



Digital Power China

A European research consortium

EUROPE'S STRATEGIC TECHNOLOGY AUTONOMY FROM CHINA

ASSESSING FOUNDATIONAL
AND EMERGING TECHNOLOGIES

JANUARY 2023 | EDITOR: TIM RÜHLIG





About the Digital Power China research consortium

The Digital Power China (DPC) research consortium is a gathering of China experts and engineers based in eight European research institutions, universities, think tanks and consultancies. Not all DPC researchers contribute to every report. For this report, DPC has been joined by invited guest researchers.

The group is devoted to tracking and analysing China's growing footprint in digital technologies, and the implications for the European Union. DPC offers the EU concrete policy advice based on interdisciplinary research. Tim Rühlig, Senior Research Fellow at the German Council on Foreign Relations (DGAP), is the convenor of DPC and co-chairs the initiative with

Carlo Fischione, a Professor at the Royal Institute of Technology in Stockholm.

DPC systematically pairs technological and country expertise, which is based on rigorous academic research combined with experience of the provision of policy advice. The informal group brings together a variety of European researchers in order to combine diverging perspectives from across the continent. Responsibility for the accuracy of the views expressed remains solely with the indicated authors. This report has been generously supported by the German Foreign Office. The report does not reflect the position of Germany's Federal Foreign Office.¹

¹ The production of this report was supported by COST Action CA18215: the China in Europe Research Network (CHERN, www.china-in-europe.net), and by

the European Cooperation in Science and Technology (COST, www.cost.eu).



