ÉTUDES
DE L'IFRI

GEOPOLITICS OF TECHNOLOGY PROGRAM

FEBRUARY
2022

# Convince and Coerce

## U.S. Interference in Technology Exchanges Between its Allies and China

Mathilde VELLIET

The French Institute of International Relations (Ifri) is a research center and a forum for debate on major international political and economic issues. Headed by Thierry de Montbrial since its founding in 1979, Ifri is a non-governmental, non-profit organization.

As an independent think tank, Ifri sets its own research agenda, publishing its findings regularly for a global audience. Taking an interdisciplinary approach, Ifri brings together political and economic decision-makers, researchers and internationally renowned experts to animate its debate and research activities.



ISBN: 979-10-373-0525-1



Cover: U.S. President Joe Biden holding a semiconductor during a speech, February 2021 © Shutterstock.com

**How to cite this publication:**
Mathilde Velliet, "Convince and Coerce: U.S. Interference in Technology Exchanges Between its Allies and China", *Étude de l'Ifri*, Ifri, February 2022.

**Ifri**

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tel.: +33 (0)1 40 61 60 00 – Fax: +33 (0)1 40 61 60 60

Email: accueil@ifri.org

**Website:** Ifri.org

# Author

**Mathilde Velliet** is a researcher in Ifri's Geopolitics of Technology program, which she joined in September 2021. Her work focuses on international issues connected to new technologies, and in particular American and Chinese technology policy and Sino-American relations.

Mathilde Velliet is pursuing a PhD in American civilization at the University of Paris: her research analyzes how the Obama and Trump administrations crafted policy for the protection of strategic technologies.

She holds a Master's degree in English Studies from the École Normale Supérieure in Lyon and a Master's in International Security from Sciences Po Paris, and has completed two research stays in the United States, at New York University and Boston University.

# Résumé

La politique de fermeté envers la Chine adoptée par les administrations Trump et Biden a – et aura de plus en plus – des conséquences importantes pour les alliés de Washington sur le plan technologique, tant dans leurs choix en matière d'infrastructures que dans leurs échanges commerciaux avec la Chine. En effet, l'objectif américain de ralentissement du développement technologique chinois se décline en multiples politiques, visant en priorité la Chine mais aussi – directement ou indirectement – les pays partenaires des États-Unis.

D'une part, Washington déploie une panoplie d'outils coercitifs et incitatifs afin d'empêcher l'adoption par les alliés de certaines technologies, fournies par des entreprises chinoises et jugées non fiables (sur le plan cyber, des données ou de sécurité des infrastructures). Les cas d'étude des efforts américains contre le déploiement de la 5G de Huawei ou des câbles sous-marins d'Hengtong Group révèlent une stratégie semblable, combinant pression diplomatique directe, campagne de « sensibilisation aux menaces » et incitations financières.

D'autre part, dans la continuité de l'utilisation historique par les États-Unis de leur position de superpuissance économique et de l'extraterritorialité de leur droit pour influer sur les décisions de leurs alliés, Washington s'emploie à restreindre les transferts de technologies jugées critiques des alliés vers la Chine. Principaux fabricants (avec les États-Unis) de ces technologies, les alliés sont de plus en plus contraints par ces restrictions juridiques et diplomatiques, qui s'appliquent à des échanges avec un partenaire commercial majeur, et dont le périmètre tend à s'étendre au-delà des technologies militaires ou de pointe. Par exemple, afin de limiter les ventes d'équipements de fabrication des semi-conducteurs, les autorités américaines conjugent modification de leur régime de contrôle des exportations et efforts diplomatiques – en bilatéral et multilatéral – pour persuader les alliés d'aligner leurs propres politiques en la matière sur celles des États-Unis.

Si l'administration Biden accorde davantage d'importance aux démarches coopératives et incitatives, il semble probable que la stratégie multidimensionnelle américaine au service de ces deux objectifs se poursuive, voire se renforce. Cette tendance a favorisé une prise de conscience en Europe à la fois des défis sécuritaires posés par certaines technologies proposées par des fournisseurs chinois, mais aussi des risques associés aux pratiques coercitives croissantes des grandes puissances, posant la question de la réponse des alliés à cette politique américaine.

# Abstract

The tough-on-China policy adopted by the Trump and Biden administrations has – and will increasingly have – important consequences for Washington's allies, both on their infrastructure choices and on their technological exchanges with China. Indeed, the U.S. objective of slowing down China's technological development has been translated into multiple policies, primarily targeting China but also – directly or indirectly – U.S. partners.

On the one hand, Washington deploys a range of coercive and incentive tools to prevent its allies from adopting certain technologies, supplied by Chinese companies and "untrusted" by American authorities (in terms of cyber, data or infrastructure security). Case studies of U.S. efforts against the deployment of Huawei's 5G or Hengtong Group's undersea cables reveal a similar strategy, combining direct diplomatic pressure, a threat awareness campaign, and financial incentives.

On the other hand, in line with the United States' historical use of the extraterritoriality of its law and its position as an economic superpower to influence its allies' decisions, Washington seeks to restrict transfers of critical technologies from allies to China. As the main manufacturers (along with the United States) of these technologies, American allies are increasingly constrained by these legal and diplomatic restrictions, which target one of their main trading partner and tend to extend beyond strictly military or cutting-edge technologies. For example, in order to limit sales of semiconductor manufacturing equipment, U.S. authorities are combining changes to the American export control regime with diplomatic efforts (bilaterally and multilaterally) to persuade allies to align their own export policies with those of the United States.

While the Biden administration appears to be placing greater emphasis on cooperative and incentive approaches, it seems likely that the multidimensional U.S. strategy serving these two objectives will continue, and even be strengthened. Among allies (and especially in Europe), this trend has raised awareness of the security challenges posed by certain Chinese suppliers, but also of the risks associated with the growing coercive practices of the great powers.

# Table of Contents

# Introduction

One year after Joe Biden's accession to the presidency of the United States, the hard-line stance initiated by his predecessor towards the People's Republic of China (PRC) continues to be upheld. From a technological standpoint, this has major consequences – and increasingly so – for Washington's allies, Europe in particular, both for their infrastructure decisions and their trade with China.

U.S. technology policy towards China has two main objectives:

- "running faster" by promoting investment into research and development for emerging technologies and their integration into the defense sector;
- make competitors "run more slowly" by implementing import and export controls, sanctions, and other obstacles to the acquisition (legal or otherwise) of certain technologies.[1]

These two objectives are reflected in multiple policies, primarily aimed at China but also directly or indirectly at the United States' partner countries. This dual approach, as it applies to U.S. allies, is reflected in a renewed commitment to scientific and technological cooperation (joint R&D efforts for certain technologies, joint infrastructure projects, cooperation on international standards…) in order to "maintain U.S. and allied leadership" in these fields.[2] Washington simultaneously works to slow China's pace by preventing allies from adopting certain technologies deemed unreliable (in terms of cyber, data or infrastructure security) and from transferring critical technologies to China, officially to avoid their contributing to human rights violations and Chinese military power. This study focuses on this second obstructive component, for which the United States employs a wide range of diplomatic, legal, economic and security measures.

The United States' use of its position as an economic superpower and of the extraterritoriality of its law to influence its allies' decisions is neither a new phenomenon nor limited to its competition with China. In recent decades, there have been many instances of secondary sanctions and re-export controls being used to accentuate the multilateral nature of U.S. measures against, for example, the Soviet Union (and, less drastically, contemporary Russia) or Iran.[3]

---

1. Described for example in C. Ford, "Four Years of Innovation and Continuity in U.S. Policy: Arms Control and International Security Since January 2017", *Arms Control and International Security Papers*, Vol. 1, No. 25, January 8, 2021.
2. This is one of the objectives attributed to the Trade and Technology Council according to the U.S. Commerce Department: International Trade Administration, "U.S.-EU Trade and Technology Council", June 2021, available at: www.trade.gov.
3. S. Marineau, « Sanctions secondaires américaines : du vieux vin dans des outres neuves ?", *Politique étrangère*, Vol. 86, No. 3, Fall 2021.

U.S. policies implemented since the Trump administration, however, are of particular importance to U.S. allies. The restrictions imposed by the United States as part of its strategic competition with China, in contrast to those imposed on the USSR during the Cold War or, more recently, on Iran after the U.S. withdrawal from the Vienna agreement, are now aimed at one of its allies' major trading partners. They therefore have a significant impact on technological exchanges between China and its allies, in both directions.

First, in recent years, U.S. authorities have begun focusing more on imports and investments *from* China. In the United States, this was exemplified by the investment control mechanism reform passed by Congress in 2018,[4] and the 2019, 2020, and 2021 presidential executive orders prohibiting U.S. companies from using power and telecom network equipment manufactured by firms deemed "national security risks", such as Huawei or ZTE.[5] The first part of this study examines how this U.S. focus on Chinese technology acquisitions and imports has manifested as an intensive campaign directed at allies to "raise awareness of the threat" and prevent the adoption of these technologies, in particular regarding 5G and undersea cables.

The second part details the means the United States has employed to restrict technology transfers from allies *to* the PRC. U.S. controls on exports and re-exports to China – which have existed since the 1950s but evolved significantly since then – have been tightened in some sectors under the Trump and Biden presidencies, and reach far beyond the field of advanced military technologies. They are coupled with a diplomatic effort to prevent certain specific transfers, and more broadly to strengthen multilateral and national export control systems. The expansion of the fields and technologies identified as strategic – and therefore subject to restrictions – by the United States and the dual use (civilian and military) of these technologies explains the wide range of sectors likely to be affected. The example of semiconductors (detailed in this study) illustrates this perfectly: used in military, but also automotive and communication equipment (among others), these chips are manufactured with the help of machines whose export to China the United States increasingly seeks to control.

