IV. LA CYBERSÉCURITÉ

### Les autorités européennes de cybersécurité

Dans son *Règlement sur la cybersécurité* de 2019, l'Union européenne a défini la « cybersécurité » comme « les actions nécessaires pour protéger les réseaux et les systèmes d'information, les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces ». Elle a utilisé la terminologie de « sécurité des réseaux et des systèmes d'information » plutôt que celle de « cybersécurité » dans ses documents juridiques avant le *Règlement sur la cybersécurité*.

En ce qui concerne les autorités responsables de la cybersécurité, l'organisme compétent est l'Agence de l'Union européenne pour la cybersécurité (ENISA). D'abord créée sous le nom d'Agence européenne chargée de la sécurité des réseaux et de l'information en mars 2004, l'objectif de l'ENISA est d'« aider la

***[34]*** *Entretiens avec un fonctionnaire allemand et avec Mikko Huotari, en ligne, juin 2021.*

***[35]*** *Entretien avec un fonctionnaire de la Commission européenne, en ligne, février 2021.*

***[36]*** *Op. cit. 10, 14, 20, 29, 34, avec trois fonctionnaires français, Paris, juin, juillet et août 2021, et avec un fonctionnaire du SEAE, en ligne, juillet 2021.*

Commission et les États membres et, par conséquent, coopérer avec la communauté des affaires, afin de les aider à répondre aux exigences de la sécurité des réseaux et de l'information ». Il était explicitement mentionné dans le règlement fondateur de l'ENISA que le fonctionnement de l'agence « ne porte pas atteinte » aux compétences des États membres. Le mandat de l'ENISA – en termes de durée – a été prolongé en 2008, 2011 et 2013 avant de devenir une agence permanente de l'Union européenne sous son nom actuel en 2019.

Au niveau national, les cadres juridiques et les structures des autorités nationales de cybersécurité varient[37]. Par exemple, pour les six pays étudiés, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) française a été créée parmi les premières en 2009, et est placée sous la supervision du Secrétariat général de la défense et de la sécurité nationale (SGDSN), sous l'autorité du Premier ministre. Le National Cyber Response Centre (Cyber-AZ) allemand a été créé en 2011. Il ne s'agit pas d'une autorité en soi, mais il exerce ses fonctions au sein de l'Office fédéral de la sécurité des technologies de l'information (BSI), sous l'autorité du ministère de l'Intérieur (BMI). En République tchèque a été mis en place le National Cyber and Information Security Agency (NÚKIB) en 2017, remplaçant à la fois le National Cyber Security Centre (NCKB) et le Cyber Security Council (CSC) créés en 2011. Le NÚKIB relève de l'autorité du Premier ministre, auquel le directeur du NÚKIB rend compte. Le National Cyber Security Centre (NCSC-NL) néerlandais a été créé en 2012 et relève du ministère de la Justice et de la Sécurité (JenV). Créé en 2016, le National Cyber Security Centre (NCSC) britannique relève de la structure du Government Communications Headquarters (GCHQ). Le GCHQ ne fait pas partie du ministère des Affaires étrangères, du Commonwealth et du Développement (FCDO), mais est placé sous l'autorité du ministre des Affaires étrangères. Pour la Grèce, le pays disposait d'une Direction générale de la cybersécurité sous l'autorité du ministère de la Gouvernance numérique, créée en 2019. Le gouvernement a établi la National Cyber Security Authority en 2024 et celle-ci reste sous la supervision du ministre de la Gouvernance numérique.

Afin de faciliter la coordination et la coopération entre l'Union et ses États membres en matière de cybersécurité, le Groupe de coopération sur les réseaux et systèmes d'information (NIS) a été créé depuis juillet 2016. Il rassemble la Commission, l'ENISA et des représentants des autorités nationales de cybersécurité. La directive, qui l'a mis en place, vise à améliorer la cohérence de l'Union en exigeant des États membres qu'ils désignent un service national ainsi qu'un point de contact unique responsable de la cybersécurité. Le groupe NIS vise à renforcer les échanges entre les États membres sur les informations concernant la cybersécurité. En même temps, la directive souligne le respect de la compétence des États membres dans la détermination de la divulgation d'informations au regard de la sécurité nationale. Il y a effectivement une résistance de la part de certains États membres à une autorité de cybersécurité au niveau de l'Union[38]. Après tout, en tant que directive, bien qu'il s'agisse d'un acte juridiquement contraignant, ce sont les États membres qui adoptent les lois nationales sur la manière de réaliser les objectifs fixés par la directive – ou « transposition » en langage juridique.

## La cybersécurité dans les relations sino-européennes

Dans les relations entre l'Union européenne et la Chine, la cybersécurité était déjà mentionnée comme une préoccupation dans le document *EU-China 2020 Strategic Agenda for Cooperation* en 2013. La perspective d'améliorer la confiance et la coopération entre les deux parties dans le domaine cyber sous le cadre de l'ONU était présente. Le *China's Policy Paper on the EU* de 2014 reprenait essentiellement le même contenu que celui du document de l'Union de 2013.