DPC institutions

PARTICIPANTS IN THIS STUDY
SHOWN IN **BOLD**

GUEST PARTICIPANTS
IN THIS STUDY

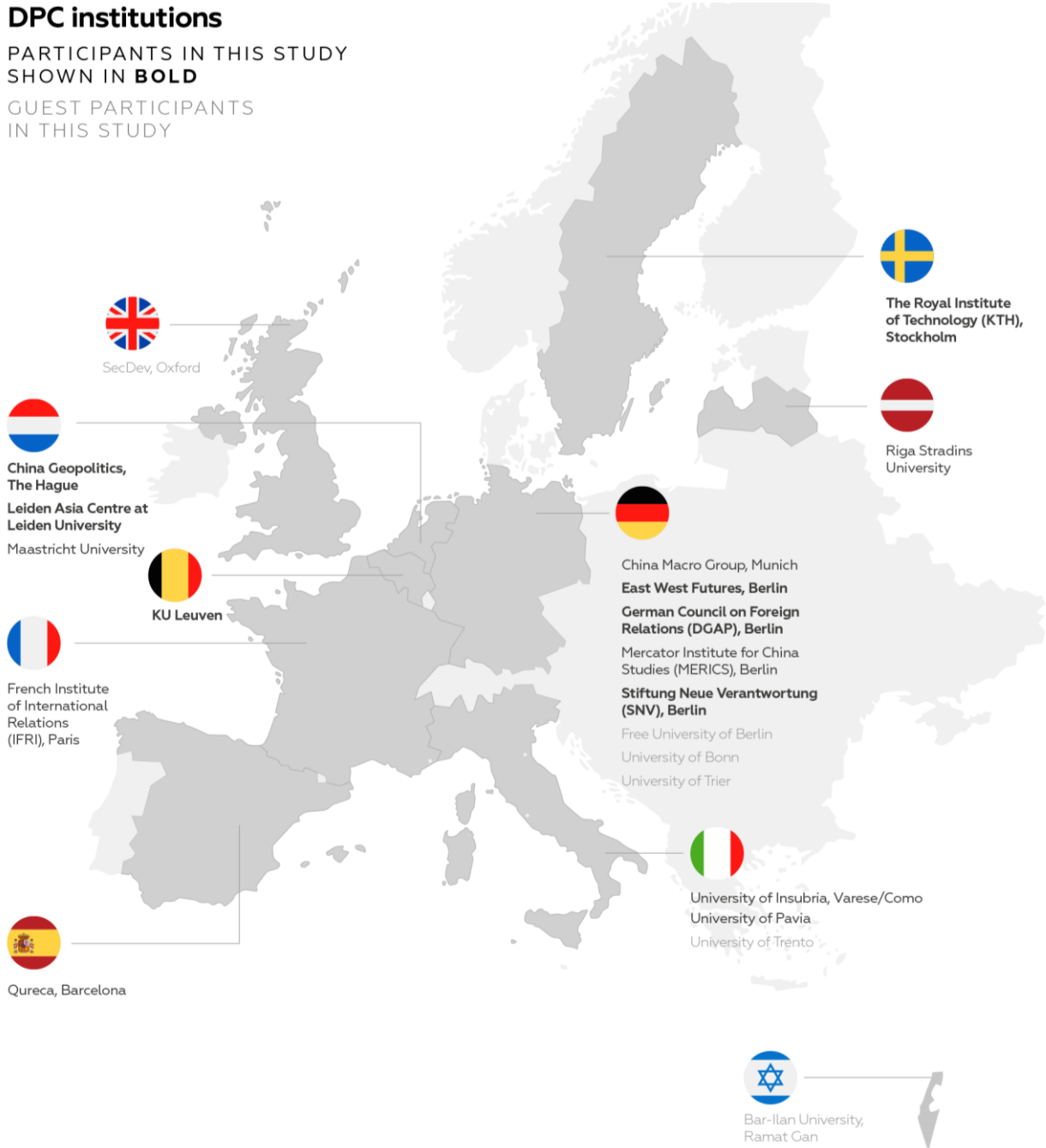






Table of content

About the Digital Power China research consortium	2
Executive Summary: Getting China’s digital technology policy right: implications for the EU	7
Introduction: European Open Strategic Autonomy in the light of China’s digital tech power.....	12
Challenges of a rising Chinese chip design ecosystem	27
In political and technological harmony or disharmony? How Europe and China advance towards 6G	41
Crypto Without the Currency: China’s Blockchain Strategy.....	59
Assessing the Financial and Geoeconomic Implications of China’s Digital Currency.....	74
Chinese Vehicle-to-Everything (V2X) Technology and the European Car Industry.....	91
AI for Urban Public Security: Threats to European Security and Values	105
The ethics of Artificial Intelligence in the European Union and China	119





Executive Summary: Getting China's digital technology policy right: implications for the EU

For decades, Europeans have considered the People's Republic of China (PRC) incapable of ground-breaking innovation. Only recently, in the middle of the digital transformation, have we found that dependence on China is not limited to critical raw materials, and that the Chinese contribution to supply chains is not limited to cheap labour. China is striving for technological leadership in a broad range of emerging and foundational technologies.

Growing geopolitical tensions have heightened the awareness that critical dependencies can be weaponized for political purposes. Russia is leveraging European dependency on fossil fuels in its war against Ukraine. The PRC's economic coercion against Lithuania leaves little doubt that China stands ready to blackmail Europe when it considers that its core interests are at stake. US willingness to act unilaterally regarding China and to exert pressure on the EU and its member states to cooperate is also now a pressing issue for policymakers.

In the light of such deep dependencies and their weaponization, the European Union (EU) is attempting to manage its capacities and its dependencies on China. It defines this as Open Strategic Autonomy, where the goal is to uphold the EU's capability to act internationally without

being constrained by technological dependencies.

The EU has started to identify critical dependencies but what reads well in the abstract is difficult to operationalize. Despite the European Commission's lead, EU actors are still trying to address divergent challenges, and therefore advocating divergent sets of tools, to achieve Open Strategic Autonomy. For example, the extent to which the EU should strive to "re-shore" the production of emerging and foundational technologies or instead aim to diversify its supply chains is a matter of controversy.