Joe Biden's accession to power led to a certain change in tone – less aggressive, more cooperative – from the American administration towards its allies. This reflects its desire to resolve certain transatlantic trade disputes in

4. The Foreign Investment Risk Review Modernization Act (FIRRMA) expanded the powers of the Committee on Foreign Investment in the United States (CFIUS) to block acquisitions based on national security considerations. Several acquisitions of American companies by Chinese companies have since been blocked.

5. See, for example, the following Presidential Executive Orders: Executive Order 13873 of May 15, 2019, Executive Order 13920 of May 1, 2020, Executive Order 14034 of June 9, 2021. For an analysis of the use of executive orders by Presidents Trump and Biden in the campaign against Huawei, see J. Sherman, "The U.S. Is Continuing Its Campaign against Huawei", *Lawfare*, July 20, 2021, available at: www.lawfareblog.com. For a complete timeline of executive actions directed at China from 2017 to 2021, see U.S.-China Economic and Security Review Commission, *Timeline of Executive Actions on China* (2017–2021), April 1, 2021, available at: www.uscc.gov.

order to focus on China,[6] as it has resumed its involvement in the multilateral and plurilateral structures which had been disregarded under the Trump presidency. Beyond these differences in approach, however, the Biden administration's technology policies remain aligned with those of his predecessor, for two main reasons. First, Biden's policies can hardly be fully appreciated only one year into his presidency, as public consultations, reports and legislative work take time, as do staff appointments. Alan Estevez, Biden's nominee for undersecretary of commerce for industry and security – a key position for export control towards China – is still not in office as his nomination has not been confirmed by the Senate.

But most importantly, the assessment of the threat posed by China to U.S. technological supremacy and national security is widely shared by the entire U.S. political elite, both in the executive branch and in Congress. The Biden administration's change in approach therefore only intends to better address the same objectives as the Trump administration.[7]

6. As illustrated by the June 2021 U.S.-EU Understanding on a Cooperative Framework for Large Civil Aircraft, which resolves the long-standing dispute between Boeing and Airbus and suspends US and European tariffs, while strengthening transatlantic cooperation to "address the challenge posed by non-market economies" (implicitly aimed at China).

7. As Julien Nocetti writes, "the United States' political and financial reinvestment in multilateral institutions and agreements [...] is conditional on Europeans aligning themselves behind U.S. policy toward China – in particular with regard to decoupling in strategic technological sectors". See J. Nocetti, "L'Europe reste-t-elle une 'colonie numérique' des États-Unis ?", *Politique étrangère,* Vol. 86, No. 3, Fall 2021, p. 61.

# "Securing Networks": Preventing the Adoption of Untrusted Chinese Technologies

In addition to measures taken to secure networks on their own territory, U.S. authorities have deployed a variety of measures to prevent U.S. allies from adopting Chinese technologies they regard as unsafe. These measures fall into three main modes of action through which Washington seeks to coerce, convince or incite its allies, which we can define as follows:

- *Coerce*: alter the cost-benefit analysis of adopting Chinese technologies for allies by threatening to impose heavy additional political, economic, or security costs (threat of degraded relationship, limited intelligence sharing, or restricted access to certain U.S. products…);
- *Convince*: attempt to have allies espouse the U.S. analysis of the risks associated with these Chinese technologies through a media and diplomatic threat awareness campaign, training efforts, sharing intelligence on said risks, etc.
- *Incite*: alter the cost-benefit analysis of adopting non-Chinese technologies regarded as safer by offering conditional development assistance, loans, and access to certain funds dedicated to the acquisition of these technologies.

These three strategies have been used together by the Trump and Biden administrations in the U.S. "network security" campaign, particularly for 5G and undersea cable infrastructure.

## A Comprehensive Campaign against Huawei's 5G

President Trump's hard-line stance toward U.S. allies over Chinese equipment manufacturer Huawei's 5G services made it a high-profile case study. Mixing arguments over security risks with a nationalist rhetoric – Donald Trump declared in 2019 "the race to 5G is a race America must win"[8] – the United States has expended a great deal of effort since 2018 to dissuade its allies from integrating Huawei's 5G systems into their telecom

8. J. Barnes and D. Sanger, "Trump Announces 5G Plan as White House Weighs Banning Huawei", *The New York Times*, April 13, 2019.

infrastructures, despite Huawei's inferior costs compared to those of competitors like Nokia or Eriksson.

## *A Primarily Coercive Approach*

For most of Donald Trump's time in office, the U.S. was quite aggressive in pursuing the cancellation of Huawei's nearly 100 5G deals around the world. As Keith Krach, the former U.S. undersecretary of state in charge of the Trump administration's efforts to convince countries to divest from Chinese actors, has explained, "the United States was literally going around the world and pounding on the table and saying, don't buy Huawei".[9] With Congressional support, the U.S. administration thus exerted considerable pressure on its allies, as illustrated by the threatening rhetoric used by members of Congress like Senator Lindsey Graham, who asserted in early 2020, "we are very firm in our commitment, Republicans and Democrats, that if you go down the Huawei road, you're going to burn a lot of bridges"[10]. The U.S.'s diplomatic campaign also drew on more specific threats: U.S. officials repeatedly stressed that countries relying on Chinese suppliers for their 5G infrastructure would undermine U.S. confidence in the reliability of their communications networks, and lead the United States to curtail its intelligence sharing with them. During a trip to Europe in May 2019, for example, Secretary of State Mike Pompeo told reporters that "[There is] a risk we will have to change our behavior in light of the fact that we can't permit data on private citizens or data on national security to go across networks that we don't have confidence [in]".[11] Similarly, Mark Esper, Secretary of Defense, said at the Munich Security Conference in February 2020 that European countries' use of Huawei technology would jeopardize the future of the North Atlantic Treaty Organization (NATO) and intelligence cooperation.[12] This rhetoric was widely used outside of media appearances by government officials, at multiple levels of the executive branch,[13] and in legislative proposals by members of Congress.[14]

9. "Transcript: The Path Forward: Safeguarding Global Innovation with Keith J. Krach & Gen. Stanley A. McChrystal", *Washington Post Live*, April 22, 2021, available at: www.washingtonpost.com.
10. G. Moulson, "Nancy Pelosi Urges Countries to Steer Clear of Huawei for 5G", *PBS News Hour*, February 14, 2020.
11. D. Brunnstrom, "Pompeo Tells Germany: Use Huawei and Lose Access to Our Data", *Reuters*, May 31, 2019.
12. P. Wintour, "US Defence Secretary Warns Huawei 5G Will Put Alliances at Risk", *The Guardian*, February 15, 2020.
13. See for example R. Strayer, "LiveAtState with Economic and Business Affairs Bureau Deputy Assistant Secretary Robert Strayer", April 29, 2019, available at: https://2017-2021.state.gov.
14. "Cotton Introduces Bill Banning Intelligence Sharing with Countries Using Huawei", January 8, 2020, available at: www.cotton.senate.gov.

## *"Educating" Allied Governments*

In addition to this strategy of coercion, U.S. authorities have also tried to persuade their allies of the risks posed by Chinese 5G providers, justifying the need for their complete exclusion from networks. This "global campaign…to start educating" U.S. allies on 5G – in the words of Deputy Assistant Secretary of State Robert Strayer[15] – emphasizes the cybersecurity risks (backdoors, espionage, data compromise) and the prospect of providers being controlled by a foreign government, citing a Chinese law that since 2017 requires companies to comply with requests from Chinese intelligence agencies.[16] Official State Department documents detail these diplomatic efforts, led in particular by the Bureau of International Security and Nonproliferation, "in drawing attention to the security threats associated with PRC colonization of 5G telecommunications markets worldwide."[17] In dealing with allies, the British and German in particular, this included sharing classified intelligence and declassifying information which bolstered the American position.[18] The Biden administration, for whom the issue of 5G security remains a "high priority", has mobilized new resources in service of the same goal, offering workshops and training for foreign policymakers and regulators, as well as booklets containing case studies describing how other allies have implemented restrictions against Huawei.[19]

Bilaterally, this persuasion effort has resulted in joint statements and memoranda signed between the United States and a number of countries, cautioning against the risk of "foreign government control [of providers]" and emphasizing the need to "transition from untrusted [5G] network hardware and software suppliers".[20] The list of signatory countries reveals Washington's particular focus on Eastern Europe, a favored submarket for Chinese equipment manufacturers but one that is highly receptive to security cooperation with the United States: from 2019 to January 2021, Poland, Estonia, the Czech Republic, Slovenia, Lithuania, Kosovo, Slovakia, Northern Macedonia, Bulgaria, and Georgia have issued such joint statements. This U.S.

15. R. Strayer, "Press Briefing with Deputy Assistant Secretary Robert Strayer", October 15, 2019, available at: https://2017-2021.state.gov.
16. For a detailed discussion of American argumentation as "rhetorical coercion", see M. Corcoral, "Omniprésence sans omnipotence : la puissance américaine contre Huawei à l'heure de la 5G", *Conflits, crimes et régulations dans le cyberespace*, ISTE Éditions, 2021, p. 115-143.
17. C. Ford, "Four Years of Innovation and Continuity in U.S. Policy", *op. cit.*
18. B. Pancevski, "U.S. Officials Say Huawei Can Covertly Access Telecom Networks", *The Wall Street Journal*, February 12, 2020.
19. According to Stephen Anderson, in charge of telecom and technology outreach efforts since January 2021, as quoted in D. Hinshaw and S. Woo, "U.S. Fight against Chinese 5G Efforts Shifts from Threats to Incentives", *The Wall Street Journal*, June 14, 2021.
20. See for example the text of the joint statements between the United States and Estonia, Lithuania, Kosovo, Northern Macedonia, and Georgia on the archived Trump administration State Department website: https://2017-2021.state.gov. The texts of the other statements are available on the *American Presidency Project* website for the statement with Poland (www.presidency.ucsb.edu) and on the websites of the U.S. embassies in Estonia, Georgia, and the Czech Republic (https://ee.usembassy.gov/, https://ge.usembassy.gov, and https://cz.usembassy.gov).

effort has continued during the Biden administration and extends beyond Europe, as evidenced by the joint statement by the U.S. President and Japanese Prime Minister asserting their commitment to open and secure 5G networks based on trusted providers.[21]

## *Multilateral Initiatives*

These bilateral commitments contribute to the various multilateral initiatives Washington is working to rally its partners around, such as the Prague 5G Security Conference and the *Clean Network*.

