



TECHNOLOGY STRATEGIES IN CHINA AND THE UNITED STATES, AND THE CHALLENGES FOR EUROPEAN COMPANIES

Laurence NARDON (ed.)

October 2020



North America
Program

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.

The opinions expressed in this text are the responsibility of the authors alone.

ISBN: 979-10-373-0239-7

© All rights reserved, Ifri, 2020

How to cite this publication:

Laurence Nardon (ed.), “Technology Strategies in China and the United States, and the Challenges for European Companies”, *Études de l’Ifri*, Ifri, October 2020.

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

Authors

Sofia Bournou, Senior Adviser, International Relations, BusinessEurope.

Jean-François Bureau, President of IOConseil (Innovation et Organisations Conseil).

Pierre Girard, International Consultant and Key Account Manager.

André Loeseckrug-Pietri, Executive Director of the Joint European Disruptive Initiative.

Éric-André Martin, Secretary General of the Study Committee on Franco-German Relations (Cerfa), IFRI.

Laurence Nardon, Research Fellow, Head of the North America Program, IFRI.

John Seaman, Research Fellow, Center for Asian Studies, IFRI.

Mathilde Velliet, Research Assistant, IFRI.

Marion Welles, Financial journalist.

Executive Summary

As international relations are increasingly reorganized around the US-China rivalry, the tensions between these two great powers are shaping a growing number of sectors, and the exchange of sensitive technologies in particular. This is a critical issue for European companies which, as manufacturers, importers and exporters, risk finding themselves at the heart of the deepening technological competition opposing the United States and China (Éric-André Martin).

The United States has a long history of using multiple regulatory instruments in managing the export of dual-use technologies, in particular towards China. Even beyond the Trump administration's aggressive positions, these regulations are expanding and increasingly strict, hinting at a potential protectionist technological warfare (Pierre Girard).

Despite China's progress in innovation (5G, artificial intelligence, Internet of Things), and an expansion of measures meant to protect intellectual property rights both for domestic and foreign firms, Beijing's predatory industrial practices and the weight of the Chinese Communist Party on the economy and society clearly live on (John Seaman).

French and European companies are thus hindered both by the prohibition of re-exporting American technologies and products enacted by Washington and by Beijing's predatory practices.

How much leeway do European companies have? What role should the European Union play in the face of such challenges? Since 2016, new propositions to reform the EU export-control regime regulating dual-use items are being intensely debated (Sofia Bournou).

The three chapters of this report examine the norms currently in place in the United States, China, and Europe, and delve more deeply into specific case studies: the battle between the Trump administration and Huawei (Marion Welles), the problems facing European companies in China (Laurence Nardon and Mathilde Velliet), and the case of the communications satellites (Jean-François Bureau).

The conclusion of this report draws up a list – of great interest for decision-makers – of the infrastructures and technologies that will be critical for European strategic autonomy in the years to come (André Loesekrug-Pietri).

Résumé

À l'heure où les relations internationales se redéfinissent autour du duopole sino-américain, les rivalités entre ces deux grandes puissances structurent de nombreux domaines, notamment celui des échanges de technologies sensibles. Or, c'est un enjeu crucial pour les entreprises européennes, qui, en tant que constructeurs, importateurs et exportateurs, risquent de se trouver au cœur de la compétition technologique entre les États-Unis et la Chine (Éric-André Martin).

Les États-Unis ont mis en place depuis longtemps de multiples instruments de régulation pour leurs exportations de technologies à double usage vers la Chine. Au-delà même des positions agressives de l'administration Trump, ceux-ci sont de plus en plus stricts, laissant présager une guerre technologique à grand renfort de protectionnisme (Pierre Girard).

En outre, malgré les progrès de la Chine en matière d'innovation (5G, intelligence artificielle, Internet des objets) et de protection de la propriété intellectuelle, aussi bien des entreprises chinoises qu'étrangères, les pratiques prédatrices du secteur privé et le poids du Parti communiste chinois sur l'économie et la société chinoises semblent perdurer (John Seaman).

Les entreprises françaises et européennes sont ainsi entravées d'une part du fait des interdictions de réexportation de matériel américain édictées par Washington, et d'autre part du fait des pratiques prédatrices des entreprises chinoises.

Quelle marge de manœuvre reste-il aux entreprises européennes ? Quel rôle l'Europe doit-elle adopter face à ces régulations et pratiques ? Depuis 2016, un vif débat entoure les propositions de réforme du régime européen de contrôle des exportations de technologies à double usage (Sofia Bournou).

Les trois parties de cette étude font le point sur les normes prévalentes aux États-Unis, en Chine et en Europe, puis sont complétées par un coup de projecteur sur une situation plus spécifique: la lutte de l'administration Trump contre Huawei (Marion Welles), les problèmes rencontrés par les entreprises européennes en Chine (Laurence Nardon et Mathilde Velliet), le cas particulier des satellites de communication (Jean-François Bureau).

La conclusion du rapport dresse une liste – particulièrement utile pour les décideurs – des infrastructures et technologies de souveraineté qui seront essentielles ces prochaines années pour garantir l'autonomie stratégique européenne (André Loesekrug-Pietri).

Table of Contents

INTRODUCTION

Export Controls At A Crossroads: The Challenge Of US-China Competition.....	13
--	-----------

By Éric-André Martin

ON THE U.S. SIDE

The Murky Waters of US-China Technological Warfare.....	23
--	-----------

By Pierre Girard

Case Study: Trump Against Huawei	33
---	-----------

By Marion Welles

ON THE CHINESE SIDE

Innovation in China and its Structural Challenges.....	43
---	-----------

By John Seaman

Doing Business in China	53
--------------------------------------	-----------

By Laurence Nardon and Mathilde Velliet

ON THE EUROPEAN SIDE

The EU's Export-Control Regime Modernization 67

By Sofia Bournou

Technological sanctions in the Space Domain.....73

By Jean-François Bureau

CONCLUSION

Which Technological Priorities for Europe's Strategic Autonomy? 87

By André Loesekrug-Pietri

Introduction

Export Controls at a Crossroads

The Challenge of US-China Competition

Éric-André Martin

By adopting United Nations Security Council (UNSC) resolution 1540, on 28 April 2004, the international community decided to address the threat to international peace and security constituted by the proliferation of weapons of mass destruction (WMD) and their means of delivery. In particular, the resolution singled out the threat of illicit trafficking and the role of non-state actors as adding new dimensions to the issue of proliferation of nuclear, chemical, or biological weapons and their means of delivery. To counter this threat, the UNSC decided that all states “*shall take and enforce effective measures to establish domestic controls to prevent the proliferation of nuclear, chemical, or biological weapons and their means of delivery, including by establishing appropriate controls over related materials*”.

This resolution was a landmark decision towards developing a universal system of strategic trade control, based on shared commitment by the international community to effectively address the threat posed by proliferation of WMD. Together with the control regimes regulating the export of military goods, the “domestic controls” required by this resolution implied that the grey area represented by the so-called “dual-use items”¹ should be properly covered.

1. Dual-use items, as currently defined in the EU regulation, shall mean items, including software and technology, which can be used for both civil and military purposes, and shall include all goods which can be used for both non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices.

Key role played by US in shaping an international framework for strategic trade control

In 2004, the United States had already developed an elaborated approach, based on the drafting of lists associated with the requirement for manufacturers to apply for a license to export the listed goods and technologies. This approach is based on a range of texts, covering all technical fields, and in particular the following ones: the International Traffic in Arms Regulations (ITAR) for military goods, and the Export Administration Regulations (EAR), which in particular sets forth the Commerce Control List for dual-use goods controlled by the EAR; controls on nuclear exports are divided among several agencies, according to the product or service being exported.² These American regulations contain an extraterritorial dimension in order to control the end-use and re-export of these goods and related technologies by customers.

By contributing to bringing together the main countries producing the goods and technologies used for the development and production of WMD, and by promoting common norms and standards for controls, the United States has played a key role in shaping an international export control system. These countries have adhered to the international standards and principles laid down by the major non-proliferation treaties,³ have supported the efforts of the UNSC in the fight against the proliferation of WMD, and most of them have joined the four main multilateral export-control regimes.⁴

The European Union (EU) has joined the efforts of the international community in this field and has put in place regulations to control the export, transfer, brokerage and transit of dual-use goods.⁵ The EU control list integrates all the lists set out by the control regimes. It is therefore considered as an international standard and many countries around the world have adopted it as their own list for export control.

In this context, China appears to be a special case, for at least three reasons: (1) Beijing has been subject to an arms embargo by the United States and the EU since 1989 and is regularly suspected of actively or passively contributing to the procurement efforts related to certain WMD

2. I. F. Ferguson and P. K. Kerr, "The US Export Control System and the Export Control Reform Initiative", Congressional Research Initiative, updated January 28, 2020.

3. Non-Proliferation Treaty (NPT); Chemical Weapons Convention (CWC); Biological and Toxin Weapons Convention (BTWC).

4. The Wassenaar Arrangement (for conventional arms as well as dual-use goods and technologies); the Australia Group (Chemical and biological goods and technologies); the Missile Technology Control Regime (missiles and drones); the Nuclear Suppliers Group (nuclear-related goods and technologies).

5. Council regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items.

programs, notably in relation to the Democratic People's Republic of Korea (DPRK).⁶ (2) Through the “Made in China 2025” strategy, China has launched an ambitious plan in order to take leading positions in the development of carefully selected emerging technologies and be able to eventually supplant its Western competitors in around a dozen industrial sectors. However, China, which has often been accused of forced technology transfer and intellectual property theft, is in turn becoming a producer of advanced technology and has developed a number of legal tools to protect its own technology. (3) More recently, the Trump administration has designated China as a strategic competitor.⁷ The first set of arguments developed by American officials is based on the need to reduce the bilateral trade deficit. But the main objective of the American administration vis-à-vis China is driven by considerations of national security and the struggle for strategic preeminence.

The confrontational course taken by the relationship between the United States and China could seriously affect the multilateral framework regarding export control, by paving the way to a mercantilist vision of technology, centered on the control of emerging and foundational technologies. This could become a major problem for European industry, in its capacity as manufacturer, exporter and client.

Three fundamental breakthroughs contribute to reshaping the international export-control framework

A political breakthrough: the extension of the field of controls.

The United States carried out an in-depth reform of its export-control legislation, which resulted in the adoption of the Export Control Reform Act (ECRA) of August 2018.⁸ This law extends the objectives assigned to the export-control policy of the United States, through missions related to national security, such as (1) preserving the qualitative military superiority of the US; (2) strengthening the American defense industrial base; (3) tailoring national security controls on those core technologies and items that are capable of being used to pose a serious national security threat to the US. The reform of export control was both simultaneous and complementary to

6. US Department of Justice, “Four Chinese Nationals and Chinese Company Indicted for Conspiracy to Defraud the United States and Evade Sanctions”, Press release, July 23, 2019, available at: www.justice.gov.

7. *Remarks by Vice-President Pence on the Administration's Policy toward China*, The Hudson Institute, Washington, D.C., October 4, 2018.

8. See J. S. Mc Cain, *National Defense Authorization Act for Fiscal Year 2019*, August 2018.

the reform of the screening mechanism for foreign direct investment, under the authority of the Committee on Foreign Direct Investment in the United States (CFIUS). Indeed, the Foreign Investment Risk Review Modernization Act (FIRRMA), adopted on August 13, 2018, requires establishing an interagency process in order to identify “emerging and foundational technologies”, which would fall under the review of critical technologies by the CFIUS as well as the Department of Commerce, as regards the export or transfer of such technologies.⁹ Export controls therefore constitute an integral part of the broader US policy regarding the control of transfers of critical technologies.

A notional breakthrough with “Emerging and Foundational technologies”(EFTs).¹⁰

These technologies defy conventional controls, are considered as “those essential to the national security of the United States”, and are not currently covered by existing export-control rules. The Department of Commerce is authorized to establish appropriate controls, including interim controls, on the export, re-export or transfer of the so-called “Emerging and Foundational Technologies” (EFTs).

The law did not define what constitute the EFTs, but refers to an interagency process, in order to identify and describe such technologies, which are essential to US national security because of their potential impact related to conventional weapons, intelligence collection and WMD programs, or because they could provide the US with a qualitative military or intelligence advantage. Initially, the US Department of Commerce identified 14 categories of technology being considered for potential designation as emerging technologies.¹¹ An additional list proposing foundational technologies is forthcoming. The categories BIS is considering potentially as emerging technologies are: artificial intelligence; biotechnology; positioning, navigation and timing technology; microprocessor technology; advanced computing technology; data analytics technology; quantum information and sensing technology; logistics technology; additive manufacturing; robotics; brain-computer interfaces; hypersonics; advanced materials and advanced surveillance technologies.

Distinguishing these technologies has two major effects: (1) intrinsically dual, they blur the traditional separation between civil and military; (2) during the Cold War, many technologies were initially designed for military purposes before “spilling over” into the civil sector, as was the case for the

9. J. K. Jackson, “CFIUS under FIRRMA”, Congress Research Service, February 20, 2020.

10. Federal Register/ Vol. 83, No. 223, November 19, 2018.

11. *Ibid.*

Global Positioning System, drones and even infrared imagery. This distinction is no longer possible for EFTs, as it is essentially a question of technologies developed in civilian laboratories, which are then adapted for military purposes.

A geopolitical breakthrough: the struggle for technological supremacy between the United States and China.

Maintaining American technological leadership in certain key sectors (aeronautics, space, telecommunications, and electronics) has substantially contributed to the pre-eminence of the American economy and its military power over time. Therefore, technology has a double dimension, both as a security and as a commercial issue. The competition between the US and China contributes to shifting the focus of export controls from the traditional sphere of international security to US economic and technological challenges.

In this context, export controls emerge as a way to curb China's rise.¹²

The licensing requirement for exports of EFTs makes very unlikely a decision favorable to China, an embargoed country for US arms exports.¹³ This requirement allows US authorities to precisely control the destination and end use of these technologies. Export controls are already used as an offensive weapon by the US administration, as evidenced by Huawei's inclusion on the Commerce Department's list of designated entities. This registration requires American companies to request a license from their authorities to be able to trade with this Chinese company. This propensity to extend the field of American controls to high-tech firms was confirmed with the designation by US authorities of the Hikvision group, for its involvement in the production of surveillance technologies by China. As part of the ECRA reform, the communication to foreign nationals of information relating to controlled technologies, through university research activities or work in a research laboratory, is subject to a license (deemed export rule). According to data provided by the Commerce Department for the 2017 fiscal year, 55% of these licenses were granted to Chinese students.

12. J. Politi, "Export Controls Emerge as a Way to Curb China's Rise", *Financial Times*, January 30, 2020.

13. S. Ezell and C. Foote, "How Stringent Export Controls on Emerging Technologies Would Harm the US Economy", Information Technology and Innovation Foundation, May 2019.

A fundamental extension of the field of controls on technologies is, therefore, taking place – as regards the technologies covered as well as the objectives pursued by these controls. Alongside the fight against illicit trafficking, through activities carried out by proliferation networks and their front companies, controls address new objectives such as: protecting the national industrial base, combating certain unfair Chinese practices pertaining to intellectual property, and even curbing the influence of certain technological players (such as Huawei or ZTE). This shift in the field of export control for reasons of national security¹⁴ is accompanied by similar developments in other sectors, through the sanctions policy but also trade, by the imposition of duties on steel and aluminum against China and the EU.

Three main challenges for Europe

How to address the challenge of regulating EFTs?

In the United States, ECRA entrusts the American government with the mandate to identify and control the export of EFTs essential to US national security. These technologies fall under categories that are not part of any of the existing control lists, but are considered as essential to the national security of the US.

In China, the authorities intend to rely on technological self-sufficiency as much as possible, drawing on Chinese research potential, in order to develop indigenous technological solutions; on the other hand, the authorities intend to protect technologies of sovereignty, in particular technologies related to national security. In doing so, Beijing will continue to explore technology abroad and accelerate its transfer, to its advantage, when possible. Even as the main technological routes in the United States are closed as a result of reforms to the control system, some will remain open, particularly in Europe and Japan.

For the EU, this issue has been raised by the new Commission. In her 2019-2024 political guidelines, the President of the Commission, Ursula von der Leyen, expressed her intention to achieve technological sovereignty in certain critical technological areas such as blockchain, high-performance computing, quantum computing, algorithms and tools for sharing and using data. The Covid-19 crisis has heightened awareness among Europeans that they have become too dependent on the Chinese market for certain medical products and equipment, and that this trend should be corrected, including

14. K. Cho, "Protectionist Export Controls Could Be Bad for Nonproliferation", *Bulletin of the Atomic Scientists*, September 4, 2018.

by the relocation of certain productions. Defining and updating the EU and member states' list of technologies that they consider to be strategic would be a necessary prerequisite.

Anyway, the question remains whether export-control rules will keep up with the pace of innovation and change, without impeding technological progress. Indeed, while the ability to develop and control these new technologies is important, the pace of innovation constitutes *a game changer*, the actual key that will determine the redistribution of roles and hierarchies between companies and national economies around the world. The country that wins this race will gain the upper hand not only economically but also in the military field, and will thus ensure its strategic supremacy.

How to effectively regulate the trade and transfers of EFTs without excluding China

Finally, this question refers to the way in which the EU can reconcile three contradictory requirements. (1) The first is the requirement to preserve the EU's competitiveness, and the integrity of its technological and industrial capital in a context of accelerating technological change and tougher technological competition. The debate on export controls at European level should be linked to a broader reflection on the economic security of the EU. This approach is necessary because the potential fields of control related to the use of EFTs extend far beyond the traditional sectors covered by export controls, essentially linked to the military, and touch on many aspects of societies, such as public liberties, through the cyber and surveillance technologies and access to private data, medical or critical infrastructure. This approach should also integrate issues linked to foreign direct investment, securing value chains, sanctions policies and extraterritorial practices. (2) The second requirement is to ensure that export controls on these goods and technologies make it possible to limit the risks of diversion for illicit purposes, and security risks: on this point, the challenge is to find adaptable regulations, in order to stay in step with a constantly evolving situation, in which technology transfers are dematerialized. (3) The third requirement is to ensure that these controls do not ultimately become tools for economic decoupling by closing the European market to foreign customers or markets, especially Chinese ones.