This report operationalizes Open Strategic Autonomy by identifying four dimensions:

- (a) *resilience of supply chains*, or the robustness of the supply of critical materials and primary products in case of major disruption ranging from natural disasters to a pandemic or war;
- (b) *criticality/national security*, or the security of IT, networks and cyberspace that are crucial not only for military defence, but also to the functioning of increasingly interconnected societies and economies;



- (c) *defence of values and sustainability*, or the protection of basic human rights in the digital age, primarily in Europe but also around the globe, as well as the prioritization of sustainability goals not least for the sake of combating climate change; and
- (d) *technological competitiveness*, or boosting Europe's own technological capabilities in terms of research, innovation and development, as well as advanced manufacturing.

All four dimensions of Open Strategic Autonomy are not necessarily of concern to the EU in every emerging and foundational technology. Even where they are, the severity and urgency of the challenges posed by China vary. Operationalization in four dimensions does not make Open Strategic Autonomy less complex, but it does help to identify weaknesses that the European Union should strive to address in its attempt to gain such autonomy in any given foundational or emerging technology.

In its analysis of several emerging and foundational technologies, this report assesses the degree to which the four dimensions of Europe's Open Strategic Autonomy are threatened by the PRC. Figure 0.1 illustrates that the challenges vary greatly across emerging and foundational technologies

and their applications. Several notifications in one box indicate divergent risks that require divergent assessment within one dimension.

While it is difficult to compare the degree of risk across several emerging and foundational technologies, ranking within a single technology is easier. Hence, the assessment across technologies summarized in Figure 0.1 needs to be taken with a pinch of salt, and the overview clearly demonstrates that there is no clearly defined ranking of concerns across technologies. For example, it is not the case that national security is the primary concern regardless of technology or that values-related issues are necessarily the least urgent to address. Instead, the priority of threats to Europe's Open Strategic Autonomy varies across the emerging and foundational technologies analysed in this study.

This risk assessment is based on rigorous research carried out by pairs of researchers that combine technical and China expertise as part of the Digital Power China (DPC) research consortium. Detailed discussion of the findings is available in this study alongside a separate chapter on the divergent approaches to Artificial Intelligence ethics in Europe and China.



DIMENSION OF OPEN STRATEGIC AUTONOMY

TECHNOLOGY	Resilience of supply chains	Criticality/ national security	Defence of universal values/ sustainability	Technological competitiveness
Chip design	●	●	●	●
6G development	●	●	●	●
Blockchain technology	●●	●●	●	●●
Introduction of central bank e-currency	●●	●●	●	●●●
Artificial Intelligence in automotive applications	●	●	●	●
Artificial intelligence in smart city applications	●	●	●	●
Artificial intelligence ethics	●	●	●	●

- very high degree of threat
- high degree of threat
- moderate degree of threat
- low degree of threat
- not applicable

Figure 0.1 – Degree of challenge to the four dimensions of European Open Strategic Autonomy presented by China in emerging and foundational technologies and their applications

For European policymaking, this means that one-size-fits-all solutions are doomed to fail. For example, a policy instrument that might be useful for increasing European technological competitiveness in a given emerging technology is of no use in protecting national security concerns in that or another emerging technology. In some cases, tensions exist between the different dimensions of Open Strategic Autonomy within the same foundational or emerging technology. For example, the mitigation of national security risks in 6G is all about the trustworthiness of Chinese technologies and vendors, and requires thinking about precautions. Given China’s technological advances, however, Europe

may not be able to maintain its technological competitiveness unless it continues to cooperate with the PRC. To strike a balance between competing policy goals is not impossible but requires a rigorous process. The introductory chapter of this study introduces a four-step process that helps to identify the challenges to the EU’s Open Strategic Autonomy across four dimensions and adequate policy tools.