With U.S. support, the first Prague Conference brought together participants from 32 countries (including France and many European countries) and 4 network operators in May 2019. It concluded with the presentation of recommendations on cybersecurity issues surrounding the deployment of 5G, the Prague Proposals, largely reflecting U.S. concerns.[22] While these proposals do not directly mention the PRC, Mike Pompeo's speech at the 2020 Prague Conference left no doubt as to their intended target: "the threats posed by the Chinese Communist Party and its technology companies".[23] At the November 2021 session, the United States, represented by Emily Horne (spokesperson for the National Security Council), reiterated its support for this conference and its new recommendations on telecom provider diversity and emerging and disruptive technologies.[24]

21. "U.S. – Japan Global Partnership For A New Era", Joint statement by the United States and Japan, April 16, 2021, available at: www.whitehouse.gov.
22. "The Prague Proposals: The Chairman Statement on Cyber Security of Communication Networks in a Globally Digitalized World", Prague 5G Security Conference, May 3, 2019, available at: www.vlada.cz.
23. M. Pompeo, "Secretary Pompeo's Video Remarks at the Prague 5G Security Conference 2020", Sepember 23, 2020, available at: https://2017-2021.state.gov.
24. "The Prague Proposals: The Chairman Statement on Telecommunications Supplier Diversity", Prague 5G Security Conference, November 30, 2021; "The Prague Proposals: The Chairman Statement on Cyber Security of Emerging and Disruptive Technologies", Prague 5G Security Conference, December 1, 2021, available at: www.nukib.cz.

**Participants Attending the Prague 5G Security Conference in May 2019**


*Source: website of the government of the Czech Republic, www.vlada.cz.*

To encourage the implementation of the Prague Proposals internationally (and network security more broadly), the United States launched the Clean Network in August 2020. This rather vague term refers to the Trump administration's approach to building a "coalition of trusted partners" that have adopted "digital trust standards". Organized into a series of "lines of effort" (Clean Carrier for telecom networks, Clean Cloud, Clean Cable…), the Clean Network includes both countries – which have signed joint declarations with the United States or adopted their own measures, such as the European Toolbox for 5G – and telecom companies which have eschewed Chinese technologies.[25] In November 2020, the Trump administration announced that 53 countries and 180 companies had joined the Clean Network.[26] While the Trump administration seemed quite quick to tout the inclusion of countries that had simply developed their own 5G cybersecurity measures, European Commissioner Thierry Breton and Undersecretary of State Keith Krach did point out the "synergies" between the European Union's (EU) 5G Toolbox and

25. Keith Krach, in charge of the Clean Network during the Trump administration, cites the following "clean telcos" as examples: Oracle, HP, Reliance Jio, NEC, Fujitsu, Rakuten, Cisco, SoftBank, VMware…
26. U.S. Department of State, "The Clean Network", available at https://2017-2021.state.gov.

the Clean Network.[27] While the Biden administration has not yet elucidated its position on the Clean Network, the emphasis this approach places on ideas of alliance and trust between countries sharing the same democratic values is very much in line with the new administration's policy – as Keith Krach himself has pointed out.[28]

## *Emerging Incentives*

Finally, these strategies to coerce and persuade U.S. allies not to use Chinese suppliers in 5G deployment are paired with new incentives, which first emerged at the very end of the Trump administration but are being further developed under Biden. Unlike his predecessor, a staunch America First advocate, President Biden has emphasized his willingness to advance funding and development assistance to provide a concrete alternative to China's Belt and Road Initiative. The first months of the Democratic presidency have already illustrated this with the G7 agreement in early June on the Build Back Better World (B3W) initiative, the international component of Biden's infrastructure plan, which includes a technology component.[29]

This presidential resolve, in conjunction with bipartisan concerns about the might of Chinese companies in the telecom sector, has resulted in legislative initiatives to incentivize the adoption of non-Chinese 5G infrastructure. One example is the Multilateral Telecommunications Security Fund, established by Section 9202 of the National Defense Authorization Act for Fiscal Year 2021.[30] The fund "should leverage United States funding in order to secure commitments and contributions from trusted foreign partners such as the United Kingdom, Canada, Australia, New Zealand, and Japan" and has three main objectives: advancing R&D of secure and trusted communications technologies, strengthening (telecommunication) supply chains, and "promoting the use of trusted vendors". While the budget for this fund and programs funded are as yet unknown, its very existence is indicative of both the U.S. desire to promote non-Chinese alternatives around the world and to involve its close allies (in this case, the Five Eyes) in this effort.[31]

27. "Meeting Between U.S. under Secretary of State Krach and Commissioner Breton on Secure Telecommunications Infrastructure and Digital Agenda", September 30, 2020, available at: https://ec.europa.eu.
28. "Transcript: The Path Forward", *op. cit.* On the pertinence of the *Clean Network*'s core principles under the Biden administration, see M. Kuo, "'Clean Network' in the US-China Tech Race: Insights from James Andrew Lewis", *The Diplomat*, March 1, 2021, available at: https://thediplomat.com.
29. S. Holland and G. Faulconbridge, "G7 Rivals China with Grand Infrastructure Plan", Reuters, June 13, 2021.
30. 116th U.S. Congress, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, H.R.6395, January 1, 2021, available at: www.congress.gov.
31. This is especially notable because in January 2020 the UK government allowed Huawei to participate (at 35%) in the construction of the country's non-strategic 5G infrastructure, but when faced with the U.S. pressure described above, it reversed course in May 2020 and announced a ban on the purchase of new

Congress is also considering other bills that offer financial incentives: the Transatlantic Telecommunications Security Act, introduced in September 2021, would, for example, allow Central and Eastern European countries to receive aid (normally reserved for developing countries) to fund the removal of Chinese telecom equipment and deployment of "secure"[32] equipment.

Thus, moving past the initially confusing and contradictory rhetoric of the Trump administration,[33] the United States has deployed a multi-faceted strategy in recent years to coerce, convince, and incentivize its allies to keep Chinese equipment manufacturers out of their 5G networks. Together with the internal dynamics of each state, it appears to have been effective in raising awareness of the risks associated with this technology: most of the United States' closest allies have banned (as is the case in Japan, Australia and the United Kingdom) or restricted Huawei's access to their telecommunications networks. After some initial reluctance, the U.S. insistence has also changed the perspective of many E.U. decision-makers on the need to develop European tools to assess, beyond the commercial dimension, the risks of dependency and vulnerabilities within their telecom network.[34] American efforts in Asia, including pressure on certain allies (South Korea, Thailand, the Philippines) or in the context of multilateral dialogues (e.g., the ASEAN-U.S. dialogue on cyber policy) have not, however, resulted in the adoption of restrictive requirements regarding equipment manufacturer origin.[35]

Huawei equipment starting at the end of 2020 and a requirement to remove existing equipment by 2027. And as of the end of December 2021, Canada had still not formalized its decision on whether to allow Huawei's 5G in the country.

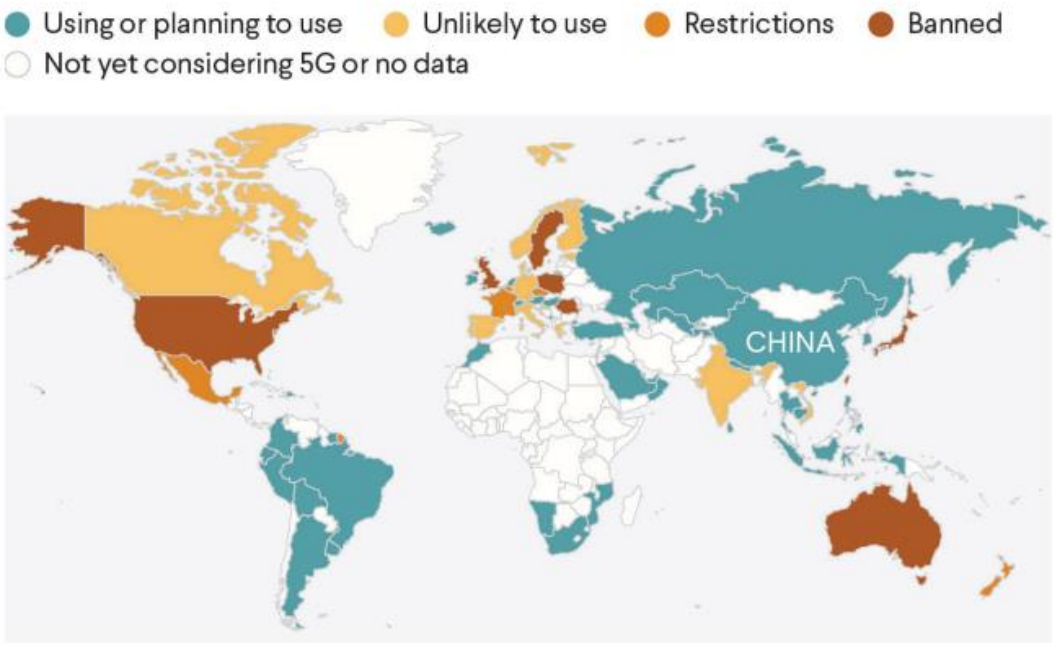
32. 117th Congress, Transatlantic Telecommunications Security Act, S.2876, introduced in the Senate on September 28, 2021, available at: www.congress.gov.