The impact on EU companies and global value chains

European companies could eventually find themselves at the heart of the technological battle between the US and China, in their capacity as a manufacturer, importer and exporter.

This issue is key in relation to the debate on European technological sovereignty because it conditions access to certain technologies and markets, and in fact forces European companies to comply with American extraterritorial regulations. The extraterritoriality of American law requires that European companies, operating in the US or incorporating components classified by ITAR or EAR regulations, apply for licenses, or comply with the prohibitions issued by the American authorities. This spans the integration of US components listed under ITAR or EAR, and henceforth touches on the possibility of re-exporting these goods to certain destinations or when containing a certain threshold of US listed goods (the so-called *de minimis rule*). At the same time, the Chinese bill reforming the export-control system, which has been discussed since 2017, could open the door to provisions copied from the American system.¹⁵ The article 10 of the bill mentions the creation of a “distrusted entity list” (entities with which it is not allowed to have business relations), an issue that could become directly as well as indirectly problematic for European companies. On top of that, through the law on foreign investments, Chinese authorities could apply the principle of reciprocity against jurisdictions that discriminate against Chinese investments.

In the event of a further escalation between China and the United States on export control, the ultimate risk would be a fragmentation of value chains, between various norms, standards and regulations, as well as a disruption of international cooperation in research and innovation. This could lead to a new burden for European companies that get caught in the crossfire.

15. Bund der Deutschen Industrie, “Chinas Exportkontrolle – Stellungnahme zum zweiten Entwurf einer nationalen Exportkontrolle Chinas”, January 23, 2020.

On the U.S. Side

The Murky Waters of US-China Technological Warfare

Evolutions and Challenges of US Technology Control Policies Towards China

Pierre Girard

On the grand chessboard of international politics, the open economic confrontation between the People's Republic of China (PRC) and the United States of America (US) was predominant in the year 2019. The signing of the “phase one” trade deal with China on January 15, 2020 marked the end of the first act of the Sino-American trade war, which saw the Trump administration take an offensive and confrontational approach. This decision was based on the grounds that the PRC is engaged in unfair trade practices, characterized by irregular implementation of its WTO obligations and the use of hidden subsidies, that its trade surplus with the US is rapidly growing, and that the enforcement of intellectual property rights is ineffective, notably through extensive practice of cyber-espionage.¹⁶ This has led to an escalation of tensions, materialized in tit-for-tat reprisals and the imposition of ever-higher tariffs on a growing range of products.

Throughout 2018, the US introduced tariffs on approximately \$250 billion of Chinese imports, and China retaliated soon after by applying custom duties to \$110 billion worth of US imports. In June 2019, the US administration raised tariffs from 10 to 25% on \$200 billion worth of already targeted imports from China; the PRC did likewise, raising the tariff rate on \$60 billion of imports from the US.¹⁷ The “phase one” trade-deal agreement put an end to this escalation of tensions, with PRC commitments to allow greater access to its markets, to buy an additional \$200 billion of US exports over the next two years, and to address US concerns about intellectual

16. D. Trump, *National Security Strategy of the United States of America*, December 2017, available at: www.whitehouse.gov.

17. C. P. Bown and M. Kolb, “Trump’s Trade War Timeline: An Up-to-Date Guide”, Peterson Institute for International Economics, September 28, 2020, available at: www.piie.com.

property theft. But Chinese customs duties have only slightly decreased since the agreement was signed and, despite a clear cut by the Americans, tariffs on products from China remain six times higher than at the start of the trade war in 2018.¹⁸

The end of the first round of the economic warfare between the USA and China has led to a situation that economically hurts both countries. The escalation of tariffs has resulted in higher prices for US consumers and companies, while China has suffered from significant export losses.¹⁹ The second phase of the economic competition should thus shift towards a new approach that brings to the forefront export and import controls, investment restrictions and economic sanctions. If the news headlines regarding the trade war have put the emphasis on the tit-for-tat tariffs and the US trade deficit, it appears that the underlying driver and primary source of this clash is the ongoing race for technology dominance, which the repositioning of the US approach attempts to address more squarely.

In 2015, the PRC unveiled an ambitious 10-year industrial plan, “Made in China 2025”, which aims to massively develop the high-tech sector. That long-term strategy, whose purpose is to ensure China’s future global tech dominance, and the means to achieve it, is perceived by the US as a major threat to their own supremacy and have been qualified by the Trump administration as “economic aggression”.²⁰ Technological competition raises many geopolitical and geo-economic issues for both parties, as many of the next-generation technologies have both civilian and military applications. While China is trying to transform from a low-cost manufacturing country to a major innovative power, the US wants to ensure that US companies, through their lead in cutting-edge technologies and R&D, can maintain their competitiveness on the world stage, and thus secure economic prosperity and growth potential in the coming years. Furthermore, as China’s military capabilities are rapidly building up, the US wants to secure its geopolitical advantage from a technological standpoint. The recent introduction of new measures by the Trump administration to protect further technology and high value-added goods, demonstrates the US willingness to curb Chinese intentions. However, these measures need to be analyzed and put into perspective in the light of the historical evolution of export-control policies, which highlights the commercial and

18. *Ibid.*

19. A. Nicita, “Trade and Trade Diversion Effects of United States Tariffs on China”, UNCTAD Research Paper, No. 37, November 2019.

20. “How China’s Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World”, White House Office of Trade and Manufacturing Policy, June 2018, available at: www.whitehouse.gov.

technological relationships with China over time and the geopolitical and economic interests of both parties.

Evolution of US technology export-control policies towards China: a historical perspective

At the end of the Second World War, the US and its allies established a system of both national and multilateral control of exports, notably through the creation of the Coordinating Committee for Multilateral Export Controls (CoCom) in 1949, towards Warsaw Pact countries and the PRC. Its main objective was to regulate and control the export of war material, technical data and dual-use goods, which, according to the Export Administration Regulations (EAR), are “[i]tems that have both commercial and military or proliferation applications”.²¹ In 1950, the start of the Korean War led the US and its allies to implement a trade embargo and harsher export controls on China than on the USSR. That decision was fueled by the perception of China as the greatest single security threat to the US in East Asia because of its supposedly aggressive foreign policy, and by the desire to make China overly dependent on Moscow. The difference of treatment towards China ended in the early 1970s with the abolition of the embargo and the loosening of export controls on the PRC.

That new phase of “rapprochement” was motivated by strategic and security considerations. In the short term, Washington wanted to facilitate the negotiations to end the Vietnam War by isolating Hanoi from the PRC. In the long run, it sought to take advantage of the Sino-Soviet split by creating a US/China tacit strategic partnership that could provide the US with greater leverage over the USSR. In 1979, Soviet policy was perceived as increasingly aggressive, with its behavior in Ethiopia and Afghanistan, and its military build-up in East Asia. The US policy establishment thus decided to loosen its export-control policy towards China and to establish several agreements to expand economic, scientific, military, intelligence and technological exchanges relationships between the two countries. The common perception of the PRC and the Soviet Union as a threat, the overall effectiveness of the multilateral framework (thanks in particular to the veto right of each CoCom member country), and a Western technological oligopoly, allowed the US and its allies to control effectively military and technology transfers to the communist bloc and China during the Cold War.

21. See Export Administration Regulations files, Bureau of Industry and Security, U.S. Department of Commerce, available at: www.bis.doc.gov.

The events of Tiananmen in 1989 and the end of the Cold War era marked a paradigm shift in the US export-control policy towards China. The policy stopped being liberalized as the multilateral framework eroded (CoCom ceased to exist in 1994, and was replaced by the less effective and binding Wassenaar Arrangement) in favor of a more unilateral state-centric one. From the early 1980s on, it changed from a policy influenced primarily by geopolitical, military and diplomatic considerations to one influenced increasingly by the economy and trade. However, after the collapse of the Soviet Union, China gradually emerged as the most likely peer competitor to the US. Annual increases in defense budgets, imports of foreign technology, research and development spending, and military-industrial espionage practices have fueled major Chinese military modernization, which has received growing attention from Washington.

In addition to the weakening of the multilateral export-control architecture, the globalization and growing importance of private industrial players (less dependent on the state than the defense industry) in the production of strategic and dual-use goods have undermined the US state's ability to control exports of sensitive technologies. Furthermore, the evolution of China's indigenous capacities and the exponential intensification of Sino-US economic relations have led to growing domestic pressure on the foreign-policy establishment elites, from domestic interest groups, to relax export controls.²² As US technological leadership eroded, and as the multilateral export-control regime collapsed, US domestic export-control policies started to undermine the competitiveness of US companies vis-à-vis foreign industries, subject to weaker export controls. The negative impact on their ability to invest in R&D in next-generation technologies *de facto* weakened the Pentagon's ability to access state-of-the-art technologies. The realization that the US strategy could not prevent China from obtaining dual-use goods and high-tech products, and its harmful nature for the national economy, has produced a shift of mentality in the American administration. A historical review of the evolution of US export-control policies towards China demonstrates that these policies are a function of a precarious and evolving balance between domestic economic considerations and strategic and geopolitical rivalries.

22. H. Meijer, *Trading with the Enemy: The Making of US Export Control Policy toward the People's Republic of China*, New York: Oxford University Press, 2018, p. 416.

From China's desire for technological power to the means to achieve it

If the US was easily satisfied and benefited greatly from China's subordinate position in the global supply chain, China's strategic development plan could eventually challenge this situation and make the PRC the main competitor of the US in the field of high technology. In 2013, shortly after his appointment as General Secretary of the Chinese Communist Party (CCP), Xi Jinping outlined his vision of China's future, which he built around the idea of national rejuvenation. Echoing the Western industrial revolutions, he then stated that China's greatness would necessarily involve major technological modernization, which would allow it (making Mao's words and vision his own), to "catch up and surpass" ("ganchao") the West.²³ This vision took shape in the 13th industrial plan of the CCP, "Made in China 2025". This strategic plan, which aims to boost China's industrial sector, is notably based on innovation in high technology, the integration of information technologies, and a restructuring and internationalization of the manufacturing sector. Ten key sectors lay at the center of the policies put in place: CNC (computer numerical control) machine tools and robots, new information technologies, aeronautical equipment, ocean engineering equipment and high-tech ships, railway equipment, new energy vehicles, new materials, biomedicine and agricultural machinery. They are the subject of massive investments (\$300 billion),²⁴ sponsored by the Chinese state, with the aim of growing and innovating at fast pace, as well as offering industries the capacity to use up to 70% of Chinese domestic content of core materials by 2025.²⁵ The "Made in China 2025" plan thus displays a desire to achieve self-sufficiency, move up the value chain, and ensure that Chinese companies control their domestic market and compete internationally in the field of cutting-edge technologies.

Although the PRC's indigenous capabilities are growing exponentially, foreign companies are still providing key inputs along China's supply chains through trade and investment. This technology transfer, and the means to achieve it, have been the subject of particular attention in Washington, and have triggered an outcry from several government officials. In 2018, a

23. C. Buckley and P. Mozur, "What Keeps Xi Jinping Awake at Nigh", *The New York Times*, May 11, 2018, available at: www.nytimes.com.

24. J. Fang and M. Walsh, "Made in China 2025: Beijing's Manufacturing Blueprint and Why the World Is Concerned", April 28, 2018, available at: www.abc.net.au.

25. S. Hsu, "Foreign Firms Wary of 'Made in China 2025', But It May Be China's Best Chance At Innovation", *Forbes*, March 10, 2017, available at: www.forbes.com.

thorough investigation conducted by the US Trade Representative²⁶ concluded that the Chinese government and state-backed companies were using an array of directives, incentives and methods, legal or coercive, to acquire valuable technologies, intellectual property (IP) and knowhow from foreign firms. The report demonstrates that China is pushing, and potentially backing financially, its companies to invest in and/or acquire foreign companies, tech start-ups and assets. They seek to obtain cutting-edge technologies (with potential dual-use applications) and IP through foreign direct investment and venture capital investment. Another tactic consists of forcing foreign firms to form a joint venture, dominated by the Chinese partner, in order to invest or operate in China (i.e. the so-called “forced technological transfers”). For instance, the report shows that US companies must partner with a Chinese company to enter the market for electric cars, thus giving full access to its IP and technologies to its Chinese counterpart. Analogously, the government can directly require a company to disclose sensitive technical data and information in order to get a licensing agreement or, more broadly, the necessary administrative approvals to operate in China.

Finally yet importantly, the investigation found that government officials and executives in Chinese companies are using undercover cyber intrusion to get “unauthorized access to a wide range of trade secrets, technical data, negotiating positions, and sensitive and proprietary internal communications”.²⁷ This valuable intel is then most likely shared and used by Chinese companies to help them develop and innovate or gain international competitive advantage. According to Keith Alexander, former director of the National Security Agency (NSA), cyber espionage constitutes “the greatest transfer of wealth in history”,²⁸ with a loss to US companies that is estimated at \$250 billion per year, through intellectual property theft. All these Chinese technology-transfer attempts usually target high-tech industries and companies, which are often in early stages of development and involved in producing dual-use goods. Both the PRC’s ambition to catch up and surpass the US from a technological and innovative standpoint, and the means to achieve it through (possibly forced) technology transfers and IP acquisitions, form the roots of the Trump administration’s desire to prevent the leak of sensitive US dual-use technologies.

26. US Trade Representative, Findings of the Investigation into China’s Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974, March 22, 2018.

27. *Ibid.*, p. 153.

28. J. Rogin, “NSA Chief: Cybercrime Constitutes the ‘Greatest Transfer of Wealth in History’”, *Foreign Policy*, July 9, 2012, available at: <https://foreignpolicy.com>.

Organization of the export-control system and the recent introduction of protectionist measures

Despite past historical experiences, which have exposed the weaknesses of unilateral export controls for sensitive technologies and dual-use goods, the US, under the impetus of the Trump administration, has decided to modernize and introduce new restrictive measures. It followed the path of the Obama administration's 2009 initiative²⁹ to review and reform export-control policies, with the objective of simplifying export licensing requirements for less sensitive goods and building better protections for the most critical technologies. In a speech about the reform, then Secretary of Defense Robert Gates described the bureaucratic structure of the US export-control system as a “byzantine amalgam of authorities, roles, and missions scattered around different parts of the federal government”.³⁰ The export-control system is administered by different agencies, reliant on federal executive departments, which implement various regulations depending on the nature of exports.³¹ The following table provides an overview:

Overview of US export-control governance system

Federal Executive Department	Department of Commerce	Department of State	Department of Treasury
Administering agency	Bureau of Industry and Security (BIS)	Directorate of Defense Trade Controls (DDTC)	Office of Foreign Assets Control
Regulation regime	Export Administration Regulations (EAR)	International Traffic in Arms Regulations (ITAR)	Trade restrictions and embargoes Assets-blocking
Type of exports	Dual-use goods, software and technologies, less sensitive military items	Defense-related articles and services (incl. biological, chemical and nuclear proliferation-related items)	Any transaction or good to a country or group of individuals subject to US sanctions

29. “President Obama Announces First Steps Toward Implementation of New U.S. Export Control System”, Press release, Washington D.C., The White House, December 9, 2010, available at: <https://obamawhitehouse.archives.gov>.

30. Secretary of Defense Robert M. Gates, speech to Business Executives for National Security, April 20, 2010.

31. “Overview of U.S. Export Control System”, Export Control & Related Border Security, available at: <https://2009-2017.state.gov>.

Despite the differences of opinion within Trump's trade team on the more or less firm position to adopt in order to "decouple" the US from China, a consensus has emerged around the necessity to protect the US from the theft of IP and (forced) technology transfers. As a result, the US administration has launched two waves of measures to exercise stricter control over foreign investment and to tighten export controls. The Foreign Investment and Risk Review Modernization Act (FIRRMA) of 2018 modernizes practices, increases prerogatives and broadens the scope of the Committee on Foreign Investment in the United States (CFIUS). This entity's main goal is "to review certain transactions involving foreign investment in the United States [...] in order to determine the effect of such transactions on the national security of the United States".³² The reform has notably implemented higher scrutiny of foreign investment in a US business dealing with sensitive personal data of US citizens or involved in "critical technology", which comprises technologies used in the defense industry or for the manufacturing of chemical, biological or nuclear weapons, and any dual-use item used within a specific subset of industries.³³ The full list of the 27 industries concerned notably includes computer manufacturing, aviation, defense, petrochemical, nanotechnology, biotechnology, semiconductors and wireless communication. For instance, following the CFIUS recommendations, Trump used his presidential veto to oppose the takeover of Qualcomm, the US chip giant, by Singapore-based Broadcom, because it could threaten US national security by divesting in 5G technology.³⁴ In September 2017, the administration had already opposed the takeover of microprocessor manufacturer Lattice by a Chinese-funded investment fund.

The FIRRMA also included the Export Control Reform Act (ECRA) of 2018, which aims to restrict the export of "emerging and foundational technologies", which are dual-use technologies that had not been targeted by previous export controls but could "provide the US with a qualitative military or intelligence advantage".³⁵ The definition of what constitutes such technologies has yet to be determined, but the current list for review includes: biotechnology; artificial intelligence and machine-learning technologies; position, navigation and timing (PNT) technologies; advanced

32. "The Committee on Foreign Investment in the United States (CFIUS), U.S. Department of the Treasury, available at: <https://home.treasury.gov>.

33. F. Jalinous, K. Mildorf, K. Schomig, C. Brayton-Lewis and S. Jorgensen, "CFIUS: FIRRMA Pilot Program Mandates Notification for Certain Critical Technology Transactions", October 13, 2018, available at: www.whitecase.com.

34. "Presidential Order Regarding the Proposed Takeover of Qualcomm Incorporated by Broadcom Limited", The White House, March 12, 2018, available at: www.whitehouse.gov.

35. "Review of Controls for Certain Emerging Technologies", *Federal Register*, Vol. 83, No. 223, National Archives, November 19, 2018, available at: www.govinfo.gov.

computing technologies; data analytics technologies; quantum information and sensing technologies; additive manufacturing (3D printing); advanced robotics, and materials and surveillance technologies.³⁶ The goal of this reform is to limit the proliferation of such technologies in foreign countries, in order to preserve “U.S. leadership in the science, technology, engineering, and manufacturing sectors”.³⁷

Towards protectionist technological warfare?