Figure 0.2 summarizes how policymaking must start from an analysis of technological ecosystems to assess the degree of dependency and associated risks based on the criticality of the items under consideration, options for supply substitution and the extent to which

dependencies are mutual, which limits the options for the PRC to weaponize European dependencies. Such analyses of technological ecosystems should be followed by an assessment of the implications for the four dimensions of Europe’s Open Strategic Autonomy.

Since no two dependencies carry similar risks, a geopolitical contextualization that considers geopolitical factors, such as regime type and the existence or absence of security alliances, is essential. The severity of dependencies and likelihood of their weaponization by China against Europe is decisive in determining the level of risk. This analysis also includes an element of foresight since truly strategic policymaking should involve a certain degree of anticipation. Knowledge of the actors that

drive policy and technological development in the PRC is necessary but not sufficient for anticipating future developments in China. For this purpose, all the chapters in this study provide an overview of the most relevant actors in the PRC that European policymakers should be carefully monitoring. Each chapter provides a brief list of actors, an actor description, including of their role in the Chinese system, and a rough indication of their relevance to European foresight exercises in the respective case studies.

Finally, European policymakers should use different policy tools to achieve clearly defined goals based on political priorities and depending on which of the four dimensions of European Open Strategic Autonomy is affected.

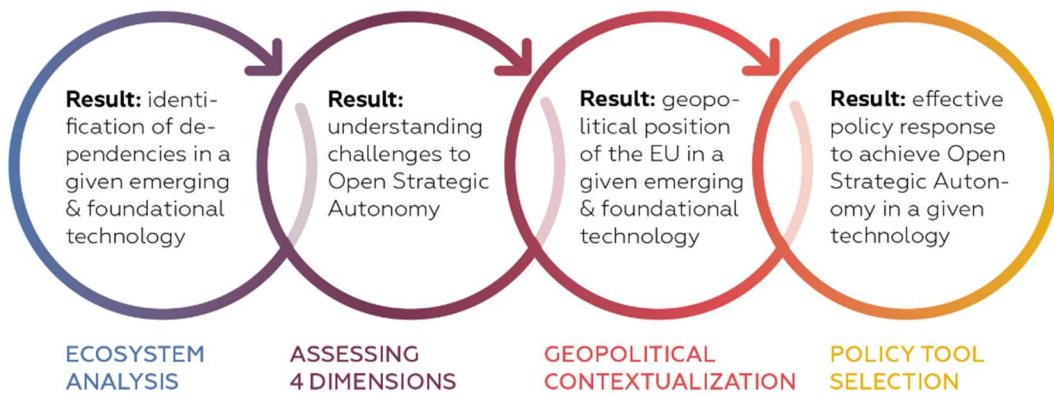


Figure 0.2. – The four-step process for identifying appropriate tools for addressing the challenges to Europe’s Open Strategic Autonomy



Appropriate policy tools differ not only depending on the four dimensions of Open Strategic Autonomy, but also across emerging and foundational technologies and their applications. However, based on the limited number of cases investigated in this study, we find that – by trend – certain types of policy tools seem to be

particularly suited to addressing one or other of the four dimensions of Open Strategic Autonomy. Figure 0.3 summarizes the predominant goals to be achieved in the four dimensions and the types of policy instruments that tend to be identified as most effective.





DIMENSION OF OPEN STRATEGIC AUTONOMY	PREDOMINANT POLICY GOAL	TYPE OF POLICY INSTRUMENTS THAT TEND TO BE MOST EFFECTIVE
 Resilience of supply chains	Diversification	<ul style="list-style-type: none"> • Transparency measures • Diversification incentives, e.g. procurement • Cooperation with third parties, e.g. Free Trade Agreements • Protection of indispensable actors
 Criticality/national security	Technical and vendor trustworthiness	<ul style="list-style-type: none"> • Regulation • Certification • Standardization • Like-minded sourcing
 Defence of values/sustainability	Like-minded coordination	<ul style="list-style-type: none"> • Regulation • Like-minded cooperation
 Technological competitiveness	Strengthening of innovation and industrial base	<ul style="list-style-type: none"> • Industrial policy • R&D investment • Protection of indispensable actors