33. J. Sherman and R. Morgus, "The Confused U.S. Messaging Campaign on Huawei", *Lawfare*, June 25, 2019

34. L. Cerulus, "Cracks Appear in West's 5G Strategy after Huawei", *Politico*, November 30, 2021; L. Nardon and S. Rust, "États-Unis/Europe : sept enjeux du numérique", *Potomac Paper,* No. 42, Ifri, July 2021, p. 18-22.

35. M. Corcoral, "Omniprésence sans omnipotence: la puissance américaine contre Huawei à l'heure de la 5G", *op. cit.*

**Official Approaches to Using Huawei Equipment in 5G Networks**




*Source: J. Hillman and D. Sacks, "China's Belt and Road: Implications for the United States", Independent Task Force Report, No. 79, Council on Foreign Relations, March 2021.*

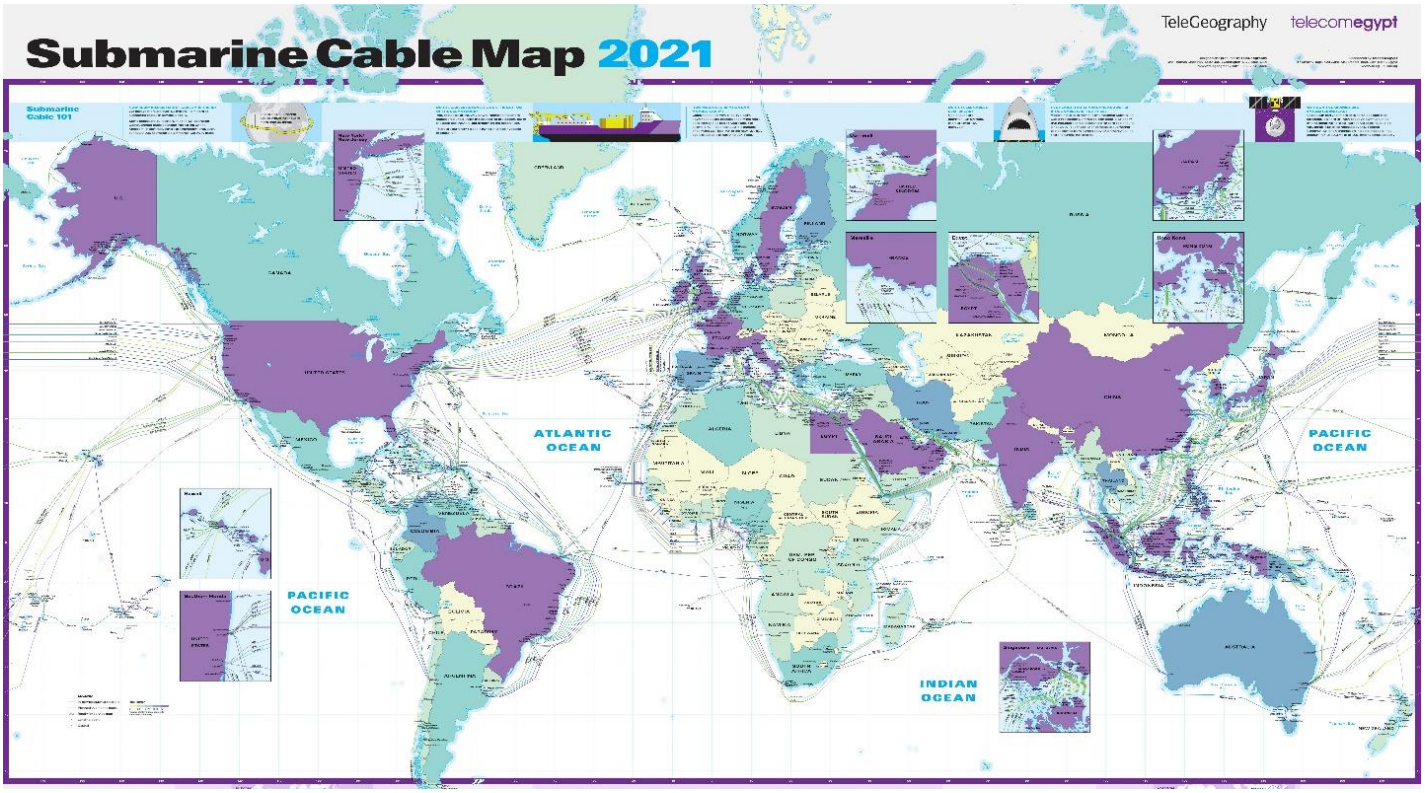
## The Issue of Undersea Cables

The international expression of the "national emergency" declared by the United States to secure its networks has led to the application of a multitude of tools, demonstrating the U.S.'s unmatched aptitude to set the agenda for its top priorities. This objective – and the U.S. pressure on its allies to achieve it – extends beyond the high-profile case study of 5G to other telecom infrastructure, including undersea cables.

The 475 cables running across the ocean floor are critical infrastructure through which more than 95% of intercontinental Internet traffic flows.[36] The explosive growth of cloud services, increasing the volume and sensitivity of data moving through these cables, and the emergence of new actors (including from China) in the construction and operation of these cables, have increased the risks and political scrutiny associated with this infrastructure.

36. J. Sherman, *Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security*, Atlantic Council, September 2021.

## Map of Undersea Cables in 2021




*Source: Telegeography, 2021.*

The United States worries about the growing importance of Chinese companies – in particular Hengtong Group and its subsidiaries Hengtong Marine and Huawei Marine[37] – in investment, but especially in the construction, ownership and operation of undersea cables. These companies, backed by the state as part of China's Digital Silk Road, are beginning to compete with the major established players: SubCom (United States), Alcatel Submarine Networks (a French company owned by the Finnish group Nokia) and NEC (Japan). U.S. concerns about this development, which Congress and the administration share, are threefold.

First, the U.S. cites cybersecurity risks, data compromise and the use of cables for intelligence gathering.[38] A bipartisan Senate report warns of the possibility of the cables being hacked to monitor or intercept data, or deny

37. Accused by Washington of being closely linked to the Chinese Communist Party (CCP) and in order to avoid any political setbacks, Huawei sold its shares (51%) of Huawei Marine to Hengtong Optic-Electric as early as 2019. Hengtong's founder's ties to the Chinese military and government and the presence of Huawei Tech Investment among the group's shareholders, however, make it unlikely for this to inspire any trust from the U.S. See the article "Banni des antennes françaises, Huawei dans les starting-blocks pour revenir par les câbles", *Intelligence Online*, No. 862, October 7, 2020.
38. The use of undersea cables for intelligence gathering and espionage has been widely practiced by the Russian, British and especially American services, both historically and more recently, as revealed by Edward Snowden in 2013.

access to the service.[39] The role of Chinese companies in the construction and operation of the cables allegedly facilitates espionage since it provides the opportunity to directly plant hacking equipment during the manufacturing or installation process (rather than needing to install it after the fact).

These companies' positioning also creates a risk of dependence on China for sensitive data transfers, which "could have an impact on U.S. and European security".[40]

Finally, long-term U.S. concerns are that the PRC will use these undersea cables to deploy an underwater network of sensors and other surveillance equipment for use by the Chinese government and the People's Liberation Army (PLA). As with 5G, the U.S. justifies its fears of civil-military collusion by pointing to Chinese companies' strong ties to the Chinese military and government: for example, Hengtong's founder and current director, Cui Genliang, is a former telecom specialist in the PLA and served in the Chinese National People's Congress.

These concerns on the part of the United States have major consequences for Washington's allies, both in Asia and in Europe, and in particular for France, which seeks to establish Marseilles as a connectivity hub, incorporating undersea cable terminals and data centers.

Indeed, while 5G exemplified the desire of the United States to discourage its allies from adopting certain Chinese technologies on their territory, the case of undersea cables shows the pressure imposed on allies to also dissuade them from participating in international infrastructure projects that include Chinese actors.

## *Threat Awareness Diplomacy on Cables*

As with 5G, since late 2019 Washington has been conducting a "threat awareness" campaign regarding these cables consisting of speeches by high-ranking U.S. officials (Pompeo, Krach…) during their international tours, informal meetings with foreign services, and official reports warning against certain cable projects. For instance, the bipartisan report *The United States and Europe: A Concrete Agenda for Transatlantic Cooperation on China*, details the risks involved in the Pakistan East Africa Connecting Europe (PEACE) Cable linking Gwadar and Karachi in Pakistan to Marseille, via Djibouti. Since 2019, the deployment of the PEACE cable – a clear component of the digital arm of the Belt and Road Initiative – is being conducted by a subsidiary of Hengtong (Hengtong Peace Cable International Network), as well as Hong Kong-based operator PCCW Global and France's

39. U.S. Senate Foreign Relations Committee, *The United States and Europe: A Concrete Agenda for Transatlantic Cooperation on China,* November 18, 2020.
40. *Ibid.*

Orange.[41] The latter only retains ownership of data transmission capabilities and not the cable itself, which is the property of Hengtong.[42]

In addition to information and persuasion campaigns, the United States has exerted direct diplomatic pressure on Paris for this project.[43] U.S. officials have engaged in a persistent, multi-ministry lobbying effort, raising the issue on almost every visit and holding multiple interdepartmental meetings (particularly with the French General Secretariat for Defense and National Security).[44] U.S. rhetoric condemning the project revolves around three main points: the cybersecurity risks it entails, the dependence on China it engenders, and the political signal conveyed through the acceptance of a cable owned and manufactured by a Chinese company which still struggles to gain the trust of many states. In addition, because France is effectively the gateway to Europe for U.S.-linked cables, the United States is concerned about how the interconnection between these data flows will be managed.[45]

Despite U.S. pressure, based on an expansive idea of their national interests, the French state has maintained its support for Orange Marine, which has committed to the cable's landing in October 2021: the cable is expected to go live in early 2022. France's persistence can likely be explained by the French president's stated desire to "avoid depending entirely on China, as well as on the United States" in technological matters.[46] Given the impossibility of completely protecting cables from end to end, the French national strategy aims to mitigate certain cyber risks (for example, by favoring landings by French companies) while multiplying cable projects and diversifying entry points.[47] The desire to establish Marseilles as a connectivity hub with the installation of multiple cables – manufactured by a range of companies (ASN, NEC, Subcom, Hengtong) – illustrates this.