While tariff escalation has had the notorious effect of bringing the Chinese back to the negotiating table, it appears that the deepening of controls on foreign investment and dual-use technology exports by the US more adequately addresses the PRC’s predatory practices. US/China economic relations are now at an important crossroads, and the major challenge seems to lie in a delicate equilibrium to be found by the Trump administration. The desire to ensure national security by retaining military and geopolitical dominance should not call into question the economic health of cutting-edge companies, while maintaining mutually beneficial trade relations with China. The success or failure of US technology control policies also seems to depend on the willingness and ability of foreign countries to adopt similar practices, thereby establishing *de facto* an effective multilateral control framework. On this point, France, Germany and the United Kingdom have already stepped forward by implementing new series of measures to scrutinize foreign investments in sensitive industries.³⁸ The European Union also established “a mechanism to cooperate and exchange information” among the Commission and member states “on investment from countries that may affect security or public order in the EU”.³⁹ President Trump may have well spread his openly protectionist trade policy trend around the globe, as a growing number of countries start to emulate the US example in this regard. While the outcome of the developing situation remains unclear, it seems certain that the technological warfare is not going to stop any time soon, and that companies, interest groups and nations around the globe will be engaged in ferocious battles over the coming years.

36. *Ibid.*

37. “Review of Controls for Certain Emerging Technologies – A Proposed Rule by the Industry and Security Bureau”, *Federal Register*, Vol. 83, No. 223, National Archives, November 19, 2018, available at: www.federalregister.gov.

38. E. Brattberg and E. Soula, “Is Europe Finally Pushing Back on Chinese Investments?”, Carnegie Endowment for International Peace, September 14, 2018, available at: <https://carnegieendowment.org>.

39. “Commission Welcomes European Parliament’s Support for Investment Screening Framework”, Press release, European Commission, February 14, 2019, available at: <https://ec.europa.eu>.

Case Study: Trump Against Huawei

Marion Welles

The US and China have been embroiled in a trade war since 2018. At that time, US President Donald Trump imposed sweeping tariffs on China for its alleged unfair trade practices. At first the US conflict with China was seen as driven by a desire to reduce the US trade deficit and boost manufacturing activity locally. However, the US motivations are far more complex and far-reaching than that. They lie, in part, in its anxieties regarding China's rapid technological advances and its desire to become the leading global technological superpower.

The catalyst for the trade wars was China's "Made in China 2025" strategy, announced in 2015. This plan aims to transform China from a low-cost manufacturing hinterland to a great innovation power. It defined 10 core industries, such as robotics, power equipment, and next-generation IT, in which China aims to achieve breakthroughs and create globally competitive companies.

For the US, the plan's announcement was a Sputnik moment, a wake-up call similar to that felt when the Soviet Union launched its first satellite in 1957, the Sputnik, thus beating the USA into space. The Chinese plan was perceived as a threat to the US's predominant power position in emerging technologies such as AI and data science, and especially fifth-generation cellular networks (5G).

5G is not just the next-generation of mobile network technology. It will be crucial to the new information and communication boom being driven by the Internet of Things (machine-to-machine interaction) and artificial intelligence (AI). The race for 5G is crucial as the first country to fully implement a nationwide 5G network will lead the world in terms of standard-setting and patents, and will dominate the global supply chain.

The US is lagging behind in terms of 5G technology developments and does not have a major company offering 5G transmission equipment. The leader in information and communication technologies, and most recently

in 5G equipment and services, is a Chinese company created in 1987, Huawei Technologies Ltd, which makes smartphones and network equipment.

Concerns about Huawei are multifold

Concerns about Huawei precede the Trump administration. As early as 2012, following an investigation, a US congressional panel warned that Huawei and rival ZTE posed a security threat, and the US banned its companies from using networking equipment. But since 2018, Huawei has been at the epicenter of the contest between the US and China.

The stakes are huge and Huawei is well placed to get the biggest part of the pie

5G mobile networks are expected to have peak download speeds as high as 20 gigabits per second and lower latency. This will enable specialized and precise functions, such as the Internet of Things, remote medicine and connected cars, as well as augmented and virtual realities. A recent World Economic Forum report concluded that, by 2035, 5G networks will contribute \$13.2 trillion in economic value globally and generate 22.3 million jobs from direct network investments and residual services. 5G networks and their related applications are expected to add three million jobs and \$1.2 trillion to the economy in the US.⁴⁰

Huawei dominates the beginning of 5G technology. The company is not only powerful because of the quality of its products, but because there is little competition. The US dominated the 4G market place after lagging behind Europe for 3G standards, but has currently no major company competing in the 5G infrastructure race. Huawei's major competitors are Finland's Nokia and Sweden's Ericsson, with Samsung and ZTE following along. Moreover, Huawei's products are cheaper.

The US sees Huawei as an arm of the Chinese Communist Party (CCP)

There are fears that China is using Huawei as a proxy so it can spy on rival nations and scoop up useful information. This concern emanates from the history of its founder. Ren Zhengfei, who grew up poor, graduated from the Chongqing Institute of Civil Engineering and Architecture and joined a People's Liberation Army research institute at the height of the Cultural

40. N. Turner Lee, "Navigating the U.S.-China 5G Competition", Brookings, April 2020, available at: www.brookings.edu.

Revolution. In 1978, he joined the Communist Party and since then has been a steady member. After leaving the army in 1983, he moved to Shenzhen in southern China. Working in the country's nascent electronics sector, Ren founded Huawei in 1987 to sell simple telecoms equipment to the rural Chinese market. Within a few years, Huawei was developing and producing the equipment itself. In the early 90s, Huawei won a government contract to provide telecoms equipment for the People's Liberation Army. In 1996, Huawei was given the status of a Chinese "national champion". In practice, this meant the government closed the market to foreign competition. Huawei started expanding overseas in 2000, and international market contracts exceeded its domestic business by 2005.

The ties between Huawei's founder and the Chinese government have raised suspicions that the company owes its rise to its powerful political connections. Faced with accusations of being an extension of the CCP, Huawei answers that it is privately held and employee-owned. Ren claims that this set-up keeps him independent from the government and allows him to invest freely. Each year, Huawei spends US\$20bn on R&D – one of the biggest such budgets in the world.

This has not alleviated concerns that Huawei may be used to spy on competitors and countries. Some even argue that the Chinese company may have built in a "backdoor" to its network software (or could be compelled to) that would allow covert surveillance or control – or even destruction – of phone networks, which are by their nature accessible via the internet.

Since 2018, the Trump administration has been waging a multi-front war on Huawei

Trump' attack on Huawei is quite typical of his transactional method of negotiating: as in his business dealings during his career, no holds are barred. The aim is to eliminate the opponent.

Step 1: Cut Huawei's access to crucial technology supplies through the US export controls regulations

One way to weaken Huawei is to cut its access to American technology. The US Export Administration Regulations (EAR) are one of the most powerful tools for the US to exert extraterritorial control over foreign companies. It allows the US to restrict the use of and access to controlled information, goods and technology for reasons of national security or protection of trade.

Under these regulations, the export of certain goods and technology may be prohibited or a government license may be required to proceed with the export. Export control regulations are not new and have been around since the 1940s. However, in recent years, attention to export control compliance has increased because of heightened concerns about homeland security, terrorism, drug trafficking and leaks of US technology to foreign competitors.

In May 2019, the US Commerce Department's Bureau of Industry and Security (BIS) added Huawei and 68 non-US Huawei affiliates to the BIS Entity List. The designation imposed an export license requirement on all exports, reexports, and transfers of items subject to EAR on Huawei and the 68 listed affiliates. That list was extended to 46 additional affiliates in August 2019. In effect, that meant that Huawei could no longer buy technology from American companies, such as Google, without a license. The US offered a reprieve to companies, allowing them to work with Huawei through temporary licenses to, according to the Commerce Department release, "afford consumers across America the necessary time to transition away from Huawei equipment, given the persistent national security and foreign policy threat".

After that rule was imposed, Huawei took steps to reduce its reliance on American chip manufacturers like Qualcomm and ramp up its in-house production through a chip unit, HiSilicon. But HiSilicon relies on outside manufacturers to mass-produce chips to its specifications, including the Shanghai-based Semiconductor Manufacturing International Corporation (SMIC), and, more importantly, the Taiwan Semiconductor Manufacturing Company (TSMC), the world chip manufacturing leader. TSMC uses American-made equipment to manufacture those chips.

So, in May 2020, the White House stepped up the pressure to deny Huawei access to global semiconductor supplies. BIS announced that foreign manufacturers using US chip-making equipment would need to get a license before being able to sell semiconductors to Huawei. This ban is far more draconian than the original measure. It is aimed at cutting off Huawei from the supply of the chips used in its base stations, servers and smartphones (which use TSMC chips at 98%), and thus its ability to provide 5G infrastructure. The blow became apparent in mid-July, when TSMC announced it was complying with US export regulations and had stopped supplying Huawei. The alternatives to TSMC are rare, as Samsung, the second chip manufacturer, will probably comply with the US export regulations too. Huawei will have then to rely on SMIC. But China's industry leader still lags far behind TSMC or Samsung in terms of technology. SMIC

has the ability to etch silicon chips with a fineness of 14 nanometers, compared to five nanometers for TSMC or Samsung.

Step 2: Charge Huawei with federal crimes

The US Justice Department has charged Huawei with a series of federal crimes.

The first indictment in 2019 accused Huawei of stealing cellphone testing technology from T-Mobile, to which it has been supplying phones for years. According to the indictment, a Huawei employee entered a T-Mobile testing lab, put a proprietary robot arm into his laptop bag, and walked out. The prosecution added that Huawei's culture of stealing secrets went deep. In July 2013, "Huawei China launched a formal policy instituting a bonus program to reward employees who stole confidential information from competitors," the indictment states. "Under the policy, Huawei established a formal schedule for rewarding employees for stealing information from competitors based on the confidential value of the information obtained." The policy "emphasized that no employees would be punished for taking actions in accordance with the policy".

The second indictment claimed that the company worked to bypass US sanctions on Iran. As part of its sanctions policies, US law prohibits US companies from selling technology to Iran, and it also prohibits companies in third-party countries from reselling US-made technology to Iran. Companies that flout that ban risk losing access to US-made technology altogether – a punishment the Trump administration briefly imposed on another Chinese smartphone giant, ZTE, over similar issues. US financial institutions are also prohibited from providing services to companies doing illicit business in Iran. This means, thanks to the dominance of the dollar in international exchanges and the fact that it has to be cleared by US financial institutions, that no foreign bank can finance any transaction with Iran.

Huawei is accused of selling technology to Iran via a shell company in 2012, using a Western bank. Huawei's chief financial officer, Meng Wanzhou, was arrested in Canada in December 2018 on a warrant issued by US authorities, who are looking to extradite her. She is accused of bank fraud for misleading HSBC about Huawei's relationship with a company operating in Iran, putting HSBC at risk of fines and penalties for breaking US sanctions on Tehran. In that case, the battle has taken a personal note; Meng Wanzhou is Huawei's founder's daughter. Since then, she has been under house arrest in Vancouver and has battled the decision in court. In June 2020, a Canadian court denied her attempt to dismiss the extradition request from the US.

Step 3: pressure US allies to keep Huawei out of their networks

To further weaken Huawei, the Trump administration is campaigning hard to keep the technology giant out of its allies' 5G networks, with success. But fears of Huawei being weakened by disruption in its supply chain is also a factor in governments' decisions.

Japan has blocked the use of Huawei equipment for its 5G network, as have Australia and New Zealand. In late June, Singapore chose Nokia and Ericsson as its main 5G network providers, leaving Huawei with only a minor role. Germany and other countries have yet to finalize decisions on Huawei. In France, Guillaume Poupard, head of the Agence nationale de la sécurité des systèmes d'information, declared to *Les Échos* in early July that there would not be a total ban on Huawei equipment. But he added: *“Operators who don't use Huawei, we're encouraging them not to do so, because that's kind of the natural direction of things. For those who are already using it, we are issuing licenses for a period of between three and eight years”*. So, while this may not be presented as a ban, the effect should be the same, as mentioned in a *Financial Times* article of August 19.⁴¹ French telecoms networks will be free of all Huawei gear by 2028 at the latest.

The UK is a particularly interesting case of successful diplomatic pressure by the US. In January, Prime Minister Boris Johnson granted Huawei a limited role in supplying kit for the UK's 5G networks, capping Huawei's market share to 35 per cent on the amount of non-core equipment, such as the kit on masts and rooftops. The rules also banned the use of the company's equipment in the critical core of mobile networks where data is stored and routed. But Johnson faced mounting pressure from Washington and from within his own party to exclude Huawei altogether. In June, he instructed officials to tighten restrictions on the company's involvement in the UK, and announced that it was examining possibilities for completely excluding Huawei from its 5G network by 2023. Finally, in July, UK mobile providers were banned from buying new Huawei 5G equipment after 31 December, and were told to remove all of the Chinese firm's 5G kit from their networks by 2027. The seven years is longer than expected, but takes into account the concerns of the industry, which has warned of the risks of service blackout and the time needed to remove all Huawei equipment from its telecom network.

41. B. Hall, “Emmanuel Macron's Low Profile on China Is Strategic”, *Financial Times*, August 19, 2020, available at: www.ft.com.

Step 4: target Huawei employees

In the latest move, in July, US Secretary of State Mike Pompeo announced that the US would restrict US visas for employees of Huawei and other Chinese firms if they were involved in human rights abuses. “Telecommunications companies around the world should consider themselves on notice: If they are doing business with Huawei, they are doing business with human rights abusers,” Pompeo said.

Meanwhile, the ban on Huawei is costly for European countries. In the UK, the government declared that its new policy is expected to add \$2.6bn to the cost of a full 5G rollout.

Conclusion

After three years, Huawei is still standing, albeit weakened. According to Eric Xu, its chairman, its annual revenues undershot expectations by \$12bn last year. But Huawei continues to perform relatively well financially: it reported in July an increase of 13% in sales in the first half of 2020, down from 23% a year earlier, but its profit margin improved from 8.7% to 9.2%. One reason is that, according to a study by GreyB and Amplified,⁴² “Exploration of 5G Standards and Preliminary Findings on Essentiality”, Huawei owns the most patents on 5G technology, ensuring that the Chinese company will get paid despite the Trump administration’s efforts to erase it from the supply chain. However, the fact that it does not have access to last-generation microchips anymore will affect it greatly in 2021, even if it has built inventories.

42. More information at: www.greyb.com/5g/.

On the Chinese Side

Innovation in China and its Structural Challenges

John Seaman

China has not shied away from advertising its goal of achieving global technological leadership by 2049, the centennial anniversary of the founding of the PRC. Through a steady stream of industrial policies, from “Made in China 2025” to “Internet +” to “China Standardization 2035” and beyond, it has sought to boost its technological prowess and stoke indigenous innovation in an effort to escape the dreaded “middle-income trap”. More fundamentally, innovation is seen as a driver for development. Massive investments and rapid advances in areas such as 5G, the Internet of Things (IoT), artificial intelligence (AI) and quantum communications suggest that China has made strong progress toward achieving its goals on the technological front.

Yet, despite its apparent success, there is still debate as to whether China’s progress is real, or simply that of a “paper dragon”, wherein substantial resources have been invested in line with government policies aimed at promoting innovation, but that commercial performance fails to live up to expectations.⁴³ A review of indicators of innovation input and output suggests that China’s progress has certainly been tangible, but remains mixed on the whole. At the same time, there is evidence that China’s state-directed innovation drive has had deleterious effects on innovation globally, and in the United States and Europe in particular.⁴⁴ In this context, calls to confront China more forcefully in areas such as technology transfer and intellectual property protection⁴⁵ have been met by hopes that, as China’s capacity to innovate grows, its policies and actions relative to these

43. S. Kennedy (ed.), “China’s Uneven High-Tech Drive: Implications for the United States”, *Report of the CSIS Trustee Chair in Chinese Business and Economics*, Center for Strategic and International Studies, February 27, 2020, available at: www.csis.org.

44. R. D. Atkinson, *Innovation Drag: China’s Economic Impact on Developed Nations*, Information Technology & Innovation Foundation (ITIF), January 2020, available at: <https://itif.org>.

45. Office of the United States Trade Representative, *Findings of the Investigation into China’s Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974*, Washington, D.C.: US Trade Representative, March 22, 2018.

issues will also increasingly shift to reflect those of technologically advanced economies, as the need to protect Chinese innovations develops.⁴⁶

More fundamentally, there is a question as to whether China's state-driven model and hardening political climate can sustainably create the conditions in which innovation can flourish. Will the country's drive for technological leadership and the limits of its state-driven model finally incite much-anticipated market reforms and recharacterize the relationship between the state and economic actors in the PRC? Despite some progress at the margins, this remains to be seen, and is on the whole unlikely in a context of a hardening of China's Party-state apparatus and deepening strategic rivalry with the United States.