Figure 0.3. – Policy goals and instruments of the four dimensions of Open Strategic Autonomy



Introduction: European Open Strategic Autonomy in the light of China's digital tech power

Jan-Peter Kleinhans, Tim Rühlig

Abstract

Open Strategic Autonomy in emerging and foundational technologies has rightly been identified as a crucial policy goal in order to preserve the European Union's capability to act. China is at the centre of this discussion, not least because of increasing geopolitical tensions and China's growing footprint in digital technologies. What sounds good in abstract terms, however, can be difficult to operationalize. We identify four dimensions of Open Strategic Autonomy: supply chain resilience, national security, values and sustainability, and technological competitiveness. All four dimensions are equally legitimate policy goals but require different policy tools that can at times be conflicting. We propose a four-step policy process that can help European policy-makers operationalize Open Strategic Autonomy in any given emerging or foundational technology, and identify the most appropriate tools to address existing shortcomings.

The challenge

For decades, Europeans considered the People's Republic of China (PRC) to be incapable of technological innovation. Authoritarianism and central planning appeared to prevent China from developing the necessary degree of creativity. As the workbench of the world, China has been accused of stealing intellectual property (IP), copying and mimicking

Western inventions. As recently as 2014, the *Harvard Business Review* published an article on "Why China Can't Innovate".²

Today, almost no one continues to hold to this illusion. Through partial protection of its markets for foundational and emerging technologies (semi-protected markets),³ learning from the West, targeted

² Regina M. Abrami, William C. Kirby and F. Warren McFarlan, "Why China can't innovate", *Harvard Business Review*, March 2014, <<https://hbr.org/2014/03/why-china-cant-innovate>>.

³ "Foundational" technologies have a higher degree of commercialization and can enable progress and applications in a variety of problem domains; examples

would be semiconductors or wireless communication. "Emerging" technologies may have a lesser degree of commercialization potential, such as quantum computing, biotechnology or AI. Even though the term "Emerging and Foundational Technologies" (EFTs) is heavily used by policymakers, there is no clear or exhaustive list of technologies at the time of



theft of knowhow, unleashing enormous investment and encouraging experimentation, the PRC has become an innovation powerhouse. As a result, China has a strong position in the supply chains of emerging and foundational technologies and in this, some argue, may have surpassed that of the West.⁴ Today, the European Union is highly dependent on Chinese technology and this dependency comes with economic, political, security and ideational costs.⁵

Economically, an uneven playing field favours Chinese tech firms that benefit from preferential treatment and lower data protection and environmental standards. This endangers the EU's digital industrial competitiveness. *Politically*, China is able to leverage political concessions from technologically (over-)dependent third countries, including EU member states. The PRC is also actively engaging with global cyber-governance in an effort to rewrite institutional processes and increase its power. In the *security field*, the inclusion of Chinese digital equipment can come with cyber-insecurities that enable espionage and sabotage by a state with which the EU has no security alliance. *Ideationally*, China's technological stronghold calls into question whether the governance principles

of the digital technologies that are increasingly penetrating entire societies reflect liberal and democratic values. Among the notable fields of divergent ideational conception between Europe and China are technical standards, data governance and effective protection of the environment.

This is not to argue that the EU should cut all ties with China. Nor is decoupling considered a feasible or desirable option. The ecosystems of emerging and foundational technologies are deeply transnational and countries are extremely interdependent. China is simultaneously a partner, competitor and systemic rival of the EU.⁶ While initially the EU was clear that China plays different roles depending on the policy field, more and more policymakers are acknowledging that the PRC has characteristics of all three roles in all policy fields. These multiple roles indicate that operationalizing Open Strategic Autonomy in emerging and foundational technologies vis-à-vis China will be highly complex.