## *Funding Non-Chinese Alternatives*

U.S. efforts have been more fruitful in the Indo-Pacific, where Washington has intensified its collaboration with Tokyo and Canberra on the subject of cables in order to counter Chinese influence and offer attractive alternatives. The East Micronesia Cable project, which calls for the construction of an undersea Internet cable to improve the communications network of the islands of Nauru, the Federated States of Micronesia (FSM) and Kiribati, is a case in

41. "Marseille, épicentre européen de la guerre des câbles", *Intelligence Online,* No. 866, December 2, 2020.
42. R. Subtil, "Internet : le câble sous-marin 'PEACE' débouche à Marseille", *La Croix*, October 19, 2021.
43. H. Fouquet, "China's 7,500-Mile Undersea Cable to Europe Fuels Internet Feud", *Bloomberg Businessweek,* March 5, 2021.
44. Author's telephone interview with Camille Morel, PhD in public law and researcher in international relations, February 1, 2022.
45. *Ibid*.
46. E. Macron, "Interview du président Emmanuel Macron au *think tank* américain Atlantic Council", February 5, 2021. Intelligence services' interest in a cable linking France to Africa may also have played a role in the French decision.
47. Author's telephone interview with Camille Morel, *op. cit*.

point. Competing with Alcatel and NEC, Huawei Marine responded to the tender with a very aggressive proposal (almost 20% cheaper than its competitors).[48] However, in late 2020, the United States – which is responsible for the defense of FSM under the Compact of Free Association agreement – expressed, via a diplomatic note to the Micronesian government, its strong strategic concerns about the participation of Chinese firms.[49] Faced with this warning and the impossibility of simply withdrawing Huawei's bid, no contract was awarded at the end of the tender process, resulting in the project's termination in June 2021.[50] Six months later, the United States, Australia and Japan announced a new component of their trilateral cooperation project dedicated to infrastructure in the Indo-Pacific: the funding of a section of cable connecting Kosrae (FSM), Nauru and Kiribati.[51] While its budget has not yet been made public, this announcement illustrates both the priority given by these three members of the Quadrilateral Security Dialogue (Quad) to the issue of undersea cables in the Indo-Pacific, and the U.S. strategy, combining deterrence and incentives.

## *The Expanding Role of American Digital Giants*

An additional indirect form of leverage appears to be emerging for the U.S. administration with the increasing role played by the American digital giants (Facebook, Google, Amazon, Microsoft). The sharp increase in data flow needs of these companies has led them to invest heavily in undersea cables, competing with the telecom operators that were previously dominant in this sector. From less than 10% prior to 2012, content providers' share of total undersea cable capacity was estimated to exceed 65% in 2020.[52] But these digital giants are subject to U.S. regulations, and their cable projects are closely monitored by Team Telecom (which includes representatives from the Pentagon, the Department of Homeland Security and the Department of Justice), which has already forced Google and Facebook to cancel certain cable projects.[53] The growing role of these companies in this sector could therefore encourage companies wishing to partner with these very prominent American giants to align themselves in turn with American regulations.[54]

48. J. Barrett, "U.S. Warns Pacific Islands about Chinese Bid for Undersea Cable Project – Sources", *Reuters*, December 17, 2020.
49. Strategic concerns which were compounded by the fact that the cable was to be connected to the HANTRU-1 cable, which is primarily used by the U.S. government and terminates in Guam.
50. J. Barrett and Y. Lun Tian, "Pacific Undersea Cable Project Sinks after U.S. Warns against Chinese Bid", *Reuters*, June 18, 2021.
51. U.S. Department of State, "Joint Statement on Improving East Micronesia Telecommunications Connectivity", December 11, 2021, available at: www.state.gov.
52. J. Miller, "All About That $8 Billion in Subsea Cable Investment", TeleGeography Blog, June 22, 2021, available at: https://blog.telegeography.com.
53. "Washington prêt à couper tous les câbles sous-marins à Hong Kong : Facebook, premier à s'incliner", *Intelligence Online*, September 14, 2020.
54. Author's telephone interview with Camille Morel, *op. cit.*

To counter China's growing influence in the critical telecommunications sector, the United States has been deploying a multi-faceted campaign since the Trump administration that combines persuasion, coercion and incentives to dissuade Washington's allies from accepting projects involving Chinese suppliers. The campaign's effectiveness has varied: depending on the particularities of each bilateral relationship, of course, but also on the legitimacy conferred to the American approach (perception of underlying American commercial interests, overlap between Sino-American security concerns and technological competition, condemnation of espionage practices that the United States itself employs…). While the multiplicity of its methods (diplomatic, commercial, legal, military) carries a risk of "fragmenting the strategic process", resulting in a lack of coherence and legitimacy, it also reveals the breadth of issues over which U.S. allies will face American pressure as strategic competition intensifies.[55] Especially since in parallel to its efforts to prevent the adoption of these Chinese technologies, the United States seeks to preserve its technological advantage by restricting the transfer of strategic technologies to China from its own territory… and that of its allies.

55. M. Corcoral, "Omniprésence sans omnipotence: la puissance américaine contre Huawei à l'heure de la 5G", *op. cit.*

# "Good Allies Do Not Sell This [...] to China": Preventing Technology Transfers to China

Since the normalization of Sino-American relations in the 1970s, and increasingly since the 1990s, the United States has gradually liberalized many of its export restrictions to China, including those on dual-use technologies and in critical sectors (civil nuclear power, high-performance computing, semiconductors...).[56] In contrast to this general dynamic, and despite the strong economic interdependence between China and the United States, the U.S. has tightened a number of export controls in recent years. These controls target certain sectors considered strategic (such as semiconductors and civil nuclear power) and certain Chinese companies (such as telecom equipment manufacturers Huawei[57] and ZTE, or semiconductor manufacturers Fujian Jinhua Integrated Circuit Co Ltd and SMIC).[58] While the reasons given vary – espionage, intellectual property or human rights violations, trade with countries under U.S. sanctions, etc. - they reveal Washington's intention to prevent U.S. technologies from contributing to China's capacity to threaten American military and technological leadership.

This has major consequences for U.S. allies and partners, whose trade with China is increasingly constrained by American restrictions of varying nature. The United States has thus been able to strengthen controls on exports but also, thanks to the extraterritoriality of U.S. law, those on re-exports, prohibiting allies from transferring certain partially American technologies to China. In addition to this legal tool, the Trump and Biden administrations have deployed a variety of instruments to prevent certain transfers, and more broadly to encourage allies to strengthen their controls on exports to China. An examination of this U.S. strategy shows that it transcends Trump's Sino-American trade war and is likely to result in increasing pressure on allies over the longer term.

56. H. Meijer, *The Making of US Export Control Policy toward the People's Republic of China, Oxford,* Oxford University Press, 2016.
57. For a detailed report of all U.S. legal restrictions applying to Huawei, see S. Mulligan and C. Linebaugh, *Huawei and U.S. Law*, Congressional Research Service, R46693, February 23, 2021.
58. L. Nardon and M. Velliet, "La guerre commerciale sino-américaine: quel bilan à l'issue de la présidence Trump ?", *Potomac Paper*, No. 40, Ifri, November 2020.

# The Extraterritoriality of U.S. Law at work

The different U.S. export control regimes apply primarily to goods located in the United States or of U.S. origin. However, the extraterritoriality of U.S. law allows Washington to prohibit certain transfers of tangible goods (components and systems, for example) or non-tangible goods (software, assistance, technical discussions) from non-U.S. companies to China.

Two U.S. regulations govern the export of sensitive goods from the United States, but also the re-export of so-called "controlled goods" from any country.[59]

The very restrictive International Traffic in Arms Regulations (ITAR), enforced and interpreted by the Department of State, apply to war materials and related items contained in the United States Munitions List (USML). This regime being specific to military goods, it will not be elaborated upon in this study.

The second regulatory framework, the Export Administration Regulations (EAR), controls goods (including dual-use goods) listed in the Commerce Control List (CCL) and is administered by the Commerce Department. Within these regulations, two rules allow the United States to require a license from U.S. authorities for the transfer of technology from any country to China:

- the so-called *de minimis* rule;
- the Foreign-Produced Direct Product Rule (FDPR).