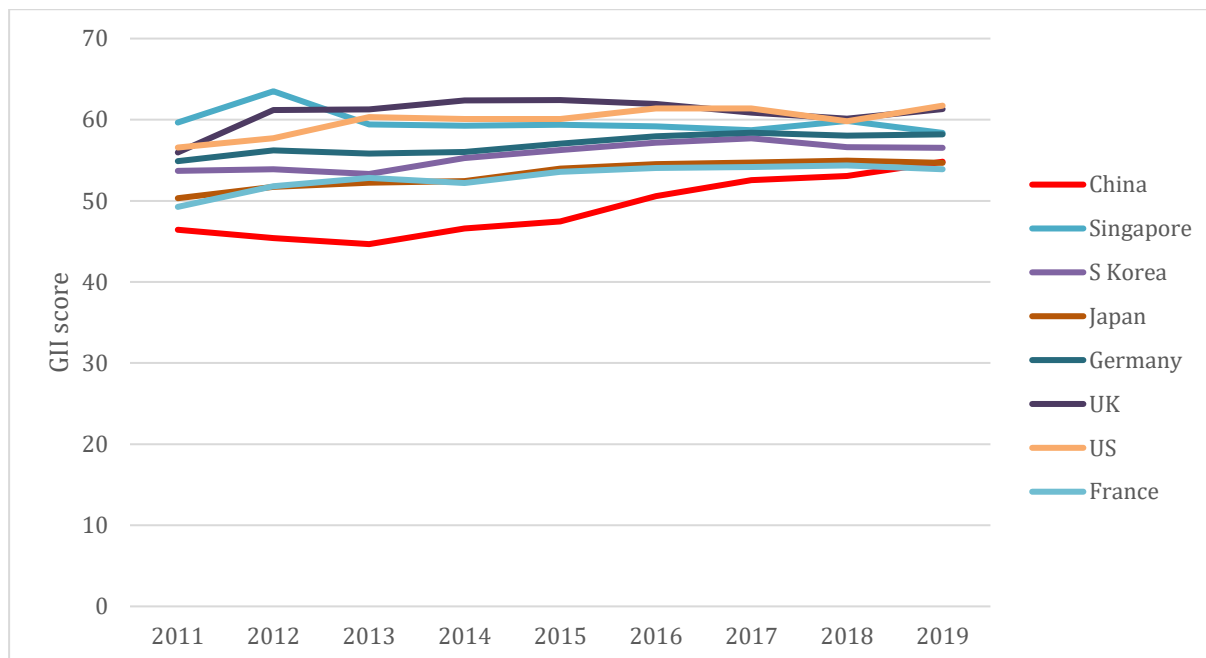
China's tangible, but mixed progress on innovation – a review of input and output indicators

On the surface, China has made steady progress in fostering the growth of its innovative capacity. The Global Innovation Index (GII), a set of 103 indicators assembled by Cornell University, INSEAD and the World Intellectual Property Organization (WIPO), demonstrates that over the last decade China has rapidly moved up the ranks of innovative capacity relative to its peers – from 35th in the world as late as 2013 to 14th in 2019, surpassing both France and Japan.⁴⁷

46. Y. Huang and J. Smith, "China's Record on Intellectual Property Rights Is Getting Better and Better", *Foreign Policy*, October 16, 2019, available at: <https://foreignpolicy.com>.

47. S. Dutta, B. Lanvin, and S. Wunsch-Vincent (eds.), *Global Innovation Index 2019*, Cornell University, INSEAD, and the World Intellectual Property Organization, 12th Edition, 2019, available at: www.wipo.int.

Comparative Scoring on Global Innovation Index (GII) for Select Countries

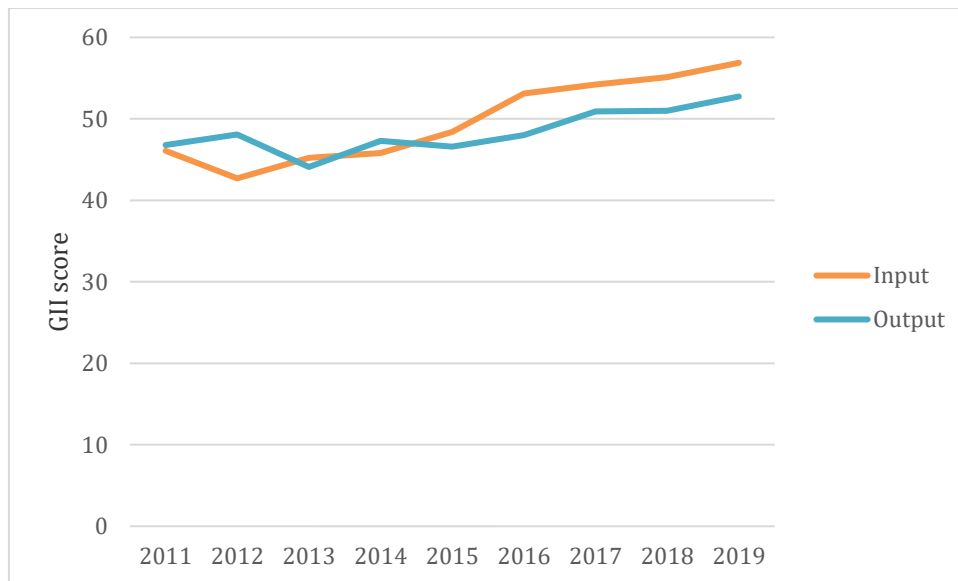


Source: Global Innovation Index 2019.

Progress in China's innovation inputs and outputs also suggests a degree of marked improvement. In 2019, China ranked 5th in innovation output, up from 21st as late as 2015 – surpassing Germany and inching ever closer to the United States. At the same time, China's progress has been more measured in inputs to innovation, which not only account for figures such as R&D expenditures, infrastructure development and market scale, where the country has excelled in recent years, but also the level of tertiary education and structural elements such as the overall regulatory and institutional environment and environmental performance, where it has lagged. A widening gap between inputs and outputs in recent years also suggests a dimension of waste related to recent policy initiatives, leading some to refer to China as a “fat tech dragon”.⁴⁸

48. S. Kennedy, “The Fat Tech Dragon: Benchmarking China's Innovation Drive”, *China Innovation Policy Series*, Center for Strategic and International Studies, August 29, 2017, available at: www.csis.org.

China's GII Input and Output Scores



Source: Global Innovation Index 2019.

Despite the overall signs of progress from these indicators, a closer look at patents and intellectual property creation, an important factor in measuring innovation output, serves to further nuance China's success. In 2018, China's official tally of patents for the year exceeded 2.3 million, the highest in the world.⁴⁹ However, a large number of these patents are utility models (63%), which are deemed as low-quality and do not constitute innovation *per se* in that they do not represent new knowledge or technology. Moreover, despite exceptions in sectors such as 5G and the strength of companies like Huawei, international patent holdings by Chinese companies remain remarkably low, with more than 95% of patents being filed in China. Domestic patent filings in Korea, for instance, account for 73% of all patents filed by Korean companies. Figures are even lower for domestically listed companies in the US (67%), Japan (62%) and Europe (53%).⁵⁰ As the cost of international patent filing is high, a low level of international applications suggests that most Chinese companies consider that their products are not worth protecting abroad.⁵¹ Furthermore, China's large trade deficit in royalties and fees paid for intellectual property rights, which exceeded \$30 billion in 2018,⁵² indicates that China's reliance on

49. China National Intellectual Property Administration (CNIPA), *Monthly Statistics Reports*, accessed on June 2020 at: <http://english.cnipa.gov.cn>.

50. *IP5 Statistics Report 2018 Edition*, Korean Intellectual Property Office (ed.), October 2019, p. 37, available at: www.fiveipoffices.org.

51. M. Qiu, "A Larger but Not Leaner Fat Tech Dragon", in: S. Kennedy (ed.), "China's Uneven High-Tech Drive: Implications for the United States", *op. cit.*, p. 8, available at: www.csis.org.

52. "Charges for the Use of Intellectual Property, Payments (BoP, Current US\$) - China", *Balance of Payments Statistics Yearbook*, World Bank, accessed on June 25, 2020, <https://data.worldbank.org>.

foreign technology remains consequential, and that the attractiveness of Chinese innovations on the whole remains low.

Technology transfer and intellectual property protection – progress or wishful thinking?

A major concern related to China's drive for technological leadership is the role that forced technology transfers and intellectual property theft has played in the country's economic transformation in recent decades. In both of these areas, China has markedly improved over time, but still has significant room for progress.

Some have estimated that intellectual property (IP) theft by Chinese companies has cost US counterparts anywhere between \$225 and \$600 billion annually,⁵³ though calculating the real impact of such practices is nearly impossible, particularly as many of these losses are calculated based on sales that would have theoretically taken place.⁵⁴ Yet, despite the hefty criticism, IP protection is one area where China has demonstrated considerable progress in recent years. Since China's first IP law was drafted in 1984, the Chinese government has been improving IP protection laws and their implementation, with regard to both Chinese and foreign firms. One particular area of progress has been the establishment of IP courts. In 2014, China reached what many consider to be a significant milestone when it established three specialized courts in Beijing, Shanghai and Guangzhou for dealing with IP infringement cases. It later added special tribunals in 18 other cities in 2017 and set up a special appellate tribunal in the Supreme People's Court in January 2019. The number of cases that appear before the courts has been rising by an average of 40% per year over the last three years; officially, there were more than 480,000 filings in 2019, almost 98% of which were concluded.⁵⁵ On the one hand, this reflects greater demand from Chinese economic actors to protect the increasing value of their investments and knowledge creation – which the high number of patent filings cited earlier indicates. On the other hand, it reflects an expectation from Chinese authorities that Chinese firms will need to employ and commercialize their

53. "The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy", *Update to the Report of the Commission on the Theft of American Intellectual Property*, National Bureau of Asian Research, 2017, available at: ipcommission.org.

54. J. A. Lewis, "Put China's Intellectual Property Theft in a Larger Context", *CSIS Commentary*, Center for Strategic and International Studies, August 15, 2017, available at: www.csis.org.

55. "Report Shows China's Greater Judicial Protection of IP in 2019", Supreme People's Court of the PRC, 29 April 2020, available at: <http://english.court.gov.cn>.

assets in order to compete in a global environment.⁵⁶ Interestingly, some preliminary analyses also suggest that foreign patent holders are just as likely to adjudicate cases in China as local patent holders, and in many instances even enjoyed higher win rates, better injunction rates and larger payouts.⁵⁷

These changes have been reflected in improved foreign investor sentiment regarding IP protection in recent years. In the most recent survey by the US-China Business Council, nearly 60% of US businesses reported an improvement in China's IP rights (IPR) protection. Nevertheless, more than 90% remain concerned about issues of enforcement.⁵⁸ Similar trends have also been noted in recent surveys of European businesses. Nearly 40% of respondents to the most recent survey of the European Chamber of Commerce in China considered enforcement of China's IPR laws to be adequate or excellent (up from 5% a decade ago), but one third of respondents also reported IP infringements, with over 50% taking place in the last one or two years.⁵⁹ While the development of China's IP courts is a clear sign of progress, one quarter of European business reported that they would refrain from bringing their latest technologies to China, with 36% indicating risks of IP infringement. This indicates a remaining gap in foreign investor confidence, particularly in sensitive sectors. Indeed, the Index of Patent System Strength developed by the University of Liverpool and the Copenhagen Business School suggests that China remains in the "very weak" category, citing ineffective customs and law enforcement, suggesting that foreign investors continue to encounter significant difficulties around patent enforcement.⁶⁰

Meanwhile, pressing for technology transfers in exchange for market access, primarily by requiring the establishment of joint ventures, has long been a central feature of China's industrial policy. Yet, there has also been notable progress in this area over the years. Since 1986, when China's first legislation was adopted allowing for wholly-owned foreign investment in select sectors, the volume of joint ventures in foreign investment entering China has steadily diminished, particularly as China liberalized in the

56. A. Malkin, "Beyond 'Forced' Technology Transfers: Analysis of and Recommendations on Intangible Economy Governance in China", *CIGI Papers*, No. 239, Centre for International Governance Innovation, March 2020, available at: www.cigionline.org.

57. R. Bian, "Many Things You Know about Patent Infringement Litigation in China Are Wrong", *SSRN*, October 1, 2017, available at: <https://papers.ssrn.com>.

58. "Member Survey: US-China Business Council", The US-China Business Council, August 2019, pp. 14-15, available at: www.uschina.org.

59. "Business Confidence Survey 2020: Navigating in the Dark", European Union Chamber of Commerce in China, 2020, p. 43, available at: www.eurochamber.com.cn.

60. "Index of Patent System Strength", School of Management, University of Liverpool, available at: www.liverpool.ac.uk.

context of its accession to the World Trade Organization (WTO), which was formalized in 2001. By 2014, over 80% of foreign direct investment (FDI) was wholly foreign-owned, though this has fallen towards 70% in more recent years as FDI shifted towards sectors that remain restricted in China.⁶¹ In January 2020, a new law on foreign investment entered into force that is expected to improve the situation further, as it formally bars forced technology transfer as a practice and increases the number of sectors where joint ventures are no longer required for foreign investors.⁶²

Nevertheless, substantial problems remain in the field of technology transfer, particularly in certain “strategic” sectors where Chinese firms have remained less competitive. Between 2017 and 2019, the number of European businesses that were reportedly compelled to transfer technology in exchange for market access doubled from 10% to 20%, with 63% reporting incidences in the last two years.⁶³ While the overall figure dropped to 16% in 2020, a sectoral analysis reveals that pressure to transfer technology is proportionally higher in sectors where European competitiveness is particularly pronounced, for instance in medical devices, aerospace and aviation, petroleum and chemicals, pharmaceuticals, the automotive industry and the environment.⁶⁴ In its recent China strategy paper, Business Europe noted that, while China’s most recent foreign investment law gives a positive signal with regard to administrative measures to tackle the problem, it is loosely worded and has seemingly weak enforcement measures. Meanwhile, the law may do little to address loopholes and non-administrative means of obtaining technology transfer (to include acquisitions through outbound investment, technology licensing and commercial espionage).⁶⁵

Given the experience of foreign companies in China, it seems we are currently in a two-tiered system. In sectors where China has succeeded in developing a strong comparative advantage, IP protections are more easily afforded and the impetus for technology transfer is lessened. Meanwhile, a separate set of practices persists in areas where Chinese competitiveness is relatively weaker and where knowledge and technology transfer continues to play an important role in facilitating China’s economic transformation.

61. N. Lardy, “Does China Force Foreign Firms to Surrender Their Sensitive Technology?”, *China Economic Watch*, Peterson Institute of International Economics (PIIE), December 10, 2018, available at: www.piie.com.

62. “Foreign Investment Law of the People’s Republic of China”, *NPCObserver*, January 1, 2020, available at: <https://npcobserver.com>.

63. “Business Confidence Survey”, European Union Chamber of Commerce in China, 2019, pp. 30-31, available at: www.europeanchamber.com.cn.

64. “Business Confidence Survey 2020: Navigating in the Dark”, *op. cit.*, 2020, p. 43.

65. “The EU and China – Addressing the Systemic Challenge”, Business Europe, January 2020, p. 83, available at: www.businesseurope.eu.

Innovation and political control in China

China's structural shift in the direction of an innovation-driven economy and the reforms it has enacted on the regulatory front with regard to IPR and technology transfer are often cited as evidence that the PRC is on a constructive path. Indeed, history suggests that countries do not develop strong IP protection regimes until their economies demonstrate formidable innovative capacity, displacing a reliance on foreign technology and knowhow with home-grown sources of innovation. Concerns about IP theft accompanied the recent rise of Japan, South Korea and Taiwan, for instance, until their per-capita incomes rose above \$20,000–25,000.⁶⁶ China's per-capita income today has barely breached \$8,000, though there is considerable difference of scale. Even the United States was an "imitation economy" for the better part of a century, as it caught up with the industrial revolution, subsequently enacting the International Copyright Act of 1891 that finally accorded legal protections to foreign innovations.⁶⁷ In this sense, while China's nefarious practices should not be ignored, some argue that the level of protections accorded to Chinese and foreign businesses, and the differences between them, reflect the relatively less-advanced stage that China is at with regard to innovation compared to other technologically advanced economies. If history is a guide, policy changes will evolve as the needs of China's economy evolve.

Yet, there is a fundamental difference between the structural role that China's Party-state plays, and will likely continue to play in the economy, and the examples cited above. Despite the great expectations that followed the 3rd Plenum of the 18th Party Congress in 2013, when China's leadership signaled a move toward deep structural reforms, China has broadly moved toward a hardening of state and Party control over the economy and society under Xi Jinping. It was long thought that a state-capitalist model would not be conducive to innovation, and that, to emerge as a technological powerhouse, China would have to loosen the reins of political control. If this were the case, indeed, we might expect China to follow the historical trend. But while China is still not the global technological leader it aspires to be, it has thus far demonstrated that technological breakthroughs and innovation are possible in a more constrained political environment. In fact, they may

66. Y. Huang, *Cracking the China Conundrum: Why Conventional Economic Wisdom Is Wrong*, New York, Oxford University Press, 2017.

67. M. W. Peng, D. Ahlstrom, S. M. Carraher, and W. (Stone) Shi, "History and the Debate over Intellectual Property", *Management and Organization Review*, Vol. 13, No. 1, March 2017, pp. 15-38, available at: www.cambridge.org.

even go hand in hand, particularly in network and data-driven areas where technology facilitates political control.⁶⁸

While China's development in the field of IP protection is therefore notable, it must also be considered in a context where there is a structural lack of independence on the part of the judiciary in China, wherein the operating principle is rule *by* law, rather than rule *of* law.⁶⁹ Judges are selected by local Communist Party of China (CPC) officials or party congresses and supervised by party organs.⁷⁰ IP courts may therefore operate on the basis of equity and fairness, until a case with political implications is presented or the broader political winds change. Likewise, as industrial policy is also a driving factor in China's technological development, the impetus for technology transfer is also at the service of broader political and strategic goals. These goals take on an added significance in a context of deepening strategic rivalry with the United States, where China's political leadership considers its legitimacy to be directly challenged by Washington. China's drive for indigenous innovation and increased self-sufficiency is not only aimed at boosting the prosperity of the Chinese people, but is also a strategic imperative in a context where CPC leadership has always been wary of deep interdependencies with the West, and the US in particular.⁷¹ Ultimately, China's internal political trajectory, coupled with increasingly antagonistic geopolitical realities, is likely to keep China on a different path towards innovation than what a classical historical narrative portends.

68. S. Heilmann, "Facing Up to China's State-Led Tech Revolution", *Nikkei Asian Review*, May 2, 2018, available at: <https://asia.nikkei.com>.

69. J. P. Horsley, "Party Leadership and the Rule of Law in the Xi Jinping Era", *Global China*, Brookings Institution, September 2019, available at: www.brookings.edu.

70. W. Weightmann, "China's IP System Was Improving Even before the Trade War", *China Business Review*, November 6, 2019, available at: www.chinabusinessreview.com.

71. J. Gerwitz, "The Chinese Reassessment of Interdependence", *China Leadership Monitor*, June 1, 2020, available at: www.prcleader.org.

Doing Business in China European Companies' Misadventures in the PRC

Laurence Nardon and Mathilde Velliet

Even though the mood in the West has turned to a degree of distrust towards China, the PRC remains a very attractive market and production hub for European companies. However, European companies of all sizes and in all sectors have experienced numerous challenges when operating in the Chinese market, generally due to a lack of understanding of the political, social and business environment. It can indeed be difficult for European operatives in China to read the low-level or weak signals that could lead to a difficult situation regarding their investments, contractual relations, shareholding, or protection of intellectual property.