Le document *Elements for a new EU strategy on China* de 2016 a commencé à indiquer les préoccupations européennes concernant le « vol cyber de droits de propriété intellectuelle et de secrets commerciaux » par la Chine. L'Union a exhorté la Chine à « appliquer le droit international existant dans le cyberespace », et à promouvoir un accord international sur la « protection des actifs cyber critiques ». En 2018, les expressions chinoises concernant la cybersécurité dans le *China's*

***[37]*** *Op. cit. 29 ; Strubel, Vincent. « Quelle stratégie pour la France face à une menace cyber en pleine croissance ? » Discours à Sciences Po, Paris, 6 mars 2024.*

***[38]*** *Op. cit. 29.*

*Policy Paper on the European Union* n'étaient qu'une paraphrase du document de 2014.

Le document *EU-China – A Strategic Outlook* de 2019 a abordé la question de la cybersécurité dans l'un des dix plans d'action. Il s'agit de renforcer la sécurité des infrastructures numériques critiques de l'Union européenne et de ses États membres. On peut donc comprendre que la cybersécurité a été classée parmi les priorités européennes dans ses relations avec la Chine. De plus, le document politique de 2019 a signalé l'implication sérieuse en matière de cybersécurité en indiquant les progrès de l'Union dans l'établissement d'un cadre de régime de sanctions contre les cyberattaques. En mai 2019, le Conseil a adopté le règlement pour établir un cadre de sanctions, permettant à l'Union européenne d'imposer des sanctions (interdiction de voyage et gel des avoirs) aux « personnes ou entités responsables de cyberattaques ou de tentatives de cyberattaques ». On peut donc observer une tendance croissante des préoccupations européennes concernant la sécurité du domaine cyber dans leurs relations avec la Chine.

Dix jours après la publication du document politique sur la Chine en 2019, le Conseil européen a invité la Commission à proposer une recommandation sur une « approche intégrée » de la cybersécurité des réseaux 5G. Quatre jours plus tard, la Commission européenne a présenté sa recommandation qui appelle les États membres à mener des évaluations nationales des risques 5G et à prendre les mesures de sécurité nécessaires en réponse à ces risques, ainsi qu'à développer une évaluation des risques coordonnée et des mesures d'atténuation communes. En octobre 2019 a été publié le *Rapport sur l'évaluation coordonnée des risques liés à la cybersécurité des réseaux 5G*. En janvier 2020, le Groupe NIS a adopté la boîte à outils pour la sécurité des réseaux 5G, visant à répondre collectivement aux défis de cybersécurité de la 5G.

La République tchèque a été l'un des contributeurs actifs à la politique de cybersécurité de l'Union. La cybersécurité est un sujet provoqué par les catastrophes : les États membres savent qu'il est crucial, mais ne font pas grand-chose de concret ou ne travaillent pas ensemble avec d'autres capitales avant que des incidents négatifs ne se produisent[39]. Lorsque la Chine a commencé à s'intéresser au renforcement des interactions avec les pays d'Europe centrale et orientale dans la première moitié des années 2010, elle ne connaissait pas beaucoup la région et n'y était pas très présente auparavant. Le renseignement a été une source importante d'acquisition d'informations pour fournir des orientations politiques à la Chine concernant la région. La République tchèque a commencé à détecter des activités de cyberespionnage attribuables à la Chine vers 2013 et 2014[40]. Écho aux préoccupations mentionnées dans les documents de l'Union européenne sur la Chine, des infractions cyber ont été observées dans les vols de droits de propriété intellectuelle d'entreprises européennes. Les services gouvernementaux concernés ont donc commencé à surveiller de près les activités cyber de la Chine vis-à-vis du pays.

L'Allemagne a abordé les préoccupations en matière de cybersécurité provenant d'acteurs menaçants étrangers[41], y compris la Chine, qui est devenue une « source majeure de cyberattaques contre l'Europe » dans le but de mettre en œuvre sa « politique industrielle ambitieuse ». La Chine est clairement considérée comme préoccupante en matière de cyberattaques[42]. En décembre 2019, l'Office fédéral de protection de la Constitution (BfV) a publié un rapport concernant des cyberattaques attribuées au *Winnti Group*, un groupe de piratage chinois prétendument parrainé par l'État. Le rapport indiquait des attaques du *Winnti Group* contre les entreprises allemandes *Henkel* (2014), *BASF* (2015), *Siemens* (2016), *Bayer* (2018) et *Roche* (2019), entre autres. Ces attaques visaient les entreprises allemandes des secteurs technologique et pharmaceutique, et ont progressivement ciblé les entités gouvernementales allemandes ainsi que les missions diplomatiques à l'étranger à partir de 2022. Le pourcentage d'entreprises allemandes ayant déclaré avoir subi des infractions cyber de la part de la Chine est passé de 30 en 2021 à 43 en 2022.