## *The* de minimis *Rule*

Under the *de minimis* rule, any product manufactured abroad by a foreign company is subject to the EAR if the value of "controlled" U.S. components or software exceeds a certain threshold, which is 25% for most countries (including China).[60] For example, a Dutch company wishing to sell advanced semiconductor manufacturing equipment to a Chinese foundry made up of 20% of U.S. (controlled) components – i.e., below the minimum threshold – will be able to do so without seeking a license from U.S. authorities. However, if this device contains a significant amount of U.S. technology (more than 25% of its value), the company will be required to obtain a U.S. license to export it – which licence is unlikely to be granted if the recipient is Chinese.

59. For a French-language summary of these two regimes, see: Secrétariat général de la Défense et de la Sécurité nationale, "Les règlementations américaines de contrôle à l'exportation de biens sensibles", June 2020, available at: www.sgdsn.gouv.fr.
60. Bureau of Industry and Security, "De minimis Rules and Guidelines", November 5, 2019, available at: www.bis.doc.gov.

Under the Trump administration, the Commerce Department proposed reducing the cap to 10 percent – the threshold currently imposed on transfers to Iran, North Korea, Syria and Cuba[61] – for certain Chinese companies like Huawei.[62] A bill to this effect was even introduced in the Senate in February 2020.[63] This proposal was met with an industry outcry, which the Pentagon supported, out of concern for the impact export restrictions could have on the competitiveness and innovation potential of U.S. companies, which are crucial to maintaining U.S. technological and military supremacy.[64] While these two initiatives did not materialize, they reveal a willingness in both branches of government to advocate for drastic unilateral restrictions on foreign technology exports to China.

## *The Foreign Direct Product Rule*

The Foreign Direct Product Rule (FDPR) stipulates that if certain controlled U.S. software or technologies are used to produce a good for certain countries (including China), then that good is subject to the EAR.[65] For example, a semiconductor manufactured abroad by machinery of U.S. origin classified under "national security" (as is almost all U.S. semiconductor manufacturing equipment) will be considered a "direct product" of U.S. technology. It will therefore require a U.S. license to be exported to China.

In keeping with its campaign against Huawei, the U.S. Commerce Department announced in May and August 2020 an expansion of the FDPR to further restrict Huawei's access to technology supplied by foreign manufacturers.[66] Huawei has been listed since 2019 alongside dozens of affiliated companies on the U.S. Entity List, which imposes a licensing requirement for the export, re-export or transfer of goods subject to the EAR. Since the 2020 amendments, these restrictions were coupled with the direct product rule for all technology transfers to Huawei-related companies on the entity list, with no *de minimis* threshold criteria or "national security" classification. Prior to this expansion, a Japanese or European company could, for example, export its goods to Huawei despite its inclusion on the

61. Group E countries. See Bureau of Industry and Security, "License Exceptions: Supplement No. 1 to Part 740", available at: www.bis.doc.gov.
62. A. Alper *et al.*, "Trump Administration Moves toward Blocking More Sales to Huawei: Sources", *Reuters*, January 15, 2020.
63. 116th Congress, Bill S. 3316, February 2020, available at: www.congress.gov.
64. J. Schoff, *U.S.-Japan Technology Policy Coordination: Balancing Technonationalism with a Globalized World*, Carnegie Endowment for International Peace, June 2020, p. 21.
65. The software and technologies covered are those classified as "controlled for national security reasons" and the relevant recipient countries are those in Groups D1 (including China) and E. See General Prohibition 3 in Bureau of Industry and Security, "General Prohibitions: part 736", October 5, 2021, available at: www.bis.doc.gov.
66. Bureau of Industry and Security, "Export Administration Regulations: Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List", *Federal Register*, May 15, 2020; "Addition of Huawei Non-U.S. Affiliates to the Entity List, the Removal of Temporary General License, and Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule)", *Federal Register*, August 17, 2020.

entity list if they were not the direct product of U.S. technology classified under "national security" or if the value of U.S. components did not exceed 25%. The 2020 amendments prohibit these exchanges (by imposing a U.S. licensing requirement).

This unilateral and sudden change in U.S. regulations has a direct impact not only on Huawei but also on companies in allied countries, prompting their objections. Organizations representing the Japanese industry thus sent a letter to the Japanese Ministry of Economy protesting these amendments:

> "The Direct Product rule, which until now had only limited applicability on re-exports[…] was expanded without notice by the [above] amendments. […] As a result, Japanese companies that re-exported products produced using certain U.S. origin equipment and software to Huawei without violating the de minimis rule had to suddenly stop their reexports. […]
>
> Another problem is that EAR stipulates the Direct Product rule which has been expanded to Huawei can apply to other companies and organizations on the Entity List by further amendment of U.S. EAR any time. Even for Japanese companies which are legally dealing with companies listed on the Entity List, there is a possibility that the future trade will be suddenly cut off, which means a situation where predictability and legal stability are sorely lacking."[67]

This last point is a major concern as the list of Chinese entities to which this rule could apply has been steadily expanded in recent years, with recent additions in June, August, and December 2020, as well as January, July and December 2021.[68]

## Leverage Beyond Extraterritoriality: The case of ASML

These rule changes are part of both the U.S. campaign against Huawei and more broadly Washington's strategy to limit Chinese advanced semiconductor manufacturing capabilities. Indeed, they are explicitly intended by the Commerce Department to "narrowly and strategically target Huawei's acquisition of semiconductors".[69] This objective has therefore resulted in the expansion of existing legal tools enabling Washington to prevent both U.S. and non-U.S. companies from selling microchips and their

67. Japan Business Federation *et al.*, "Requests with Regards to the Extraterritorial Application of Chinese and United States Regulations, Focusing on China's Export Control Law and United States' Expanded Direct Product Rule", November 11, 2020, available at: www.cistec.or.jp.
68. Bureau of Industry and Security, "Supplement No. 4 to Part 744 – Entity List", December 17, 2021, available at: www.bis.doc.gov.
69. U.S. Commerce Department, "Commerce Addresses Huawei's Efforts to Undermine Entity List, Restricts Products Designed and Produced with U.S. Technologies", May 15, 2020, available at: https://2017-2021.commerce.gov.

design and production tools (software and hardware) to China. But even when the requirements for the imposition of U.S. licensing requirements on technology transfers to China are not met, the United States still has a number of options to discourage its allies from exporting certain equipment deemed to be strategic.

The case study of the sale by Dutch company Advanced Semiconductor Materials Lithography (ASML) of semiconductor manufacturing equipment to a Chinese company is a perfect demonstration of the deployment and effectiveness of these different tools.

In 2018, one of China's leading semiconductor manufacturers, Semiconductor Manufacturing International Corporation (SMIC), purchased semiconductor manufacturing equipment from ASML that employed state-of-the-art technology: extreme ultraviolet lithography, or EUV.[70] This process, over which ASML has a monopoly, is essential for the manufacture of the most finely engraved chips (7 nanometers and below). In order to prevent China from securing this capacity to produce the most technologically advanced chips, the Trump administration sought to have the sale cancelled. However, the audit conducted by the Commerce Department showed that the value of U.S. components in this equipment did not reach 25%: under the *de minimis* rule, Washington could not directly block the sale by enforcing U.S. re-export law.[71] The Trump administration therefore had to resort to other means – diplomatic, commercial and informational – to coerce and convince the Dutch government not to grant ASML the export license necessary for this sale.

First, the United States exerted heavy diplomatic pressure on the Dutch government, with at least four rounds of negotiations in the year following the sale's announcement and involvement at very high levels: Secretary of State Pompeo urged Prime Minister Rutte himself to block the sale during a visit to the Netherlands in June 2019.[72] Similarly, when Dutch diplomats visited the White House a month later, Charles Kupperman, then deputy national security adviser, explicitly warned them that "good allies do not sell this type of equipment to China".[73] To this diplomatic pressure, Kupperman added a thinly veiled trade threat, pointing out that ASML's machines could not function without certain U.S. components, whose export to the Netherlands the White House could restrict.[74] Besides this coercive approach, as with Huawei's 5G, Washington has also sought to promote its perception of the Chinese threat through intelligence sharing. The U.S. for

70. ASML, "EUV Lithography Systems", available at: www.asml.com.
71. A. Alper *et al.* "Trump Administration Pressed Dutch Hard to Cancel China Chip-Equipment Sale: Sources", *Reuters*, January 6, 2020.
72. *Ibid.*
73. S. Woo and Y. Jie, "China Wants a Chip Machine from the Dutch: The U.S. Said No", *The Wall Street Journal,* June 17, 2021.
74. For example, U.S. company Cymer, acquired by ASML in 2013 but still operating in the U.S., makes some of the lasers used for EUV lithography. See White House Report, *Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth*, June 2021, p. 50.

example shared a classified report with Rutte in July 2019 on the potential impact of China's acquisition of ASML's technologies.[75]

This intense American pressure seems to have borne fruit, since shortly after these exchanges the Dutch government decided not to renew the export license granted to ASML, thereby preventing the delivery of the $150 million machine. ASML's CEO protested this decision, warning that the overuse of export restrictions by governments as part of overall semiconductor leadership strategies could curtail R&D and therefore innovation in the medium term.[76]

On the issue of semiconductors, these industry arguments do not appear to succeed in influencing the U.S. strategy of Chinese technological containment, which the Biden administration has maintained. Indeed, according to U.S. officials, the continued restriction of ASML's business with China is at the top of National Security Advisor Jake Sullivan's list of priorities.[77] The Biden administration even seems to want to go further than only blocking the transfer of the most advanced technologies like EUV equipment. Washington has begun lobbying to prevent ASML from selling argon fluoride (ArF) immersion lithography technologies, used in DUV (deep ultraviolet, less advanced than extreme ultraviolet) machines and for which ASML faces competition from Japan's Nikon,[78] yet the sale of DUV equipment to China is permitted under the multilateral export control regime (the Wassenaar Arrangement), and accounts for nearly 20% of ASML's sales in 2020. The expanded scope of technologies subject to U.S. pressure has led some Dutch politicians to claim that the current administration is "going too far".[79] It carries serious consequences for high-tech companies such as ASML but extends far beyond the most high-tech sectors, given the ubiquitous and growing use of chips manufactured using DUV technology (in 5G, artificial intelligence, data centers, automobiles…).