In recent years, reforms have been implemented in China to ease market restrictions and reduce intellectual property rights (IPR) infringements. But their impact often remains limited for European companies, which also have to face obstacles stemming from the recent resurgence of China's state-owned sector and the increasing politicization of business.

This article aims at offering a typology of the major challenges European companies face when doing business in China. It uses case studies from a wide range of industrial sectors covering various types of technologies – from the aerospace to the fashion, food and energy industries.

The most common problems faced by European companies in China revolve around the following major issues.

Underestimating the importance of politics in Chinese trade and business life

Inescapable links between Chinese executives and the Communist Party

In the PRC, the Chinese Communist Party (CCP) and the Chinese business community are closely tied, in what is often a clear superior-subordinate relationship. Many Chinese executives, especially at a high level, are members of the CCP. As underlined in a 2018 report on Chinese corporate governance, “the same individual who is chairing a party committee meeting on a Monday might well be chairing a board meeting later in the week.”⁷² These close ties characterize not only Chinese (private and state-owned) enterprises, but also foreign companies. For instance, at a time when the links between the CCP and Huawei’s founder have come under increased scrutiny,⁷³ it is worth shedding light on some of its rival companies’ ties to the CCP: the Scandinavian telecom companies Nokia and Ericsson both have party members in their subsidiaries in Chinese teams. Several directors of Nanjing Panda Electronics, Ericsson’s joint venture (JV) partner in China, hold CCP positions; and the chairman of Nokia Shanghai Bell is also the secretary of the company’s party branch.⁷⁴ Such political affiliation undoubtedly influences the decisions of Chinese executives, and therefore should not be overlooked by their Western partners.

Increased CCP pressure on foreign enterprises

More generally, the level of CCP control over business activities in China has drastically increased since Xi Jinping took power in 2012. If party organizations in joint ventures or foreign-owned enterprises⁷⁵ had previously no management or governance role, some have recently demanded more power. Several European executives in China explained

72. R. McGregor, “How the State Runs Business in China”, *The Guardian*, July 25, 2019, available at: www.theguardian.com.

73. For more on this, see Marion Welles’s case study of Trump vs. Huawei in the present report, p. 33-39.

74. Telesoft, “Nokia and Ericsson Have Links to China’s Communist Party,” *Telecoms Tech News*, August 13, 2018, available at: <https://telecomstechnews.com>.

75. Based on Chinese Company Law, CCP groups should be permitted to be created in foreign companies that employ three or more party members. See J. Laband, “Fact Sheet: Communist Party Groups in Foreign Companies in China”, *China Business Review*, May 31, 2018, available at: www.chinabusinessreview.com.

that they had experienced political pressure from party representatives, either to bring them in to the executive committee, to pay for party organization overhead expenses, or to revise the terms of their joint ventures to give more power to the party on business and investment operations.⁷⁶ The numbers show that this CCP pressure on European enterprises is far from anecdotal. In a 2020 survey of the European Chamber of Commerce, nearly 25% of European businesses operating in China reported having experienced political pressure from the Chinese government to join certain events or review internal policies to align with China's political agenda.⁷⁷ The pressure is especially acute when it comes to strategic issues such as those related to the "One China policy" or the Belt and Road Initiative (BRI). Indeed, the most common action that the Chinese government has pushed for is that European companies review their website to see if Hong Kong, Taiwan, and Tibet are listed as part of the People's Republic of China.⁷⁸ Supporting the pro-democracy movement in Hong Kong or expressing solidarity with the Uyghurs in Xinjiang are most likely to provoke reprisal from the authorities.

Among numerous examples, the recent cases of backlash – both by the Chinese government and by mainland Chinese consumers through social media – that European fashion houses have experienced illustrate the importance of sovereignty sensitivities in business life in China. Indeed, in 2019, the French luxury house Givenchy and the Italian company Versace have both had to apologize publicly for selling T-shirts on which Hong Kong and Macau appeared as independent countries.⁷⁹ Similarly, the Shanghai branch of the Chinese cyberspace administration accused the Spanish apparel retailer Zara of placing Taiwan in a pull-down list of countries on its Chinese website. Dior was also fiercely criticized for using during a presentation a map of the PRC which did not feature Taiwan. Beijing's strict policing of how foreign companies refer to these territories is expanding, and reaches far beyond the fashion sector.⁸⁰

76. M. Martina, "In China, the Party's Push for Influence inside Foreign Firms Stirs Fears", *Reuters*, August 24, 2017, available at: www.reuters.com.

77. European Union Chamber of Commerce in China, "European Business in China – Business Confidence Survey: Navigating in the Dark", 2020. p. 50.

78. 10% of the European companies that responded to the European Chamber of Commerce Business Confidence Survey reported that the pressure exerted by the Chinese government targeted such a review of their website; 12% that it aimed at securing their participation in the Belt and Road Forum or Initiative, and 8% that it encouraged them to review their social media policy related to employees and their postings. See European Union Chamber of Commerce in China, "European Business in China – Business Confidence Survey: Navigating in the Dark", *op. cit.*, p. 51.

79. E. Paton, "Versace, Givenchy and Coach Apologize to China after T-shirt Row", *The New York Times*, August 12, 2019, available at: www.nytimes.com.

80. Chinese authorities have indeed heavily criticized companies in a wide range of sectors (automobile, aviation, medical technologies...) for their "misrepresentations" of the Chinese territory. See B. Goh and

The noose tightens: reinforced security legislation and control on society

Since Xi Jinping took over in 2013, and even more since the 19th Party Congress of October 2017, a set of security laws has been passed to reinforce the CCP's control over society, both in mainland China and in special administrative regions such as Hong Kong.⁸¹ This package of legislation includes laws on Counterespionage (2014), National Security (2015), Counterterrorism (2015), Cybersecurity (2016), National Intelligence (2017) and, more recently, the PRC's National Security Law in Hong Kong (2020).⁸² This arsenal aims at strengthening the legal basis for Chinese security activities and require citizens and companies – Chinese and foreign – to cooperate with them. This political climate thus has numerous implications for foreign enterprises, which are concerned, in such a bridled environment, about having to share information on their employees or customers, as well as about the safety of their employees and partners. For instance, article 7 of the National Intelligence Law reads: “Any organization or citizen shall support, assist and cooperate with the state intelligence work in accordance with the law [...]”. Foreign companies are thus obligated by law to provide all the information required by the Chinese intelligence authorities for “national security and interests”.

Alongside this tightened security arsenal, the first years of Xi Jinping's leadership were characterized by massive CCP anticorruption campaigns – sometimes bordering on political cleansing – with a ripple effect potentially affecting European companies. Indeed, in sectors where joint ventures (JVs) are mandatory, such as the automobile sector, the consequences of anticorruption investigations targeting members of the local JV partner can be quite crippling for its European counterpart. At least a few thousands companies have been affected in the auto industry alone, the most famous example is that of Xu Jianyi, the head of Volkswagen's 40%-owned joint venture FAW group, who was arrested in 2015.⁸³ Among other examples in the medical industry, local units of China's State Administration for Industry and Commerce (SAIC) have charged Chinese executives at British drug maker GlaxoSmithKline with bribery and corruption and visited the offices

J. Ruwitch, “China Cracks Down on Foreign Companies Calling Taiwan, Other Regions Countries”, *Reuters*, January 12, 2018, available at: www.reuters.com.

81. Interview with Marc Julienne, Ifri, September 2020.

82. For mainland China, one could also mention the law on Foreign NGO Management (2016), the Ninth Amendment to the PRC Criminal Law (2015), the Management Methods for Lawyers and Law Firms (both 2016). See M. S. Tanner, “Beijing's New National Intelligence Law: From Defense to Offense”, *Lawfare*, July 20, 2017, available at: www.lawfareblog.com.

83. F. Mayer-Kuckuk, “Graft Crackdown: Head of VW's Chinese Venture Arrested”, *Handelsblatt Today*, March 17, 2015, available at: www.handelsblatt.com.

of Swiss drug maker Roche Holding AG, of Danish drug maker Novo Nordisk A/S, of British AstraZeneca Plc, and Belgium's UCB SA... In the telecom sector, the death of Jia Lining, the head of human resources at ASB (a joint venture between the French telecom company Alcatel-Lucent and China's state-owned investment arm), soon after he publicly denounced his superiors' corrupt practices, also illustrates the potential consequences of such campaigns for European companies' joint ventures.

Even though the evidence is more anecdotal in terms of sheer numbers, European entrepreneurs can also be targeted in such corruption or security-related investigations, sometimes leading to their detention. One of the executives of the British drug making company AstraZeneca was for instance detained after the Chinese police raided the firm's headquarters in Shanghai.⁸⁴

Unequal opportunities: market access restrictions and preferential treatment of Chinese state-owned and private companies

Another longstanding issue put forward by companies and governments, especially from the West, is China's insufficient commitment to market opening reforms, and unfair competition between Chinese and foreign firms.

Unfair competition against favored Chinese state-owned and private enterprises

If over the past forty years, incremental market-opening reforms have been initiated in some areas, they have largely been overshadowed by the continued predominance of state-owned enterprises (SOEs) in many sectors, which still hold a clear advantage over private firms in market access, taxes, government financing, communication with the government and public procurement. This division between sectors, particularly penalizing for Europeans in technology-related areas, had led some observers to conclude that the PRC is moving towards a "one economy, two systems" model: "on one side, market forces and modern regulatory mechanisms look increasingly international; on the other, critical sectors of the economy are dominated by state-owned national champions, while private enterprises are at best stifled or at worst forced out of the market

84. L. Robin, "AstraZeneca Executive Detained after Chinese Police Raid Shanghai HQ," *The Independent*, July 23, 2013, available at: www.independent.co.uk.

entirely.”⁸⁵ This dichotomy may be aggravated by the Covid-19 crisis, which could reinforce the government’s support for SOEs as a source of stability in these uncertain times, draining even more resources from the private sector.

To a different degree, even in the private sector, Chinese companies often benefit from numerous advantages over foreign companies, such as privileged access to loans, tax benefits and subsidies.⁸⁶ Furthermore, while procurement laws heavily encourage the purchase of Chinese goods and services, foreign enterprises are penalized by direct and indirect market restrictions.

Direct market restrictions

In addition to this unfair competition against Chinese SOEs, European companies operating in China still face persistent direct and indirect market access restrictions.

The year 2019 saw a number of seemingly important reforms: the Special Administrative Measures on Access to Foreign Investment were revised in July, as well as their equivalent for free trade zones (FTZs), and the Negative List for Market Access (which defines market access for all businesses, domestic and foreign) was updated. Nevertheless, the impact of these reforms has been marginal for European companies, and limited to a few sectors. Critical sectors such as oil and gas exploration, aerospace, IT and telecom saw little improvement.⁸⁷

Indirect market restrictions

Furthermore, for European businesses in China, indirect barriers (such as opaque licensing procedures, or other complicated administrative approvals) remain twice as common as direct ones. Despite modest progress, such as improved bureaucratic procedures, the regulatory environment in China is still perceived by European companies as unpredictable, with ambiguous regulations enforced in a discretionary way. If the Chinese government seems willing to ease some restrictions on foreign companies, it has yet to push the universal implementation of these reforms. In the meantime, local governments are often reluctant to enforce regulations that may weaken Chinese private and state-owned enterprises, and thus create a slump in local tax revenue. As a consequence, in 2020, 40%

85. “European Business in China – Business Confidence Survey: Navigating in the Dark”, *op. cit.*, p. 2.

86. P. Allard, “La Chine, championne technologique ou géant empêtré ?”, *Politique étrangère*, Vol. 85, No. 1/2020, Spring 2020. p. 125

87. “European Business in China – Business Confidence Survey: Navigating in the Dark”, *op. cit.*, p. 12.

of European companies operating in China reported that regulations were implemented in an unfair manner and that they received unfavorable treatment compared to domestic firms.⁸⁸

Forced technology transfers imposed by restrictions

By forcing foreign companies to form joint ventures with Chinese partners or to open assembly lines in China in order to access the Chinese market, many of these restrictions lead to forced transfers of technology from European to Chinese companies. This has been the case for many companies,⁸⁹ particularly those dealing with high-end technologies (hospitality, education, medical devices, aerospace, transportation, logistics and distribution, automobile...), which face high compelled tech transfer rates.⁹⁰

The case study of Spanish wind turbine manufacturer Gamesa provides a clear example of the consequences of such market access restrictions on European companies operating in China. Gamesa is an old-line machinery company which entered the wind turbine business in 1994, and managed to control more than a third of the Chinese wind turbine market by 2005.⁹¹ However, on 4 July 2005, the National Development and Reform Commission – China’s main economic policy agency – announced that Chinese wind farms were now required to buy equipment in which at least 70% of the value was manufactured domestically rather than imported. This new restriction, known as “Notice 1204”, forced Gamesa to teach local suppliers how to make different steel forgings and elaborate electronic controls, thereby transferring its technology and know-how to Chinese companies so as to maintain its access to the Chinese market. These suppliers then started to sell parts to Gamesa’s competitors, which were already aided by low-interest loans and cheap land from the PRC government, as well as by preferential contracts with state-owned power companies (the main buyers of wind turbines).⁹² Five years after Notice 1204, these Chinese companies controlled more than 85% of the Chinese market – while Gamesa’s share was down to 3%. As the New York Times summarizes, “Chinese companies acquire the latest Western technology by

88. *Ibid.*, p. 16.

89. 16% of European companies felt compelled to transfer technology in order to maintain market access in 2020 (against 20% in 2019). See “European Business in China – Business Confidence Survey: Navigating in the Dark”, *op. cit.*, p. 43.

90. For more on this topic, see John Seaman’s paper in the present publication, p. 26-32.

91. K. Bradsher, “To Conquer Wind Power, China Writes the Rules”, *The New York Times*, December 14, 2010, available at: www.nytimes.com.

92. *Ibid.*

various means and then take advantage of government policies to become the world's dominant, low-cost suppliers.”⁹³

Some argue that European aircraft manufacturer Airbus faces the exact same risk as it is building assembly lines in China. One final assembly line for the A320 opened in 2008 and one Completion and Delivery Centre for the A330 opened in 2017, both in Tianjin.⁹⁴ Among other factors, this local presence helped Airbus secure large deals with China's state buying agency, the China Aviation Supplies Holding Company, and access more easily the fast-growing Chinese market. Last year, Airbus agreed to sell 300 aircrafts to China in a deal worth tens of billions of dollars.⁹⁵ However, this is also a risky move, as all of Airbus's local partners are more or less directly linked to its Chinese competitor, the China Aviation Industry Corporation (AVIC). AVIC is a shareholder of the Commercial Aircraft Corporation of China (COMAC), which is developing a rival to the A320 called the C919. This puts Airbus (as well as other companies working in rapidly expanding markets, such as Gamesa) in a tricky position: “their problem is that their biggest customer wants to become their biggest rival”, Michael Goldberg of Bain & Company said.⁹⁶ This competition is all the more challenging for European companies given that, in strategic sectors (such as aerospace and renewable energy), the Chinese government is increasing pressure on domestic buyers (like airlines or wind farms) to use products manufactured in China in order to encourage the Chinese industry to move up the manufacturing value chain.

Enduring IPR infringements despite improvements in the R&D and innovation environment

Intellectual property theft

The case study of Airbus and its presence in the PRC also sheds light on another enduring issue for European companies: the risk of intellectual property (IP) theft. Indeed, alongside forced technology transfers, European companies have to protect their latest technologies from IP rights

93. *Ibid.*

94. Airbus official website: www.airbus.com. Accessed on September 9, 2020.

95. “China/France: Airbus Wins China Order for 300 Jets as Xi Visits France”, *Asia News Monitor*, March 27, 2019.

96. “We are Sorry to Announce; Chinese Aerospace”, *The Economist*, Vol. 421, No. 9014, November 5, 2016, pp. 65-58.

infringement, which 35% of them have already experienced despite notable progress in drafting and enforcing IPR-related regulations in recent years.⁹⁷ In the case of Airbus, as many as eight attempts at gathering information on the A320 assembly line are said to have occurred in its first year of operation in Tianjin.⁹⁸ However, the long history of problems regarding IP in China has led European companies such as Airbus to take all necessary precautions: the engine is still built in Europe, and the final assembly lines only represent 5% of the plane's added value, according to then-CEO of Airbus Fabrice Brégier.⁹⁹ Similarly, strategic European companies investing in R&D in China (such as the French firm Thales) tend to steer clear of research in dual-use technologies.

Even regarding trade secrets, many European companies report that the confidential business information they are required to disclose to access the Chinese market is not effectively protected from their competitors. According to the latest report of the European Commission on the global challenges of protecting IP, the opaque regulatory and administrative environment enables the Chinese government, “sometimes in coordination with Chinese joint-venture partners”, to extract foreign technology.¹⁰⁰ And, in cases of unfair commercial use and unauthorized business disclosure information, EU companies have difficulties obtaining effective protection before the courts.

Patents and problems

This same report also points out that, despite recent reforms, Chinese policies on patents remain quite challenging for European firms. Indeed, the Chinese authorities still grant questionable patents, frequently invalidate patents of foreign companies seeking legal protection against Chinese infringers, and encourage dense groups of IP rights in certain fields of technology (“patent-thickets”), which hamper the patentability and commercialization of new inventions.¹⁰¹

Chinese companies also often fail to pay adequate royalties when they use technologies protected by standard essential patents (SEPs) and owned by EU companies, such as the telecommunication standard ‘4G’.¹⁰²

97. *Ibid.* p. 43. For more on this, see John Seaman's paper in the present report, p. 43-51.

98. V. Lamigeon, “Pourquoi Airbus ouvre une usine en Chine pour son A330”, *Challenges*, September 23, 2017, available at: www.challenges.fr.

99. *Ibid.*

100. “Report on the Protection and Enforcement of Intellectual Property Rights in Third Countries”, Brussels, European Commission, January 8, 2020, p. 18, available at: <https://trade.ec.europa.eu>.

101. *Ibid.*, p. 17.

102. *Ibid.*, p. 17.