On observe une attention croissante de l'Union européenne et de ses États membres à la cybersécurité dans leurs relations avec la Chine depuis 2013. Bien

**[39]** *Ibid.*

**[40]** *Ibid.*

**[41]** *Op. cit.* 28.

**[42]** *Ibid.*

que la Chine ne soit sûrement pas le seul pays, elle est clairement l'un des principaux pays responsables d'infractions cyber contre les institutions de l'Union. Les acteurs européens – bien que très différents en termes de structures juridiques – ont créé des agences responsables de la cybersécurité ainsi qu'un organe de coordination entre l'Union et ses États membres. La difficulté principale pour la coordination et la coopération européennes en matière de cybersécurité réside dans le fait que la compétence des États membres prévaut lorsque la sécurité nationale est en jeu. La boîte à outils pour la cybersécurité 5G adoptée en janvier 2020, fournit un cadre aux institutions de l'Union et aux États membres pour atténuer collectivement les défis de cybersécurité de la 5G.

***

La question de la sécurité dans les domaines technologique, cyber et des infrastructures numériques n'a pas vraiment émergé comme un sujet important dans les relations UE-Chine en 2013. Depuis la seconde moitié des années 2010, elle est devenue une préoccupation de plus en plus sérieuse pour les institutions de l'Union et les États membres.

Alors que la politique *MIC 2025* aspire à moderniser les capacités technologiques et industrielles de la Chine, les investissements du pays à l'étranger ont été très ciblés sur les actifs high-tech et de fabrication avancée. L'Union européenne et ses États membres ont de plus en plus réalisé la nécessité de sécuriser leurs technologies critiques face aux investissements et acquisitions chinois. En matière de cybersécurité, la Chine a été identifiée comme une source majeure d'attaques. Concernant les infrastructures numériques, les acteurs européens sont devenus de plus en plus vigilants face aux défis sécuritaires posés par l'engagement chinois dans les infrastructures numériques, en commençant par la 5G.

Conçu et mis en œuvre en étroite coordination avec les États membres, le filtrage des IDE a été adopté par l'Union en mars 2019. Ce mécanisme a créé un cadre pour que la Commission et les États membres coordonnent leurs actions concernant les IDE. Il s'agit du nouvel outil européen pour examiner et modérer l'augmentation des investissements et acquisitions chinois dans les technologies et infrastructures critiques de l'Europe, pour des raisons de sécurité ou d'ordre public. L'Union européenne et ses États membres ont mis en place cet outil de manière très efficace et ont mobilisé la compétence européenne en matière de commerce et d'investissement pour la lier au domaine de la sécurité.

L'Union européenne et ses États membres ont ainsi intégré le lien croissant entre sécurité et technologie dans leur formulation stratégique de politique vis-à-vis de la Chine. Les acteurs européens sont passés de la prise de conscience à une vigilance accrue, puis à la mise en place de mesures pour répondre aux défis posés à la sécurité technologique de l'Europe dans leurs interactions avec la Chine. La sécurité technologique a été un élément significatif dans la formulation stratégique de la politique européenne envers la Chine.

Outre les efforts des institutions communes, les États membres ont joué un rôle significatif dans le processus de cette formulation stratégique, car la sécurité nationale relève de leur compétence. L'efficacité de la stratégie européenne en matière de sécurité technologique dépend de la coordination et de la coopération entre les niveaux européen et national. À cet égard, la boîte à outils pour la sécurité des réseaux 5G, le régime de sanctions contre les cyberattaques et le cadre européen de filtrage des IDE peuvent être considérés comme des réalisations concrètes. Cependant, la mise en œuvre effective des mesures de sécurité technologique vis-à-vis de la Chine par les États membres reste le principal devoir pour qu'une stratégie bien formulée de l'Union soit couronnée de succès.

Les discussions liées à la sécurité technologique européenne vis-à-vis de la Chine ont repris récemment. À la suite de la stratégie *ProtectEU* publiée en avril 2025, la Commission européenne aurait exploré les moyens de convaincre et de demander aux États membres d'exclure *Huawei* et

*ZTE* (les « fournisseurs à haut risque ») de leurs réseaux de télécommunications. Des États membres comme la Grèce et l'Espagne n'ont pas encore interdit la participation de ces entreprises chinoises. L'approbation par l'Espagne en juillet 2025 d'un contrat de plusieurs millions d'euros avec *Huawei* pour le stockage des données judiciaires a suscité de vives critiques en Europe et aux États-Unis. L'Allemagne, de son côté, est en train d'étendre son interdiction des fournisseurs de technologies chinoises à haut risque des réseaux de télécommunications à d'autres secteurs critiques comme l'énergie, les transports, la santé, etc. La réalisation de la stratégie européenne visant à consolider sa sécurité technologique reste donc un sujet crucial à suivre.

**Earl WANG**

Docteur, chercheur associé et chargé d'enseignement au Centre de recherches internationales (CERI) - Sciences Po/CNRS

Retrouvez l'ensemble de nos publications sur notre site :
**www.robert-schuman.eu**

Directeur de la publication : Pascale JOANNIN
ISSN 2402-614X