## Reinforcing Multilateral and National Export Controls

Beyond interventions on specific sales, this development reflects Washington's desire to align the export control systems of its allies (particularly the Netherlands and Japan) with U.S. restrictions.

75. A. Alper *et. al.* "Trump Administration Pressed Dutch Hard to Cancel China Chip-Equipment Sale: Sources", *op. cit.*
76. S. Woo and Y. Jie, "China Wants a Chip Machine from the Dutch. The U.S. Said No", *op. cit.*
77. *Ibid.*
78. E. Witterman, "USA Tries to Prevent All Export of ASML Machines to China", *Techzine*, March 10, 2021.
79. Michiel Hoogeveen, conservative member of the European Parliament, quoted in C. Hetzner, "'Gone Too Far': Meet the Dutch Chips Giant That Silicon Valley Loves and Biden Fears", *Fortune*, October 19, 2021.

## *Building a Multilateral Consensus on New Restrictions…*

Well aware that enforcing restrictions multilaterally makes any attempt at technological containment both much more effective and less burdensome for U.S. firms (who otherwise suffer a competitive disadvantage),[80] the United States is attempting where possible to strengthen the international export control system. Thus, even under the Trump administration, the United States has maintained its involvement in multilateral structures – both old and those newly formed for this purpose. Washington has various means of promoting multilateral export controls,[81] chief among them its participation in the Wassenaar Arrangement. This Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies has 42 members, including the main manufacturers of strategic technologies (United States, Japan, South Korea, Germany, Netherlands, France… but not China). It is not binding for the States Parties, but they commit to controlling exports of goods listed in the Arrangement according to their national legislation. U.S. diplomacy has thus been pushing for the expansion of this list, leading to the adoption of new controls on six specific technologies (including software designed for EUV lithography, as well as finishing technologies essential to the production of 5-nanometer wafers)[82] by consensus at the December 2019 plenary.[83] These additions to the Wassenaar list were translated into U.S. domestic legislation by the Commerce Department's publication of new controls on these technologies in October 2020. The long delay between the Commerce Department's first public consultations on emerging technologies to be controlled, in late 2018, and the actual adoption of these controls two years later reveals that Washington prioritizes the multilateral implementation of restrictions over the speed of their enforcement, despite pressure from Congress.[84]

In addition to this traditional multilateral forum, the United States has deployed dedicated initiatives to address the "pervasive and systematic technology transfer threats" posed by countries like China.[85] The U.S. State Department, for example, has organized three editions (2018, 2019, and

80. J. Pelter, "Testimony Before the U.S.-China Economic and Security Review Commission", September 8, 2021, p. 9, available at: www.uscc.gov.
81. See the list of the main multilateral regimes for the control of dual-use goods and technologies on the France Diplomatie website, "Contrôle des biens et technologies sensibles à double usage", February 2020, available at: www.diplomatie.gouv.fr.
82. "2020 Year-End Sanctions and Export Controls Update", February 5, 2021, *Gibson Dunn*, available at: www.gibsondunn.com.
83. The 2020 plenary did not take place because of the pandemic. The list adopted following the December 2021 meeting includes some additions, including computer-aided design (CAD) software useful in the design and production of integrated circuits. See Wassenaar Arrangement Secretariat, *List of Dual-Use Goods and Technologies and Munitions List,* December 2021, available at: www.wassenaar.org.
84. "New Controls on Emerging Technologies Released, While U.S. Commerce Department Comes Under Fire for Delay", *Gibson Dunn*, October 27, 2020, available at: www.gibsondunn.com.
85. C. Ford, "Technology Transfer Diplomacy and the Challenge of Our Times", State Department archive, September 15, 2020, available at: https://2017-2021.state.gov.

2020) of the Multilateral Action on Sensitive Technologies (MAST) conference, with the goal of improving coordination among some 15 countries on common technology transfer concerns. This multilateralist component of U.S. "technology security diplomacy" aims to build "coalitions of caution" to slow China's acquisition of sensitive technologies.[86]

More recently, the creation of the Trade and Technology Council – which brought together EU and U.S. leaders for its first session on September 29, 2021 – has dedicated a working group to transatlantic discussions on export control cooperation (including dual-use technologies).

As with 5G, the United States also employs international cooperation measures – including financial – that incentivize rather than coerce: for example, Congress voted in the major defense budget bill for fiscal year 2021 to establish a Multilateral Semiconductor Security Fund.[87] This fund is meant to support secure semiconductor development and supply chains and is only available to countries that "maintain export control licensing policies on semiconductor technology substantively equivalent to the United States with respect to restrictions on such exports to the People's Republic of China",[88] thus creating some incentive to align with U.S. regulations.

## ...or Directly Pressuring Countries Producing Key Technologies?

Given the inherent difficulties of this multilateral approach (the slowness and complexity of building consensus, the non-binding nature of decisions...), Washington is simultaneously pursuing a strategy aimed directly at certain countries where key technologies are produced to encourage them to tighten their national controls on exports to China. These bilateral efforts have been a constant in U.S. diplomacy since Washington implemented export restrictions on the PRC, when the regime first came into being. As early as 1952, Washington made any future American assistance conditional on the signing of a bilateral agreement imposing severe restrictions on Japanese exports of "all commodities on international control lists [and] all items on U.S. security lists" (among others), which the Japanese were forced to accept.[89] Even after the normalization of U.S. relations, and even in the 21st century, there is no shortage of such examples. In the early 2000s, under U.S. pressure, Israel cancelled lucrative contracts

86. *Ibid.* See also N. Barkin, "Export Controls and the U.S.-China Tech War: Policy Challenges for Europe", *China Monitor,* Mercator Institute for China Studies, March 18, 2020 ; A. Imbrie *et al.*, *Agile Alliances: How the United States and Its Allies Can Deliver a Democratic Way of AI,* Center for Security and Emerging Technology, February 2020, p. 61.
87. 116th United States Congress, *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*, *op. cit.*
88. *Ibid.*
89. J. Dover, *Empire and Aftermath: Yoshida Shigeru and the Japanese Experience, 1878-1954,* Cambridge (MA), Harvard University Press, 1979, p. 400-414; R. Foot, *The Practice of Power: U.S. Relations with China since 1949*, Oxford, Clarendon Press, 1995, p. 57.

with China (on Phalcon Airborne Early Warning (AEW) Systems, and for the modernization of 100 Harpy drones), signed a statement of understanding with the United States in 2005, tightened its export control system for defense articles, and created one for dual-use articles. At the request of the U.S. diplomacy, Israel is also strengthening the role of the Ministry of Foreign Affairs on the issue of export control.[90]

In this respect, current U.S. endeavors do not represent a major departure from past practices. However, China's growing importance as a trading partner and the expanding range of technologies that Washington wants to restrict are making this strategy increasingly burdensome for allies. The United States has conducted numerous bilateral negotiations with countries (often allies) producing technologies it deems strategic to encourage them to strengthen their controls towards China, as illustrated by the example of ASML. In his review of the four Trump years, former Under Secretary of State for Arms Control and International Security Christopher Ford, for example, praised efforts to leverage "programs [...] to help U.S. partners develop and implement 'best practices' [...] in order to] apply them also in ways that serve U.S. national security interests in the arena of great power competition".[91] It is very likely this U.S. strategy will continue, as the National Security Commission on Artificial Intelligence (NSCAI) report released in March 2021 recommends. Arguing that a multilateral body like Wassenaar was too slow to respond and that its decisions were not binding, NSCAI recommended working directly with the Netherlands and Japan to "align their export control policies" and "establish a policy of presumptive denial of export licenses" to Beijing for extreme ultraviolet (EUV) and argon fluoride (ArF) immersion equipment.[92] In addition to an already extensive extraterritorial application of U.S. re-export regulations, Washington is therefore ready to throw its weight behind bilateral negotiations to align its allies into restricting China's access to certain key technologies like semiconductors.

Despite President Trump's unilateralist bent and President Biden's pleas for international cooperation, both administrations have attempted to leverage the extraterritoriality of their law, their influence in multilateral structures, and the United States' leverage in bilateral negotiations to convince and coerce its allies not to export certain technologies to China.[93] While most allies share U.S. concerns about China to varying degrees (in particular its predatory technology acquisition practices, and the risk of their

90. H. Meijer, *Trading with the Enemy*, *op. cit.*, p. 253.
91. C. Ford, "Four Years of Innovation and Continuity in U.S. Policy: Arms Control and International Security Since January 2017", *op. cit.*
92. E. Schmidt *et al.*, *Final Report*, National Security Commission on Artificial Intelligence, 2021, available at: www.nscai.gov.
93. For a summary of the efforts of U.S. diplomacy regarding export controls in bilateral, plurilateral, and multilateral settings, see Jeremy Pelter, Under Secretary for Industry and Security at the Department of Commerce since 2019 : J. Pelter, "Testimony Before the U.S.-China Economic and Security Review Commission", *op. cit.*

use for military purposes or in violation of human rights), support for what is perceived as a desire to slow Chinese technological development is much less unanimous, and the prospect of growing U.S. restrictions on their trade causes some concern.