IP theft and patent infringements by Chinese competitors over European technology have therefore been a persistent concern for European companies in past decades. However, in the last ten years or so, the paradigm has been turned on its head: European enterprises are, in turn, increasingly facing (sometimes dubious) accusations of IP infringement, at a time when the number of Chinese patent applications is growing exponentially. As Catherine Sun, patent law expert at Foley & Lardner in Shanghai, explained in the *Financial Times*: “Normally we advise Chinese companies when they go to the US or Europe that they might be sued. We never advise foreign companies that come to China they might be sued – we tell them their product might be copied. Now we should tell them: Chinese companies are filing more patents locally. Foreign companies can face significant damages in China too.”¹⁰³

One of the first and most emblematic cases of this shift was the Schneider vs. Chint trial in 2007–2009. Schneider Electric, a French company specializing in electric energy and components, has been present in China since 1987. In 2006, it was accused of IP theft by its Chinese competitor Chint, which claimed that Schneider Electric produced low-voltage electrical elements based on a patent owned by Chint. Indeed, Schneider Electric owned the patent for these elements in France but had neglected to deposit them as well in China. As a consequence, in 2007, a Chinese court in Wenzhou ordered Schneider Electric to pay a €31m penalty, reduced to €23m after the 2009 agreement between the parties, with other undisclosed dispositions. The fact that Chint’s CEO Nan Cunhui had political connections – he was a member of the National People’s Congress – certainly played a role in the outcome of the trial. Many feared that a settlement of this magnitude would encourage Chinese patent owners to take legal action against foreign rivals.¹⁰⁴

Being squeezed out: a persistent risk for the European JV partner

Stemming from market access restrictions (such as mandatory joint ventures), and frequent IP infringements by Chinese companies (regarding patents, trademarks, designs, etc.), another risk faced by European companies in China is that of being evicted from their joint venture without fair compensation. According to Steve Dickinson, a China-based attorney in the international law firm Harris Bricken: “The standard fate for joint ventures in China is that once the Chinese JV partners either believe they no

103. P. Waldmeir, “Schneider Settles China Fight,” *Financial Times*, April 15, 2009, www.ft.com.

104. *Ibid.*

longer need their foreign joint venture partner or simply no longer want to share in the JV spoils with their foreign JV partner, they will work to drive the foreign partner out of the venture.”¹⁰⁵

The joint venture between the European group Danone and the Chinese company Wahaha is one of the most emblematic examples of how Chinese-European JVs can go wrong.¹⁰⁶ Group Danone SA is a Paris-based multinational corporation (MNC) which, since its founding in the late 1980s, has become a giant in the global dairy and bottled-water markets. In 1996, it entered its first joint venture with Hangzhou Wahaha Group Co., Ltd, a smaller company specialized in the production of supplemental nutrition drinks for children. Around 2006, it came to light that Wahaha's general manager Zong Qinghou had created a number of other companies outside the joint venture, which sold products under the Danone/Wahaha trademark. Danone thus filed lawsuits and arbitrations (first in Stockholm in 2007), but reciprocal accusations and personal attacks complicated the proceedings. After a few years of litigation in several countries, the two sides finally opted for an amicable settlement whereby Danone agreed to sell its part of the JV to Wahaha. According to an interview with the French daily *Les Echos* in March 2009, Danone demanded at that date €1.6bn for its 51% of the JV, but ended up agreeing to sell for a meagre €300m.¹⁰⁷ In addition to the lack of protection of the Danone-Wahaha trademark, Wahaha managed to drive Danone out because Zong Qinghou was a very strong opponent, with connections to the Chinese government, and in a position to appeal to Chinese consumers' patriotism. Combining trademark-law violation and joint-venture squeeze-out, the Danone-Wahaha example illustrates how loopholes in the protection of trademark owners and the overwhelming support of the Chinese public for local companies over foreigners can affect European firms.

Conclusion

This paper does not argue that Europeans should not invest in China nor that they should distrust Chinese partners. Many European companies still strike lucrative deals and develop fruitful collaborations in the rapidly growing Chinese market. Despite market restrictions and intellectual property issues, its sheer size makes it an attractive opportunity, still seen as

105. S. Dickinson, “The China Joint Venture Squeeze Out -- How It Works and How You Must Respond,” *China Law Blog*, August 27, 2019, available at: www.chinalawblog.com.

106. D. Barboza, “Danone Exits China Venture after Years of Legal Dispute”, *The New York Times*, September 30, 2009.

107. Y. Rousseau, “Danone perd son bras de fer avec Wahaha”, *Les Échos*, October 1, 2009, www.lesechos.fr.

unmissable in some sectors (aerospace, civil nuclear power, etc.). However, to avoid potentially major losses, European entrepreneurs should extensively study the regulatory environment, actively protect their company's IPR, and expect CCP attempts at influencing their decisions.

More importantly, wide-ranging negotiations should continue with the PRC in order to push for more progress towards a level playing field in China. Considering the size of the Chinese market, such efforts may not be fruitful unless they take place between China and a united European Union, rather than with individual member states. These past few years, ambitious public commitments – such as those on non-discriminatory market access during the 2019 EU-China Summit's statement, for instance – were not turned into concrete policies.¹⁰⁸ However, the EU has been adopting a tougher stance since March 2019, when the European Commission's report on China first qualified it as a “negotiating partner, [...] economic competitor, [...] *and systemic rival*” (emphasis added), and even more following China's behavior during the coronavirus crisis. The EU is currently pushing for the signing of a comprehensive EU-China investment agreement, originally planned during the Leipzig summit on 14 September but now postponed to the end of the year (at best). The EU goals in these talks are ambitious: eliminating equity caps, joint-venture requirements, and other limits on EU investment into China; securing non-discriminatory regulatory treatment relative to SOEs; achieving more transparency on state aid and subsidies, and restricting forced technology transfers.¹⁰⁹ If signed, such an agreement would fundamentally transform the position of European companies and investment in the PRC in the coming years.

108. “EU-China Summit Joint Statement”, Brussels, European Council, April 9, 2019, available at: www.consilium.europa.eu.

109. J. Brunsten and S. Fleming, “EU Warns China That Investment Talks Are Entering ‘Critical Stage’”, *Financial Times*, June 28, 2020, available at: www.ft.com.

On the European Side

The EU's Export-Control Regime Modernization

How to Best Reflect a Global Changing Reality While Maintaining the Competitiveness of EU Industry

Sofia Bournou

How has the world changed since 2009, when the EU's current Exports Controls on Dual Use Items Regulation entered into force? How can these developments be best reflected in the EU's regime? Four years after the launch of the process by the European Commission to modernize the EU regulation, these remain the key axes of discussion. However, despite general recognition of the need to update the regulation, decision-makers – the member states in the Council and the European Parliament – have not yet found common ground.

Traditionally, the objective of the control of dual-use trade – concerning goods, services and technologies that can be used both for civilian and military purposes – is to prevent the proliferation of weapons of mass destruction (WMD) and to contribute to the mitigation of security risks. In practice, export-control regimes, including the EU one, work on the basis of lists. Dual-use items are divided into categories. Depending on the category each dual-use item belongs to, a set of rules – or criteria – applies when they are exported, transited or brokered. For instance, all items included in Annex I of the EU's export-control regulation are subject to export authorization. The destination country also plays a role, as controls may be in place in certain cases. Annex II of the regulation covers these cases. For example, while Annex IIa allows exports of dual-use items listed in Annex I to a specific list of countries, including Australia, Canada, Japan and the US, Annexes IIb and IIc allow exports of certain dual-use items to a list of destinations if specific conditions and requirements are fulfilled.

It is important to note that many export-control regimes, such as the EU regulation, also include provisions to cover cases where exports of dual-use items not included in the lists may raise humanitarian risks. These are the so-called “catch-all controls”. In the case of the EU, authorizations are granted by member states’ competent authorities for specific items and end-users not included in the lists in the annexes of the regulation.

The weaponization of trade policy

Export controls on dual-use items is an area where security and economic policy objectives come together, in an increasingly complex relationship. On the one hand, the emergence of new technologies brings opportunities for growth and contributes to the production and delivery of high-end goods and services in all areas of the economy. Dual-use items can contribute substantially not only to the information and telecommunications sectors, but also to other sectors, directly or indirectly, such as the chemicals, pharmaceuticals and even automotive sectors. On the other hand, security risks have also increased, including cyber-security threats and human rights violations, for instance, by oppressive regimes.

More recently, the Covid-19 pandemic has further underlined the need to look at ways to balance the benefits and risks of these technologies, including through export controls. But it has also accelerated a more structural policy shift: the increasing weaponization of trade policy to fulfil other policy objectives. For instance, the two most prominent trading partners of the EU, the US and China, have developed an increasingly assertive stance in dual-use trade.¹¹⁰ Taking the example of the US, the so-called “technological decoupling” from China has led to the adoption of a number of measures¹¹¹ with detrimental effects. With its *America First* motto, the current US administration does not hide the ultimate purpose of these policies, which is to ensure American leadership in high-end products and technologies. However, given the extraterritorial nature of the US legislation, the impact of this approach is global, as companies, including American ones, rely on global trade and supply chains to deliver new, innovative goods and technologies. At the same time, China is also working on the adoption of its own export-control legislation. The overall

110. B. Dekker and M. Okano-Heijmans, “The US–China Trade–Tech Stand-Off and the Need for EU Action on Export Control”, *Clingendael Report*, Clingendael, August 2019, available at: www.clingendael.org.

111. Introduced in 2018, the Export Control Reform Act (ECRA) updated the US export-control regime. Several pieces of the legislation are in the process of further development, including measures related to “emerging technologies” and “foundational technologies”, concepts still poorly defined.

objective of the “Made in China 2025” strategy is also to achieve a leadership position in critical areas of the economy, including those relevant to dual-use trade. Furthermore, taking a leaf out of the US policy-making book, China’s export-control law is very likely to have extraterritorial application, therefore having an impact on non-Chinese companies.

Where does the EU stand in this context? Some voices argue that adopting a “Europe first” strategy is the right way forward. They suggest that becoming self-sufficient in areas considered strategic – such as information technologies, communications infrastructure, energy or health, which are all relevant areas in the current debate on dual-use trade – would help the EU to become a global leader. Nevertheless, from the perspective of European business, we would be cautious about such approaches. Trade should not be perceived as a zero-sum game, but rather as a key enabler for growth and jobs, and a driver for research and innovation. The EU is and will remain dependent on access to raw materials, intermediary goods and final products, as well as services. From this point of view, it is not only impossible but also unrealistic to seek self-sufficiency. The concepts of “open strategic autonomy”, as put forward by the European Commission, or “smart technological sovereignty”, coined by BusinessEurope, are better placed to ensure that the EU continues to pursue an open trade policy, yet a more strategic one.¹¹² Refraining from the adoption of protectionist measures, what is critical is to have the right conditions in place to help companies take better-informed decisions, maintain their access to global supply chains and contribute to the EU assuming a leadership position. A combination of instruments under different policies – trade, industrial, innovation, employment – are necessary to achieve the most effective results.

Balancing European security and economic goals

Going back to the question of how the EU’s export-control regime should be updated in the current policy environment, the view that the EU’s approach should continue to strike the right balance between security and economic policy objectives prevails among businesses. In other words, the increased attention in the European Commission’s proposal of 2016 on the human security approach should be carefully balanced with measures to support the competitiveness of EU industry globally.

112. Business Europe Position Paper, *Smart Technological Sovereignty: How It Could Support EU Competitiveness*, June 25, 2020, available at: www.busesseurope.eu.

To offer an example, in an area such as dual-use trade, the private sector is considered the first line of defense. Companies on the ground can often acquire information about potential security risks, including human rights violations. However, even with increasingly sophisticated systems of due diligence in place, access to such information is not a given, or without challenges. Due diligence is a process, not an end in itself. It should not be perceived as a ticking-the-box exercise but as a results-oriented one, measured against the continuous efforts of companies to increase transparency and effectively address risks in their supply chains. It should also give the necessary flexibility to companies to adapt their due-diligence processes depending on their size, position in the supply chain and the markets they trade with and/or operate in.

These concerns are not met by the 2016 proposal.¹¹³ The current Regulation of 2009 already provides the framework to address risks related to human rights by allowing EU member states to prohibit or impose export authorization requirements for reasons of public security or for human rights considerations.¹¹⁴ Nevertheless, the way the concept of due diligence in the area of human rights is introduced in the 2016 proposal¹¹⁵, instead of clarifying the exporters' obligations, increases uncertainty in the conduct of their business and their liability in the context of the EU regulation. Where do the exporters' obligations stop and where do the governments' obligations begin? The responsibility of the private sector to respect human rights and to contribute to their protection in the frame of their activity is clear, and international standards agreed by the United Nations and the Organisation for Economic Cooperation and Development (OECD) apply in this regard. It is also clear, however, that the responsibility of the state cannot be undermined by placing an additional burden on businesses.

Unless this is addressed in the ongoing legislative process to modernize the EU's regulation, the risk of overcompliance is elevated, as companies will very likely decide to go beyond what is necessary to mitigate compliance risks and avoid possible penalties. Furthermore, the administrative burden for both exporters and member states' competent authorities would increase in a similar manner. Companies, trying to

113. European Commission, Proposal for a Regulation setting up a Community regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (recast), September 2016, <https://eur-lex.europa.eu>; Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, consolidated version of 2017, <https://eur-lex.europa.eu>.

114. Article 8, Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, consolidated version of 2017.

115. Article 4, Proposal for a Regulation setting up a Community regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (recast), September 2016.

ensure their compliance with the regulation, will submit more requests for licenses, especially under the category of catch-all controls. In addition, it cannot be excluded that competent authorities may deny licenses, even in those cases where there is no clear proof of human rights violations. This may have a significant impact on the competitiveness of EU companies, as their competitors in other jurisdictions would not be obliged to follow similar rules. Moreover, besides the economic impact, the human security risks may not be effectively mitigated. As is often said, global problems require global solutions. Therefore, it is important for the EU to ensure that our trading partners follow our lead and that the EU is not left fighting alone.

The effectiveness of multilateralism and international cooperation

In this regard, multilateral efforts to control exports of dual-use items should not be undermined. There is a vast network of national and international regimes, including the UN Security Council Resolution 1540 or the Wassenaar Arrangement,¹¹⁶ that govern export controls, while the EU and its member states are, and should continue to be, a vital part of global efforts. Without neglecting the challenges of multilateral negotiations, which are often slower than the pace of developments in the economic and technology fields, action at the international level is more effective. Multiple parties jointly agree on policy objectives and on implementing common rules. From an economic perspective, this ensures a level playing field while, from a human security angle, concerted action is better warranted.

The 2016 proposal of the European Commission takes some encouraging steps towards increasing international cooperation in the area of export controls. This is already exemplified by the open-dialogue policy the EU pursues with core trading partners, such as the US, Japan and others, but also with China, which is not a party to most of the multilateral export control regimes.¹¹⁷ In the current context of fast technological progress and antagonistic approaches among trading partners, it is essential to maintain an honest and comprehensive dialogue that promotes multilateral over unilateral approaches.

It is also important to ensure a transparent and inclusive process both during the discussions to modernize the EU's export-control regulation as

116. The main four multilateral export-control regimes are: the Wassenaar Arrangement, the Australia Group, the Nuclear Suppliers Group and the Missile Technology Control Regime.

117. Of the four multilateral regimes mentioned above, China is a member of the Nuclear Supplier Group.

well as afterwards, once the updated rules enter into force. European companies have valuable experience and expertise that they can share with the European Commission and the member states' competent authorities. To this end, decision-makers should consider ways to engage with the private sector – and other stakeholders – on a more regular and comprehensive basis than the exceptional participation in the Dual-Use Coordination Group, as suggested in the 2016 proposal.

Technological Sanctions in the Space Domain

How Can the Europeans Find their Way Between the United States and China? The Case of the Communications Satellites

Jean-François Bureau

Professor Joseph Nye, who famously developed the notion of “soft power”, argues in his most recent book that, along with the “rise of Chinese power”, “the other great power shift is driven by technology” (...) which “has increased economic, political, and ecological interdependence and created more transnational linkages and issues that are often outside the control of governments, but affect the relations between them”.¹¹⁸

The space domain is a convincing illustration of this double shift, in terms of state power, with the increasing US/China rivalry and competition, and in terms of technological interdependences as space-based applications are ever more needed “in a world of growing complexity” where “the most connected states are the more powerful”.¹¹⁹

The early period of space competition between the US and the Soviet Union has often been described as a matter of prestige for each competitor. The Sputnik launch of October 1957 was a worldwide soft-power event for the Soviet Union, while the Apollo moon landing of 1969 was the US revenge. On 3 January 2019, the Chinese landing of its Chang-e 4 on the Van Karman crater on the far side of the Moon was also a big step forward, which confirmed, if needed, the substantial development of the Chinese knowledge and ability to deploy, control and make use of space technologies and assets.

¹¹⁸. J. S. Nye, *Do Morals Matter? Presidents and Foreign Policy from FDR to Trump*, Oxford, Oxford University Press, 2020, p. 196.

¹¹⁹. *Ibid.*, p. 210.

It is now more than twenty years since the United States identified China as *the* competitor it intends to control, while limiting the pace of its space activities and progress. This aim has materialized in US space export control rules, which – among others but no less than the others – have seriously affected the Europeans. At the same time, China took stock of that situation and developed an export-driven policy of space communications satellites which has helped it to reduce its technology gap in this domain.

With the emerging paradigm of global technological competition between Washington and Peking, where all the key players – government, private firms, universities, regulatory entities – are mobilized on the US side, the rules have changed, and the US has reformed its space technologies export policy, not to reduce the access barrier China is facing, but, on the contrary, to update it along with the new main developments in that field. This new game, with more assertive regulations and Chinese ambition that now covers every segment of the space programs, which are now a true segment of the connectivity competition, will challenge the Europeans even more. They will have to make hard decisions if they want to maintain a competitive position.