Although Open Strategic Autonomy reads well in the abstract, it is difficult to operationalise in practice. At an abstract level, Open Strategic Autonomy is about enabling

writing. See e.g., *Torres Trade Law*, "BIS's new approach to Identifying 'emerging and foundational technologies'", 7 January 2022, <<https://www.torrestradelaw.com/posts/BIS%E2%80%99s-New-Approach-to-Identifying-%E2%80%9CEmerging-and-Foundational-Technologies%E2%80%9D/285>>.

⁴ Graham Allison et al., *The Great Tech Rivalry: China vs the US*, Cambridge, MA: Belfer Center for Science and International Relations, December 2021, <https://www.belfercenter.org/sites/default/files/GreatTechRivalry_ChinavsUS_211207.pdf>.

⁵ Rogier Creemers et al., "Getting China's digital technology policy right: Implications for the EU", in

Tim Rühlig (ed.), *China's Digital Power. Assessing the Implications for the EU*, Berlin, Digital Power China, January 2022, pp. 5–19, <https://timruhlig.eu/ctf/assets/x93kiko5rt7l/4uiZoNQtrkni5KfuNDRBbx/fd52e3320cfe21e6b304ad31d81279d8/DPC-full_report-FINAL.pdf>.

⁶ European Commission et al., "An open, sustainable and assertive trade policy: Open strategic autonomy", [n.d.], <https://trade.ec.europa.eu/doclib/docs/2021/february/tradoc_159434.pdf>, accessed 16 December 2022.



or preserving Europe's ability to act in its own best interests. To this end, the EU has begun to identify critical dependencies, which are summarized in Box 1.1. However, EU actors still aim to address divergent challenges when they speak of Open Strategic Autonomy, so different actors advocate divergent sets of tools for achieving such autonomy. For example, to what extent the EU should strive to re-shore the production of emerging and foundational technologies or instead aim to diversify its supply chains remains controversial.

This paper proposes operationalization of Open Strategic Autonomy in four dimensions: (a) resilience of supply chains; (b) criticality/national security; (c) values and sustainability; and (d) technological competitiveness. All four dimensions are not of equal concern to the EU in every emerging and foundational technology. In addition to the four dimensions, geopolitical contextualization is required to identify the extent to which and in what ways the EU's Open Strategic Autonomy is being challenged. These are not depen-

dencies as such, but a proper risk calculation that considers the criticality of the item under consideration, the degree of reliance on suppliers and whether options exist for substitution, as well as political factors such as security alliances and regime type. Severity of the challenges in the four dimensions and the likelihood that a given dependency might be weaponised are decisive.

Our operationalization does not make Open Strategic Autonomy any less complex. Instead, we introduce the four dimensions to help identify which weaknesses the European Union should strive to address in its attempt to gain Open Strategic Autonomy in any given foundational or emerging technology. In some cases, tensions exist between the different dimensions of Open Strategic Autonomy. We therefore propose a four-step process that can help to identify the challenges to the EU's Open Strategic Autonomy along the lines of the above four dimensions and suggests the right tools for addressing these challenges.



Box 1: Europe's technological dependencies on China: an initial estimate

The European Commission's Staff Working Document of 2021 identifies the 137 products most dependent on third country imports, of which 16 per cent are raw materials, 50 per cent are intermediate goods and about 27 per cent are final products.⁷ The PRC alone accounts for 52 per cent of the import value of these goods. Especially in the area of raw materials, the EU is highly dependent on China, which is the EU's primary supplier of, for example, Antimony, Bismuth, Magnesium and Tungsten, as well as light and heavy rare earth elements (LREs; HREs).⁸ These materials are used in many sectors, such as healthcare or chemical processing, and are crucial for emerging innovations and indispensable in the production of Li-ion cells, fuel cells, wind generator and solar panels, and thus for achieving the European twin transition.⁹ While the EU remains high performing in advanced manufacturing, advanced materials and mobility, it has gradually lost its capacity compared to China in key technologies such as Artificial Intelligence, Big Data, micro- and nanoelectronics and Robotics.¹⁰