# Conclusion and Future Perspectives

The perception by the U.S. political elite that the United States is engaged in a "competition with China and other countries to win the 21st century",[94] a competition that is primarily technological, has led it to deploy a multifaceted strategy to prevent allies from adopting and exporting certain technologies. Despite an undeniable change in approach under the Biden administration, the first year of this new presidency has shown that these two objectives remain priorities, and that U.S. efforts to convince, coerce and incite allies may intensify in the coming years.

## Likely New Restrictions on Exports

In keeping with the decisions outlined above (and after the latest restrictions in December 2021),[95] new U.S. controls on exports and re-exports seem likely, particularly for technologies tied to artificial intelligence or semiconductor manufacturing equipment.[96] The administration (and in particular the Commerce Department) is under pressure from a segment of Congress, which is calling for more restrictions, as evidenced by the October 22, 2021 letter to Commerce Secretary Gina Raimondo signed by 17 Republican members of the House Foreign Affairs Committee.[97] In it, they call for the "urgent" implementation of 10 recommendations, to which the executive branch must respond before the confirmation of the new Under Secretary of Industry and Security (which these Representatives are currently blocking).[98]

These recommendations include:

- expanded use of the Foreign Direct Product (FDPR) rule;
- the extension of the licensing policy applied to SMIC to all Chinese semiconductor manufacturing companies (foundries);
- the introduction of new restrictions on certain technologies required for

94. J. Biden, "Remarks by President Biden in Address to a Joint Session of Congress", Washington D.C., April 28, 2021, available at: www.whitehouse.gov.
95. Bureau of Industry and Security, "Addition of Certain Entities to the Entity List and Revision of an Entry on the Entity List", Federal Register, December 17, 2021, available at: www.federalregister.gov.
96. E. Schmidt *et. al.*, *Final Report*, *op. cit.*
97. M. McCaul *et. al.*, "Letter to The Honorable Gina Raimondo", October 22, 2021, available at: https://gop-foreignaffairs.house.gov.
98. K. O'Keeffe, "House Republicans Call for Tougher Controls to Keep U.S. Tech From China", *The Wall Street Journal,* October 25, 2021.

semiconductor manufacturing (including EUV and ArF photolithography);

- the leveraging of the June 2021 U.S.-EU agreement on civil aircraft to "coordinate [transatlantic] technology transfer policies".

Part of Congress has therefore already taken a clear position in favor of additional restrictions (targeting both technological processes and companies) and expanded application of existing rules.[99] In addition, many officials, experts, and official reports have criticized the Commerce Department for its slowness in establishing, as required by the 2018 law,[100] the list of "emerging and foundational technologies" which should receive greater U.S. attention... and export controls.[101] Given that administration officials (such as Jake Sullivan[102] and Katherine Tai[103]) also do not rule out the possibility of new trade barriers, these factors suggest that new trade restrictions could be announced in the coming months, although industry lobbying emphasizing the risks of overly broad and unilateral controls on firms' innovation capabilities does seem to be at least partially incorporated into the administration's thinking.

## Continued Efforts to Align Allies' Export Controls

In addition to these U.S. policy changes, Washington's diplomatic efforts to persuade allies to align their own export control policies toward China with those of the United States are likely to escalate in multilateral and bilateral settings. The U.S. commitment, prior to the Biden presidency, to building an international consensus on new controls (through bodies such as Wassenaar or the TTC) is confirmed by the current administration's focus on multilateralism and cooperation among allies. The two bills addressing competition with China – the United States Innovation and Competition Act passed by the Senate in June 2021 and the America COMPETES Act passed by the House of Representatives in February 2022 – explicitly state that it is U.S. policy to collaborate "with allies and partners to protect critical

99. However, as companies affected by the first expansion of the FDPR in the summer of 2020 have pointed out, the possibility of further amendments of this type (which would risk halting trade that has until now been legal) creates a problematic, unstable environment. See Japan Business Federation *et al.*, "Requests with Regards to the Extraterritorial Application of Chinese and United States Regulations", *op. cit.*
100. The law in question is the August 2018 Export Control Reform Act (ECRA).
101. Examples include testimony by D. Hanke and G. Cinelli, Hearing on U.S.-China Relations in 2021, "U.S.-China Economic and Security Review Commission", September 8, 2021, available at: www.uscc.gov, as well as the following reports: "U.S.-China Economic And Security Review Commission", *2021 Report to Congress*, November 2021 ; E. Rafaelof, *Unfinished Business: Export Control and Foreign Investment Reforms*, Issue Brief for the U.S.-China Economic and Security Review Commission, June 1, 2021 ; I. Fergusson and K. Sutter, *U.S. Export Control Reforms and China: Issues for Congress*, Congressional Research Service, January 15, 2021.
102. G. Bade, "White House Debates to Delay Biden's Plan for Tariffs on Key Chinese Industries", *Politico*, October 29, 2021.
103. K. Tai, "A Conversation with Ambassador Katherine Tai, U.S. Trade Representative", Center for Strategic and International Studies (CSIS), October 4, 2021.

technologies by crafting multilateral export control measures" to "ensure that the United States leads in the innovation of critical and emerging technologies".[104] These discussions could prove difficult, however, as some allies, notably the EU, do not share the U.S. conception of export controls as a tool for competitiveness and technological leadership, and wish to limit their use to security issues (terrorism, human rights).[105] Given these difficulties, it is likely that in some key sectors (such as semiconductors) the United States will combine this strategy of careful plurilateral coalition building with unilateral pressure directly targeting certain states (Japan, the Netherlands),[106] as recommended in the National Security Commission's report on artificial intelligence. Such a campaign by the U.S., encouraging certain allies to "implement unilateral export controls" without deferring "all decisions [...] to multilateral organizations such as the Wassenaar Arrangement and the European Union" could be problematic for European coordination on this issue.[107]

## Network and Foreign Investment Security: Towards Incentives and Cooperation?

U.S. diplomacy also seems far from relenting in its efforts regarding network security and, more broadly, to prevent Chinese suppliers from participating in projects (international or national) involving its allies. In line with Joe Biden's political project, the new administration's strategy seems to be to develop more incentives (development aid, loans, competitive alternatives, new partnerships or extension of existing ones) to encourage its partners to turn away from Chinese goods.[108]

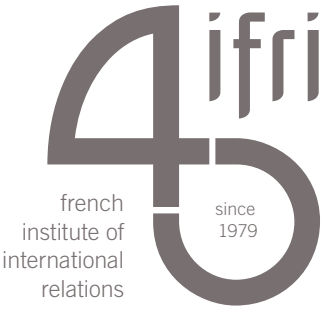
Between securing infrastructures and preventing involuntary technology transfers, U.S. attention to its allies' Chinese investments will persist, and seems to include a renewed desire for cooperation. In order to guard against the risks associated with Chinese investment in U.S. companies – data capture, control of strategic infrastructure, acquisition (legal or through intellectual property theft) of cutting-edge technology – Washington reformed its investment control system in the summer of 2018. This reform (which may in turn prevent foreign companies that have received

104. 117th Congress, *United States Innovation and Competition Act of 2021 (S.1260),* Section 3004 (b) (10), passed by the Senate on June 8, 2021, available at: www.congress.gov. This text has yet to be harmonized with the *America COMPETES Act,* passed on February 4, 2022 by the House of Representatives, which contains a similar passage, Section 30003 (b) (9), available at: https://docs.house.gov.
105. Statement by S. Chardon (DG Trade, European Commission), "Joint U.S.-E.U. Outreach to EU and US Stakeholders On Dual-Use Export Controls", October 27, 2021.
106. "Game of Chiplomacy: A Global Contest over Semiconductors", *The Economist*, January 29, 2022.
107. E. Schmidt *et al.*, *Final Report, op. cit.*
108. D. Hinshaw and S. Woo, "U.S. Fight against Chinese 5G Efforts Shifts from Threats to Incentives", *op. cit.*

Chinese investment considered unsafe from investing in the United States) and U.S. encouragement have prompted many countries to amend their own legislation.[109] The U.S. preoccupation with Chinese investment in technology companies runs through the Trump and Biden administrations, but the current administration does appear to differ in its approach: it seems marked by a desire to "multilateralize" the screening of foreign investments (e.g., through intelligence-sharing partnerships, coordinated screening with allies...).[110] The Quad (Australia, Japan, India, United States) and Working Group 8 of the Trade and Technology Council could thus be a forum for enhanced cooperation in this area.

The Biden administration is therefore in line with the multidimensional strategy deployed by U.S. authorities in recent years to coerce and convince allies not to adopt or transfer technologies that could provide an advantage to China. These efforts have helped create awareness in Europe both of the security challenges posed by certain technologies offered by Chinese suppliers (notably Huawei's 5G), but also of the risks associated with the increasingly coercive practices of major powers. In response, the EU has begun to develop tools – Toolbox 5G, a proposed anti-coercion regulation, modernization of the European export control system... – to try to address these twin challenges. However, member states differ in their perception of these risks, their vulnerability to commercial, diplomatic and security pressures, and more broadly in their relationship with the United States and China, making the articulation of a unified position particularly complex. After only one year, it is too early to determine whether Biden's rhetoric will actually translate into more multilateralism and incentives, or whether the bipartisan perception of urgency and influence of the "China hawks" will lead to unilateral and coercive policies. The fact that this second option cannot be entirely ruled out should encourage Europeans to continue the work they have begun in order to maintain genuine agency and decision-making capabilities while furthering the dialogue with Washington.

109. For Japan, which amended its *Foreign Exchange and Foreign Trade Act* for this reason in 2019, see: J. Schoff, *U.S.-Japan Technology Policy Coordination, op. cit.* p. 24
110. A. Cha, CFIUS, "Team Telecom and China", *Lawfare*, September 28, 2021.




27 rue de la Procession 75740 Paris cedex 15 – France

Ifri.org