The technological containment of China and the EU/US relationship

Since the Report of the Select Committee on US National Security and Military/Commercial Concerns with the People's Republic of China, known as the Cox Report, was issued on 3 January 1999 by the House of Representatives, the space domain is very much under scrutiny by the US administration and legislators. From the start, the concerns about Chinese technological developments have been bipartisan. The US International Traffic in Arms Regulations (ITAR), enacted in 1976 to prevent the export of sensitive technologies to Warsaw Pact countries, has been substantially updated since 1999 to ban the transfer of sensitive space technologies to China. At that time, all of them (satellites, including components and software, launchers, etc.) were included in the United States Munitions List (USML), which is established and controlled by the Department of Defense.¹²⁰ Every communication satellite and launching service was subject to such ITAR regulations, and Western space manufacturers seeking to export to the US and other customers had to implement the ITAR rules. As a consequence, the Chinese market remained closed to the Western space industry. Some manufacturers, such as Thales Alenia Space, planned to

120. The other export-control regime is managed by the Department of Commerce, which is in charge of the Export Administration Regulations (EAR) and based on the Commerce Control List (CCL).

develop ITAR-free satellite platforms in order to extend their export portfolio to new customers, but faced difficulties in developing their products without any US component.

This technological containment of China has had several direct or indirect consequences.

For China

First of all, over the past twenty years, there has not been any significant export of Western space technology to China. It is difficult to assess whether this situation has incited the Chinese stealing and spying that has increased during this period, according to most Western analysis, but this side-effect cannot be excluded. At the same time, China's communications-satellite technology has not been able to develop in the way that the Western technology has. For example, China is expecting to achieve its first all-electric satellite in the next few years, while European and US manufacturers achieved this competence at least five years ago.

That gap in competence may have been another incitement to focus the research and development of telecommunications in the terrestrial segment, whereby government can more easily keep information flows under its control. Even broadcasting activities, which have been mostly driven by satellite technology all over the world, have not been a stimulus for China's communications-satellite industry, and the 2008 Olympic Games confirmed that the Chinese government can be reluctant to promote satellite connectivity. What is certain is that foreign satellite operators' access to the Chinese public will be closed as long as the Chinese supply by Chinese satellite operators is not yet ripe.

Even if US policy may have kept the technological development of the Chinese satcoms industry under control, it is clear that Chinese manufacturers have developed an export policy and strategy with substantial results. In the mid-2000s, the Chinese players started to export telecommunication satellites to developing countries with which they had close relations or looked for a deeper relationship, such as Nigeria, Laos, Bolivia, Pakistan, Venezuela and, more recently, Algeria. As China operated in other domains, it offered their partners to build the satellite and to launch it with Long March as well as a loan to pay for the package and even proposed content programs and training of the teams. This policy, despite initial success, has not proved enduring. In many cases, once launched, the satellite did not provide the expected services or was difficult for the teams to manage. It even happened that the terrestrial segment (teleport, gateways),

which is indispensable, was a missing link. As a consequence, some governments turned to Western actors for a follow-up.

The lessons of these deficiencies have obviously been learned, and China has reconsidered its cooperative approach, especially in the context of the Belt and Road Initiative, in which telecommunications and connectivity are supposed to be a key segment. In addition to the political benefit it can expect from such projects, Peking is eager to partner with European operators to develop projects that could fit the needs of some important developing countries, such as Indonesia and even Argentina.

For Europe

Facing the ITAR regulations, the Europeans did not deny the “Chinese risk” and tried to adjust their priorities.

As already mentioned, the ITAR-free approach did not produce much results in terms of technological autonomy. Even if some countries, like France, have monitored the areas and segments of products where autonomous procurement of components could be contemplated,¹²¹ this approach never became a true European policy despite some approaches developed in the framework of Horizon 2020¹²² by the European Commission. In fact, developing true European autonomy for all components needed to design a space system devoted to communications has not been listed as a key political objective.

Paradoxically, European adjustment to the US sanctions related to China in the space domain has led to an increased relationship between the European space communications operators and their US partners and providers. In this peculiar segment of the space business (but the first one in terms of value,¹²³ a situation which will last), it is important to consider that three of the four worldwide satellite operators are based in Europe: SES, born from a decision of the Luxembourg authorities to play a key role in the space domain; Eutelsat, the satellite operator acting under the umbrella of the Eutelsat intergovernmental organization to which 49 European

121. In France ST Microelectronics is a significant player in the chipset industry.

122. Horizon 2020 was the R&D program that the European Commission developed during the previous Multiyear Financial Framework (MFF) covering 2014–2020. Of a €79bn budget, €57.7bn was allocated among 31,256 specific contracts (data updated 6 April 2020).

123. The recent *Bryce Space and Technology Report*, issued in June 2020, states that the services provided by the satellite operators amounted to \$123bn in 2019 (among which TV amounted to \$92bn, telecommunications and internet to \$22.5bn). In comparison, the value of the satellites manufactured in 2019 was \$12.5bn, the launchings to \$4.9bn, and the ground equipment related to the space segment to \$130.3bn. In a nutshell, the breakdown of the commercial space domain (the value of which was \$271bn in 2019) is: 48% for the ground equipment, 45% for the services provided by the operators, 5% for the satellite manufacturing, and 2% for the satellite launching segment.

countries belong, and incorporated in Paris; Inmarsat, acting under the umbrella of the International Mobile Satellite Organization (IMSO), and based in London. And Intelsat¹²⁴ is legally based in Luxembourg.

As the Eurospace study¹²⁵ has demonstrated, during the last ten years (2009–2018):

- 95% of satellites exports have been communications satellites.
- The value and number of satellite exports has increased by comparison with the previous decade: €27bn in 2009–2018 compared to €16bn in 1998–2008.
- The United States is the leading exporter of communications satellites worldwide (57% of the total); EU ranks second (36% of the total).
- After a trade balance in satellite exports between the US and Europe was roughly achieved in 1998–2008 (US exports to EU, \$2.4bn; EU exports to US, \$2.27bn), the next decade saw a dramatic EU deficit: between 2009 and 2018, US exports to the EU totaled \$5.92bn versus \$3.83bn in EU exports to the US.

Of course, the \$2.09bn EU deficit with regard to the US cannot be strictly related to the US sanctions policy related to China. In fact, this situation must also be related to the fact that the US policy has been attractive for European operators in regard to defense and security business opportunities. For some years now, in parallel with developing proprietary satellite fleets (like WGS), the Pentagon has developed a policy of commercial procurement services by which European satellite operators were able to provide services to US forces, especially where deployments of drones were significant. All European operators with worldwide satellite coverage have been included in this policy, which the US Space Force seems to plan to continue.

124. Intelsat is the US space operator acting under the umbrella of an intergovernmental organization (ITSO), based in Washington, to which 149 member states belong; as a private entity, Intelsat is incorporated in Luxembourg.

125. ASD Eurospace, *Facts and Figures: The European Space Industry in 2018*, June 2019, available at: <https://eurospace.org>.

In a nutshell, the recent past can be described as follows:

- The US sanctions policy related to China has focused on space for two decades now, and targeted the communications satellites included in the USML.
- China tried to ease the constraints by exporting its own technology, but had only limited success; there is still a gap between Western and Chinese technological advancement.
- The US has increased its satellite exports worldwide, and created a trade imbalance with the Europeans; at the same time, the Europeans have been attracted to provide commercial military services to the US.
- Even if the European manufacturers are second worldwide to the US, they must prepare for a situation where they are not only competing with the US but also facing a new drive by China, based on its telecommunications strengths.

This picture has, however, begun to be modified by a new space complex that the US is leading.

Relaxing the space sanctions but opening a new and wider sanctions front

At the beginning of the current decade, the US satellite manufacturers were concerned that the competitiveness of their European counterparts could limit their export opportunities. They put forward the argument that some companies planned to develop ITAR-free satellites. They played the “China card” and managed to get a relaxation of the ITAR rules, in 2014.

In April 2012, the Department of Defense and the Department of State issued the Report 1248, which states:

“These satellites and related items do not contain technologies unique to the United States (U.S.) military industrial base nor are they critical to national security. In particular, the Departments believe the following items are more appropriately designated as dual-use items on the Commerce Control List (CCL) and controlled under the Export Administration Regulations (EAR):

- Communications satellites (COMSATs) that do not contain classified components;

- Remote sensing satellites with performance parameters below certain thresholds;
- and Systems, subsystems, parts and components associated with these satellites and with performance parameters below thresholds specified for items remaining on the USML.”¹²⁶

This reform was welcomed by the US Satellite Industry Association (SIA), which recalled¹²⁷ that, after they had considered opening the way for exports of space systems to China, “Congress reversed that decision in the FY1999 defense authorization act (P.L. 105-261) after a special congressional committee determined that U.S. satellite manufacturers violated export control laws and assisted China in developing its missile technology by aiding in analysis of launch failures of Chinese rockets that were carrying U.S.-built satellites. No U.S.-built satellites or satellites containing U.S. components have been exported to China for launch since that time.”

The SIA added: “European companies began building satellites without U.S. components that are ‘ITAR-free’ — not subject to the U.S. ITAR rules — and selling them to customers who do not want to deal with the U.S. export control system. Today’s report states that the current U.S. export control regime places the U.S. industrial base at a distinct competitive disadvantage when bidding against companies from other advanced satellite-exporting countries that have less stringent export control policies and practices.”

The Law of May 13th 2014 reformed the USML list, and transferred the export rules of the communications satellites (sub items 500) and the related components (sub items 600) to the CCL, and subject to the EAR.

The new regulation defines three classes of products:

- military, relevant to the ITAR/USML rules;
- dual use, subject to the EAR ECCN regulation, and
- non-controlled, relevant to the EAR 99 regulation.

It is interesting to note that some weeks before the new legislation was issued, both Presidents Hollande of France and Obama of the US had to discuss the case of the Falcon Eye contract in which Airbus and TAS aimed to export Pléiades satellites (observation) to the United Arab Emirates, which the US administration had blocked for six months. At the end of their meeting on 13 February 2014, it was decided that the US would authorize the export.

126. Report to Congress. Section 1248 of the NDAA for FY 2010.

127. Press release of the Satellite Industry Association, April 18, 2012.

In this new framework, all ITAR-related products cannot be exported to China but some dual-use products can be, subject to the EAR ECCN license.

In its statement, the SIA said: “This report does not recommend changing how China is treated, however. (...) It prohibits launching U.S. satellites on Chinese rockets without a presidential waiver. Such waivers were granted in the first half of the 1990s, which allowed U.S.-built satellites to be launched by China and led to the problems addressed by the 1999 law. (...) If this report’s recommendations are followed and hundreds of thousands of items are transferred from the USML to the CCL, that restriction might no longer apply. However, the report calls for changes to the CCL, too. It recommends prohibiting items on the CCL from being transferred to any ‘embargoed country’, a category that includes China, Syria, North Korea and others.”

The Obama reform of the USML/ITAR rules confirms that, even if the ITAR-free concept has not been very successful, the mere idea was strong enough to drive significant changes in the US sanctions policy, and to show that China can easily be the “elephant in the room” of the US/EU relationship in that strategic field.

As the Trump administration has focused its sanctions related to China on the telecommunications industry, be it the devices and ground network manufacturers like Huawei and ZTE, or digital applications platforms like Tik Tok, it is important to assess the different scenarios for the near future, building on the assumption that space telecommunications will be widely included in an ecosystem that integrates all kinds of infrastructure – terrestrial, space, submarine cables and mobile – in order to serve everyone, everywhere at any time. In this new complex of players, GAFA (Google, Apple, Facebook and Amazon – and especially Google as a service provider using a huge amount of data provided by satellites and Amazon as a space investor (Blue Origin; Kuiper) – can contribute to reshaping the picture along with Elon Musk’s SpaceX and Starlink. In addition, it must be highlighted that the technological challenge China is posing to the US is widely recognized in the US Congress: the two sides of the US political spectrum share very close views about the risks China represents in terms of technology competition.

China as a confrontational challenger of US supremacy

Whatever about the US sanctions, China aims to reach the most advanced level of communications satellite performance in the next few years. There

is no reason to believe that it will not achieve that ambition, which could be furthered by the lead that the Chinese claim to have taken in the cryptology sphere, with quantum-based cryptology. Hence, China could use a convincing cyberdefense capability to promote its communications satellites.

To serve its ambition, China can develop linkages between its space development plans and its already advanced telecommunications and digital industry. Such a strategy would soon include services providers like Alibaba, the e-banking and digital payment system, and the retailers that could include a space component to benefit from the dimensions of the country. In addition, the large spectrum of artificial-intelligence and data-managed applications which Chinese players are developing could be embedded in and served by such a dense network of connectivity.

If China develops such a strategy, it will be able to compete with its US counterparts, extend its influence far beyond its borders, and be in a position to offer attractive deals to the Europeans; for example, between Chinese telecommunications operators and European satellite operators. Then, the Belt and Road digital strategy would combine space and ground telecommunications infrastructure to build a network of digital services and applications centered in China but in direct competition with the US ones. In addition, China would be able to leverage the output of its space-based navigation system, Beidou, which will become operational very shortly.¹²⁸

Because of the sanctions related to the Chinese telecommunications industry, which are now being implemented by some key countries in Europe like the United Kingdom, and to a lesser extent by Germany and France, this confrontational model cannot be excluded.

What can the Europeans look for?

In the absence of “European GAFAs”, the Europeans will have to balance their alliances with the US players on one side, which means they will more or less align with the US sanctions, and the Chinese opportunities, which will of course have their own price. Given the European situation, and taking account of the recent EU move towards a more cautious relationship with China, it is highly probable that Europe will prefer to continue the US-based alliance, which would guarantee US market access to European satellite operators. To be more precise, the room for common projects with China,

128. On June 23, 2020, China launched the last of 30 satellites, Beidou-3, which will enable the worldwide extension of the navigation service.

assuming that China will agree to them, will be determined by the freedom of maneuver that the US sanctions allow.

There may be another policy that would bypass the Chinese “elephant” and seek other partners that could be as significant in terms of development. In that case, India, with its 1.3 billion citizens, could be the alternative option. It seems that the UK is considering such an option, given the partnership agreed between OneWeb and Bharti, the most important telecommunications operator in India, which resulted from the Chapter 11 process related to OneWeb in July 2020. As is well known, the Indian domestic market is far from being wide open to non-Indian telecommunications and satellite operators. The fact that OneWeb and Bharti have established a strategic alliance could change the situation, and help the Indian authorities to consider the non-Indian actors with more interest. At the same time, there is no doubt that the US administration would also favor such schemes. They would not only add a new period of cooperation between India and Western players but also open up options to build an alternative to the Chinese pressure on most countries in the region. However, it would demand a degree of engagement that India has not yet really contemplated. The opportunity that India’s extensive IT industry might wish to grasp may change that situation.

The norms and standards challenge?

Whatever the web of alliances that will shape the future of the connectivity business worldwide, the competition on norms and standards will be key.¹²⁹ In that field, the Europeans, who have demonstrated their capability to shape the personal data regulations, could build a very influential position. The many fora where the technical discussions take place (ITU, ETSI, ISO...) are all of importance. However a more politically driven conversation seems to be needed. The importance the new European Commission is paying to the connectivity and technological challenges is a convincing signal of attention. Beyond the intention, it is of utmost importance to deliver regulatory concepts and proposals when Europe’s competitors (often leaders of key technologies) are more united in their views, and build on a vibrant ecosystem to design innovations. In that field, Europe, Japan and Korea may have to develop common views that they could share with the US and India.

In conclusion, there is no doubt that technology diplomacy is becoming a major part of geopolitical relations between Europe, the US and China, not only in the space domain but, more broadly, in the wide domain of

129. See J. Seaman, “China and the New Geopolitics of Technical Standardization”, *Notes de l’Ifri*, Ifri, January 2020, available at: www.ifri.org.

connectivity. Sanctions will still influence options, opportunities and alliances. However, innovation could be the true differentiator among the players. In the 21st century, geopolitics and geoeconomics will have to be managed together, and more consideration be given to the universal changes that digital technology will lead to.

Conclusion

Which Technological Priorities for Europe's Strategic Autonomy?

André Loeseckrug-Pietri

New technologies are steadily changing the way we work, travel, communicate and relate to each other. They also exert a major influence on the strategic autonomy of state actors – that is, the ability to freely take decisions and actions in an interdependent world without being subject to foreign interference.¹³⁰

In a world characterized by a high level of global economic interdependence and by the importance of scale, this can only be achieved at the European level for the countries of the old continent. European strategic autonomy in critical technologies refers to the ability of European actors to own a degree of control over strategic technologies, i.e. technologies playing – or about to play – a critical role in the functioning and resilience of our economies and societies. This also includes technologies that may have a significant impact on our political models, institutions and values. “Owning a degree of control” does not automatically imply that Europe should replicate and develop a whole industry for each of these technologies. Nor should strategic autonomy in critical technologies be understood in absolute terms. It should rather be understood as a flexible concept, as a capability that actors can and must extend as far as they can to increase their freedom of decision and action.

European strategic autonomy in critical technologies starts with identifying them in the first place. The following selection of three technological categories on which Europe should focus its efforts is proposed: critical infrastructures, strategic technological sectors, and lastly selected key technological bricks (“pillars”), without which a sufficient level of control over infrastructures and technological sectors could not be achieved.

¹³⁰. L. Poirier, *Essais sur la stratégie théorique*, Paris, Fondation pour les études de défense nationale, 1982.

Critical infrastructures

The first fundamental pillar for strategic autonomy is the control, protection and strengthening of our critical technological infrastructures.

▀ Submarine cables

Submarine cables use fiber-optic technology, whereby information is encoded in waves of light transmitted by lasers across thin glass.

Carrying more than 90% of international communications traffic and, as of 2017, transporting \$10trn of financial transfers every day,¹³¹ submarine cables represent a critical information and communication infrastructure. Any damage to these cables has major consequences for telecommunications and therefore for the economy of countries affected by a breakdown. Non-state actors control over those cables is growing strongly (Google, Facebook).

▀ 5G & 6G networks

The shift of cellular communication networks from the 4th to the 5th and then 6th generation (5G and 6G) of cellular network standards will have a major impact on our societies. For 5G alone, it is estimated that it will contribute to roughly 5.3% of gross world product growth over the next 15 years¹³² and reduce energy consumption across industrial sectors by 15%.¹³³

The 5G and 6G networks will be a game changer for the competitiveness of European industries, but will also play a critical role in healthcare, energy management and the military. Their disruptive character makes them a strategic asset that Europe cannot afford to not control.