The EU's approach to Open Strategic Autonomy

In May 2021, the European Commission made Open Strategic Autonomy the guiding concept and lens through which to assess and influence Europe's position in the world.¹¹ The Commission defines Open Strategic Autonomy as "the ability to shape the new system of global economic governance and develop mutually beneficial bilateral relations, while protecting the EU from unfair and abusive practices, including to diversify and solidify global supply chains to enhance resilience to future

crises".¹² One area of focus is Europe's position within global supply chains, which is assessed and defined in terms of *strategic capacities, dependencies* and *strategic dependencies*.

The European Commission recognizes that a dependency is not necessarily bad in and of itself, but that this depends on various factors, and that its Open Strategic Autonomy can be strengthened if a mutual dependency exists with a trusted international partner. The Commission also

⁷ European Commission, "Commission Staff Working Document: Strategic dependencies and capacities", SWD(2021) 352 final (2021), 5 May 2021, <https://ec.europa.eu/info/sites/default/files/swd-strategic-dependencies-capacities_en.pdf>.

⁸ Magnus Gislev, Milan Grohol et al., *Report on Critical Raw Materials and the Circular Economy*, European Commission Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, Brussels, 2018, <http://publications.europa.eu/resource/cellar/d1be1b43-e18f-11e8-b690-01aa75ed71a1.0001.01/DOC_1>.

⁹ European Commission, *Critical Raw Materials for Strategic Technologies and Sectors in the EU: A Foresight Study*, European Commission, Joint Research Centre, accessed 24 May 2022 at <https://rmis.jrc.ec.europa.eu/uploads/CRMs_for_Strategic_Technologies_and_Sectors_in_the_EU_2020.pdf>.

¹⁰ European Commission (note 9).

¹¹ See e.g. European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Updating the 2020 New Industrial Strategy: Building a stronger Single market for Europe's recovery". COM (2021) 350 final, 5 May 2021, <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021DC0350&from=EN>>; Cristiano Cagnin et al., *Shaping and Securing the EU's Open Strategic Autonomy by 2040 and Beyond*, European Commission, Joint Research Centre, 10 October 2022, <<https://data.europa.eu/doi/10.2760/877497>>.

¹² European Commission, "Commission presents an updated in-depth review of Europe's strategic dependencies", 23 February 2022, <<https://www.pubafairsbruxelles.eu/eu-institution-news/commission-presents-an-updated-in-depth-review-of-europes-strategic-dependencies/>>.



recognizes that such an approach fundamentally relies on intricate and continuous mapping of important technology ecosystems, as well as a case-by-case assessment of appropriate policy measures. Box 1 provides a brief overview of some of the dependencies identified by the European Commission.

What sounds nuanced and certainly well-intentioned on paper is extremely challenging to operationalize and put into practice at the policy level. Europe faces countless “make or buy” decisions. Although Brussels often says that the overarching goal is not autarky, in reality, especially with regard to digital technologies, Europe is highly dependent on foreign technology providers and must therefore decide whether to live with dependency or invest in its own capabilities.

With export restrictions and investment screening on the rise, another question for Europe is whether it can follow the US government’s lead in curbing the technological advancement of China in critical areas without completely halting trade and investments. Should it be open for business or protect the ecosystem? In many areas, it is unclear whether Europe would benefit from decoupling and being less dependent on Chinese industry. A form of control would be lost if China decoupled from certain technology ecosystems. This might amount to strengthening autonomy while maintaining (mutual) dependence. These are just a few examples of the challenges in operationalising Europe’s goal of Open Strategic Autonomy. Numerous actors within the EU use the terminology but do not agree on the related goals or the means of achieving it.

How can Open Strategic Autonomy be conceptualised and operationalised?