▀ Satellites

The multiplication of devices using satellite positioning systems such as GPS or Galileo, the development of space imagery services for defense and industry, and the vital role of telecommunications are increasing our dependence on satellites.

Their protection is thus of strategic importance. Europe is facing two main security challenges related to satellites. The first relates to protecting them from the growing risks of collision with space debris. The second relates to potential crisis situations in space. By successfully conducting an

131. W. Nielsen *et al.*, "Submarine Telecoms Industry Report, 7th Edition", Submarine Telecoms Forum, 2019, available at: <https://subtelforum.com>.

132. "Mobile Industry Generates \$565 Billion in Additional Global GDP by Unlocking the Right 5G Spectrum: GSMA Study", GSMA, released on December 12, 2018, consulted on September 9, 2020, available at: www.gsma.com.

133. B. Ekholm, "3 Ways to Boost Innovation in the 5G Digital Economy", World Economic Forum, released on January 15, 2020, consulted on September 9, 2020, available at: www.weforum.org.

anti-satellite missile test on 27 March 2019, India became the fourth country capable of destroying an enemy satellite, after the US, Russia and China.¹³⁴ Other coercive actions that could be conducted in space include blinding or obscuring the sensors of an observation satellite, jamming or intercepting a communication satellite, using a space maintenance device maneuvering to damage equipment, or blinding it from the ground with a laser.

▀ Data centers & cloud computing

The amount of data generated by human activity grows at an ever-increasing rate. The International Data Corporation (IDC) estimates that the global volume of data, generated by both individuals and companies, will grow from 59 zettabytes (ZB, equivalent to 10^{21} bytes) in 2020 to 175 ZB by 2025.¹³⁵

For now, 90% of the data generated globally is stored and managed in data centers, with the remaining 10% stored in objects such as smartphones and personal computers. While the growth of the Internet of Things and of edge computing will decrease the importance of centralized data centers.¹³⁶ One issue of particular importance for European strategic autonomy is their location, which determines the legal regime that applies to these data – and thus our degree of control over them.

▀ High performance computing

Increasingly needed to harness big data and facilitate scientific discoveries that need large computational efforts, such as cryptography, materials science, artificial intelligence technologies and climate modelling, supercomputers can be considered as a strategic resource for research performances and competitiveness.

▀ Critical energy grids

Energy grids are critical for the daily functioning and resilience of our societies. As the 2015 hacking of the Ukrainian power distribution grid highlighted, a main concern about this type of infrastructure has been the cybersecurity threats attached to the increasing digitalization of European energy systems.

134. A. J. Tellis, “India’s ASAT Test: An Incomplete Success”, Carnegie Endowment for International Peace, April 15, 2019, consulted on September 11, 2019, available at: <https://carnegieendowment.org>.

135. D. Reinsel, J. Gantz and J. Rydning, “Worldwide Global DataSphere Forecast, 2020–2024: The COVID-19 Data Bump and the Future of Data Growth”, *The International Data Corporation*, April 2020.

136. IRDS, “International Roadmap for Devices and Systems – Systems and Architecture”, 2020 Edition, p. 3-4, available at: <https://irds.ieee.org/editions/2020>.

Strategic technological sectors

Technologies are evolving at an ever-faster pace. Identifying the main sectors where disruption and technological acceleration are most likely to occur, and that have major societal, economic and strategic impact, is critical.

■ Artificial intelligence (AI) systems

AI systems,¹³⁷ especially deep learning, are undoubtedly the technological repertoire that has recorded the most substantial advances in recent years, mainly thanks to the increase in data and computing capacities, and the improvement of algorithmic and learning techniques.

Due to their consequences and pervasiveness, AI systems and their related technologies are critical for the strategic autonomy of Europe. They have met the conditions for a qualitative leap in many areas of human activity: by 2030, AI-powered technologies could, for instance, increase labor productivity by an average of 30% compared with 2015¹³⁸ and contribute \$15.700trn to the global economy.¹³⁹

■ Information and communication platforms

Information and communication platforms, and more specifically social networks, have fundamentally transformed our ways of interacting with others and of informing ourselves, as well as our consumer behavior. A 2019 survey conducted by Eurobarometer in 34 countries – including the 28 EU member states – indicated that 64% of Europeans were using social networks once a week, and 48% using them every day or almost every day.

137. Artificial intelligence systems are defined by the EU panel of experts on AI as “software – and possibly also hardware systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions”. Using the classification of Goodfellow *et al.*, there are four main types of AI systems: Rule-based systems, Machine Learning systems, Representation learning systems and Deep learning systems.

For more information see: EU Commission’s High-Level Expert Group on Artificial Intelligence, “A definition of AI: Main Capabilities and Scientific Disciplines”, made public on April 8, 2019, consulted on July 7, 2020, p. 6, available at: <https://ec.europa.eu> and I. Goodfellow, Y. Bengio and A. Courville, *Deep Learning*, The MIT Press, 2016, p. 2-5.

138. J. Manyika *et al.*, “Jobs Lost, Jobs Gained: What the Future of Work Will Mean for Jobs, Skills, and Wages”, *McKinsey Global Institute Report*, November 2017, available at: www.mckinsey.com.

139. “The Mobile Economy 2019”, *GSMA Intelligence Report*, 2019, p. 43, available at: www.gsmaintelligence.com.

This number rose to 87% for the 15–24 age group, suggesting that the importance of these communication platforms will rise in the near future.¹⁴⁰

As highlighted by the Cambridge Analytica affair, the impact of these platforms on citizens' perceptions, formation of public opinion and on our democratic life should not be underestimated.

▀ **Face recognition and contact-tracing systems**

While they inspire with good reasons anxiety among European populations, surveillance technologies may also be beneficial in our societies. These benefits will not be restricted to law enforcement but also spread to other sectors, such as healthcare. Contact-tracing applications are considered as having played an important role in limiting the Covid-19 epidemic in South Korea.¹⁴¹ Face recognition can be used to track a patient's use of medication, support pain management procedures, detect genetic diseases and support impaired individuals.

State actors have expressed growing interest in these technologies. The AI Surveillance Index developed by the Carnegie Endowment for International Peace identifies at least sixty-four countries that are incorporating facial-recognition systems in their AI surveillance programs, the majority of them being advanced democracies, including seven European member states.¹⁴²

▀ **Quantum technologies**

Quantum technologies will revolutionize our way of performing information computing activities, currently based on the binary logic of Boolean algebra. The quantic paradigm is expected to carry out, on an exponential basis, much more efficient algorithms for solving important problem classes,¹⁴³ to enable the development of very accurate sensors, and, with quantum cryptography, to improve the security of our communications.¹⁴⁴

140 . "Media Use in the European Union", Standard Eurobarometer 92, survey requested and coordinated by the European Commission's Directorate-General for Communications, Autumn 2019, p. 6 and 21, available at: <https://op.europa.eu>.

141. H. Lee, "These Elite Contact Tracers Show the World How to Beat Covid-19", *Bloomberg*, last updated on July 27, 2020, consulted on September 7, 2020, available at: www.bloomberg.com.

142. "AI Global Surveillance Technology", Carnegie Endowment for International Peace, consulted on September 7, 2020, available at: <https://carnegieendowment.org>, and S. Feldstein, "The Global Expansion of AI Surveillance", Carnegie Endowment for International Peace, September 2019, available at: <https://carnegieendowment.org>.

143. IRDS, "International Roadmap for Devices and Systems – Executive Summary", 2018 Edition, p. 16. <https://irds.ieee.org/editions/2018>.

144. "Science & Technology Trends 2020-2040 – Exploring the S&T Edge", *NATO Science & Technology Organization Report*, 2020, p. 19.

■ Genomics technologies

“Living technologies” may have the greatest impact on our century. Gene-editing technologies such as CRISPR/Cas9 – recently celebrated by the Nobel Prize – and gene drives are particularly powerful. These tools, separately, can dramatically modify a gene pool, including genes responsible for malformations and serious diseases.¹⁴⁵ RNA messengers have been massively highlighted by the Covid-19 pandemic and may disrupt the way and speed with which we develop new vaccines.¹⁴⁶

Genomics technologies will significantly change our health-management disease diagnosis and treatment. Their high disruptive potential and the bioethical questions arising from their use makes them of strategic interest for Europe and its populations.

■ Clean energy

One of the most pressing challenges faced by our societies today is to limit global warming. To achieve this goal, the production, transportation, distribution and use of clean energies – that is, energies that do not emit any greenhouse gas (GHG) when in use and that were produced through non-polluting methods – will be absolutely critical. Beyond their immediate interest for decarbonization, clean energies can also be a strategic asset, an opportunity to increase European energy autonomy.

Technological pillars

Not all technologies have the same importance. In order to remain technologically sovereign, it will need to master the most critical ones, those which are at the core of several sectors and with the biggest strategic and economic impact. Focus and significant investments will be required.

■ <10 nm semiconductors

Semiconductor-based devices are *the* building components of our information-processing systems. They are used everywhere, from high-performance computing systems, connected devices, cars, smartphones, to the infrastructure of our communication systems.

■ AI accelerators

One of the essential technological pillars fueling AI development is AI specific computing hardware (called AI accelerators). The last decade has

145. X. Xun, “We Are Witnessing a Revolution in Genomics – and It’s Only Just Begun”, World Economic Forum, released on June 24, 2019, consulted on September 7, 2020, available at: www.weforum.org.

146. See for example W. Shih, “Could COVID-19 Spur a Revolution in Vaccine Development?”, *Forbes*, released on February 16, 2020, consulted on September 11, 2020, available at: www.forbes.com.

seen the rise of these devices, especially Graphics Processing Units (GPUs) and Application Specific Integrated Circuits (ASICs) such as Google's Tensor Processing Unit (TPUs).¹⁴⁷

▀ **5G antennas**

5G small cells are critical for the effective deployment of the 5G network, constituting the low-powered access point connecting mobile devices to the broader cellular networks. One of the advantages of these small antennas in comparison to 4G macro-cells is that they enable the densification of the radio access network. This leads to increased performance in terms of coverage, capacity and quality of service, especially in dense urban areas.¹⁴⁸

▀ **Natural-language processing**

Natural language processing (NLP) based on AI refers to the set of tools enabling information-processing systems such as computers to automatically recognize, understand, interpret and alter human language. This has enormous implications in terms of development of autonomous systems and decision-making, be it in healthcare, in industry, in energy or in the defense sector. Through its ability to automatically extract information or to recognize what is expressed in a comment or sentence, NLP will constitute a strategic shift in the ability of actors to take informed, real-time decisions and understand situations.¹⁴⁹

▀ **AI-powered cybersecurity protocols**

AI algorithms can greatly benefit the cybersecurity of information and communication networks at four levels: the use of biometric log-ins instead of passwords; earlier and faster detection of cyberthreats and malicious activities; continuous updates on the evolution of threats through monitoring and analyzing cyberspace; strengthening cybersecurity capabilities by adapting the authentication framework and blocking access to a user behaving suspiciously.¹⁵⁰

147. IRDS, "International Roadmap for Devices and Systems – Application Benchmarking", 2020 Edition, p. 10, and L. Du and Y. Du, "Hardware Accelerator Design for Machine Learning", in H. Fahradi (ed.), *Machine Learning – Advanced Techniques and Emerging Application*, Londres, IntechOpen, 2018, available at: www.intechopen.com.

148. "Setting the Scene for 5G: Opportunities and Challenges", *International Telecommunications Union Report*, 2018, p. 10, available at: www.itu.int.

149. W. D. Eggers, N. Malik and M. Gracie, "Using AI to Unleash the Power of Unstructured Government Data", *Deloitte Insights*, released on January 16, 2019, consulted on September 10, 2020, available at: www2.deloitte.com.

150. N. Joshi, "Can AI Become Our New Cybersecurity Sheriff?", *Forbes*, released on February 4, 2019, consulted on September 10, 2020.

■ Next-generation batteries and green hydrogen-related technologies

Among clean energy options, electricity and hydrogen produced by renewable sources of energy are considered by many observers as among the best solutions to decarbonize our societies.

In terms of storage, both batteries and hydrogen offer solutions to store, transport and even use the energy produced by renewable sources. Indeed, one of the shortcomings of wind and solar energy is that they are intermittent, making energy storage solutions – and, thus, hydrogen and batteries – necessary for their adoption. In terms of transport and end-uses, both electric batteries and green hydrogen – that is, hydrogen produced by electrolysis powered by renewables – are considered as important and complementary solutions to decarbonize hard-to-abate sectors. With regard to green hydrogen and its derivatives (ammoniac or synthetic fuels), they are in addition considered as a powerful alternative to fossil fuels in several industries, as well as in the heavy aerial, maritime and terrestrial transportation sectors.¹⁵¹

Conclusion

The concept of what is a “critical technology” is pervasive, covering technologies used in sectors ranging from healthcare through industry to the decarbonization of our societies. It is also a concept in constant evolution; the technological sector is evolving at an ever-faster pace, generating new ideas and paradigms that we could not have imagined.

Europe has a great number of assets and a true potential in several strategic technologies discussed above: it has a very strong research and development activity in the quantum and green energy technological sectors, it is the home of 5G world industry leaders, and the continent that is the most advanced in the realm of robotics and is a space world power. But despite these advantages, it remains significantly dependent from the United States and increasingly from China for most of its critical digital infrastructures, be it data centres, cloud computing, information and communication platforms, but also for supercomputers, AI and autonomous systems, synthetic biology or submarine cables.

151. See for instance International Energy Agency, “The Future of Hydrogen – Seizing Today’s Opportunities”, report prepared for the G20, Japan (June 2019), available at: www.iea.org, and C. Philibert, “Perspectives on a Hydrogen Strategy for the European Union”, *Études de l’Ifri*, Ifri, April 2020, available at: www.ifri.org.

To tap into its potential, protect its assets, and gain a true geopolitical influence, Europe needs a significant political push - and a revolution in mindset. Progress cannot be achieved without the adoption of a strategic perspective on the technological sector. Acknowledging the urgency of the situation, the new Commission made several steps in this direction. Despite these first good efforts, it remains too little and too slow. The true challenge remains the need to achieve significant progress to reach scale (through the completion of single digital markets in the technology and digital space), inefficient funding mechanisms that rely sometimes more on “spray and pray” than on focused and result-driven approaches, coupled with an overall absence of independent impact assessments of policies, preventing agility and improvements. Lack of cohesion and cooperation among Member States (as recently highlighted in the AI or hydrogen space where most member states have their own strategy), hinders the capacity to anticipate while there is an absolute imperative to focus on the *next big things*, on the strategic issues of the near and medium term future rather than on the battles of the past. European-based leading-edge technologies cannot be developed without the scale of the Single Market. And a European strategic autonomy cannot be achieved without strong capabilities in leading-edge technologies that will shape the future.

Innovation is moving fast, with the key success factors being foresight, agility and speed. So must be the EU if it wants to keep up in the technological race of the 21st century.

Glossary

3GPP	3 rd Generation Partnership Project
AI	Artificial Intelligence
AMD	Advanced Micro Devices
ASB	Alcatel Shanghai Bell
ASICs	Application Specific Integrated Circuits
AVIC	Aviation Industry Corporation of China
BATX	Baidu, Huawei, Alibaba, Tencent et Xiaomi
BIS	Bureau of Industry and Security
BRI	Belt and Road Initiative
CCL	Commerce Control List
CCP	Chinese Communist Party
CEO	Chief Executive Officer
CFIUS	Committee on Foreign Direct Investment in the United States
CNC	Computer Numerical Control
CoCom	Coordinating Committee for Multilateral Export Controls
COMAC	Commercial Aircraft Corporation of China
COMSAT	Communication Satellite
CPC	Communist Party of China
CRISPR	Clustered Regularly Interspaced Short Palindromic Repeats
DARPA	Defense Advanced Research Projects Agency
DDTC	Directorate of Defense Trade Controls
DPRK	Democratic People's Republic of Korea
EAR	Export Administration Regulations
EC	European Commission
ECCN	Export Control Classification Number
ECRA	Export Control Reform Act
EFTs	Emerging and Foundational technologies
ETSI	European Telecommunications Standards Institute
EU	European Union
EU	European Union
EV	Electric Vehicle
FAW	First Automobile Works

FDI	Foreign Direct Investment
FIRRMA	Foreign Investment Risk Review Modernization Act
FTZ	Free-Trade Zone
GAFA	Google, Apple, Facebook, Amazon
GDPR	General Data Protection Regulation
GHG	Greenhouse Gas
GII	Global Innovation Index
GPS	Global Positioning System
GPU	Graphics processing unit
HSBC	Hong Kong & Shanghai Banking Corporation
IBM	International Business Machines Corporation
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and communication technology
IDC	International Data Corporation
IEA	International Energy Association
INSEAD	Institut Européen d'Administration des Affaires
IoT	Internet of Things
IP	Intellectual Property
IPR	Intellectual Property Rights
ISO	International Organization for Standardization
IT	Information Technology
ITAR	International Traffic in Arms Regulations
ITIF	Information Technology and Innovation Foundation
ITU	International Telecommunication Union
JV	Joint Venture
MFF	Multiyear Financial Framework
MNC	Multinational Corporation
NLP	Natural language processing
NSA	National Security Agency
OECD	Organisation for Economic Cooperation and Development
PLA	People's Liberation Army
PNT	Position, Navigation and Timing
PRC	People's Republic of China
R&D	Research and Development
R&I	Research and Innovation
RNA	Ribonucleic acid
SAIC	State Administration for Industry and Commerce

SEP	Standard Essential Patents
SES	Société Européenne des Satellites
SIA	Satellite Industry Association
SME	Small and medium-sized enterprises
SMIC	Semiconductor Manufacturing International Corporation
SOE	State-owned enterprises
STEM	Science, Technology, Engineering, and Mathematics
TPU	Tensor processing unit
TSMC	Taiwan Semiconductor Manufacturing Company
UCB	Union Chimique Belge
UN	United Nations
UNSC	United Nations Security Council
US	United States
USML	United States Munitions List
VC	Venture Capital
WEF	World Economic Forum
WGS	Wideband Global SATCOM
WIPO	World Intellectual Property Organization
WMD	Weapons of Mass Destruction
WTO	World Trade Organization
ZB	Zettabytes
ZTE	Zhongxing Telecommunication Equipment Company Limited



French Institute
of International
Relations