Fundamentally, four dimensions of European Open Strategic Autonomy can be identified in emerging and foundational technologies. Any operationalization of Open Strategic Autonomy should start with identification of the specific *strategic capacity* or *strategic dependency* that is of concern to the EU. The four dimensions will enable policymakers to identify or prioritize the specific concern in any given foundational and emerging technology and to identify trade-offs where they exist.

1. *Global supply chain resilience and second- and third-order effects*
The global value chains (GVC) of many, if not all, emerging and foundational technologies are characterised by a transnational division of labour. No region is in control of all the production steps and its supplier markets. Thus, to strengthen security of supply it might be in Europe’s best interests to strengthen the resilience of the GVC in order to reduce second- and third-order negative impacts on European industries in case of supply



disruptions. Strategies to strengthen resilience vary greatly between specific GVCs, such as semiconductors, batteries or quantum computing, depending on their individual characteristics.

2. *National security/criticality*

Not reducing *strategic dependency* or losing *strategic capacity* might have (in)direct negative impacts on European member states' national security. Of the four dimensions, assessing the potential impact on national security is the one with which policymakers are traditionally the most familiar. However, strategic dependencies in foundational technologies, such as semiconductors, or general-purpose technologies, such as AI, might have an indirect impact on national security. The national security risks that stem from dependence on Chinese mobile network equipment vendors are different from the national security risks to member states that rely heavily on drones, surveillance cameras or AI chips from Chinese vendors. Some of these risks can be mitigated at the technical level, while others come down to the trust-worthiness of the technology provider. One example is Europe's increasing dependence on Chinese back-end manufacturing (the last step of semiconductor

manufacturing), which could be utilized to compromise a chip or to implement hardware backdoors or kill switches.

3. *Values and sustainability*

Strategic dependency or technology cooperation can also conflict with European values. Like implementation of export restrictions to protect human rights, strategic dependence can also be scrutinized according to the human rights violations that such technology would enable. One example is the increased scrutiny of Hikvision surveillance cameras in Europe and the company's ban in the US due to its involvement in human rights violations against Uyghurs in the PRC.¹³ Thus, reducing dependency on Chinese surveillance cameras could be based on European values rather than solely national security concerns. Similarly, sustainability is of growing concern, and emerging and foundational technologies play an increasingly important role. While both Europe and China emphasise its importance, the priority attributed and approaches to sustainability vary, which has implications far beyond the EU for global goods such as combating climate change.

4. *Technological competitiveness*

Europe might invest in *strategic capacities* or try to reduce *strategic*

¹³ Joel Griffin, "Report: US may impose sanctions on Hikvision", Security Infowatch, 4 May 2022, <<https://www.securityinfowatch.com/video-surveillance/>

[article/21266640/report-us-may-impose-sanctions-on-hikvision](https://www.securityinfowatch.com/video-surveillance/article/21266640/report-us-may-impose-sanctions-on-hikvision)>.

dependencies to be able to compete internationally in the long term if a certain technology or market is deemed highly important in the future. Current examples include Europe’s investments in quantum computing and photonics. The Dutch government, for example, has invested heavily in the PhotonDelta consortium to strengthen the long-term competitiveness of its domestic photonics ecosystem.¹⁴ In the light of the intensifying US-China technological rivalry, government incentives to support the technological competitiveness of a specific domestic industry or technology provider can also be motivated by maintaining “strategic indis-

pensability”; that is, ensuring that a company continues to play an indispensable role within the GVC in the long term.¹⁵ Technological competitiveness therefore creates geopolitical leverage.

Finally, after assessing a *strategic capacity* or *strategic dependency* linked to these four dimensions, geopolitical contextualization is required. Being highly dependent on US technology providers or Japanese technology providers might come with a very different risk profile than being highly dependent on Chinese companies for the same technology – due to factors such as foreign relations, security alliances, political economy and market access. Figure 1.1 summarizes the four dimensions of *Open Strategic Autonomy*.

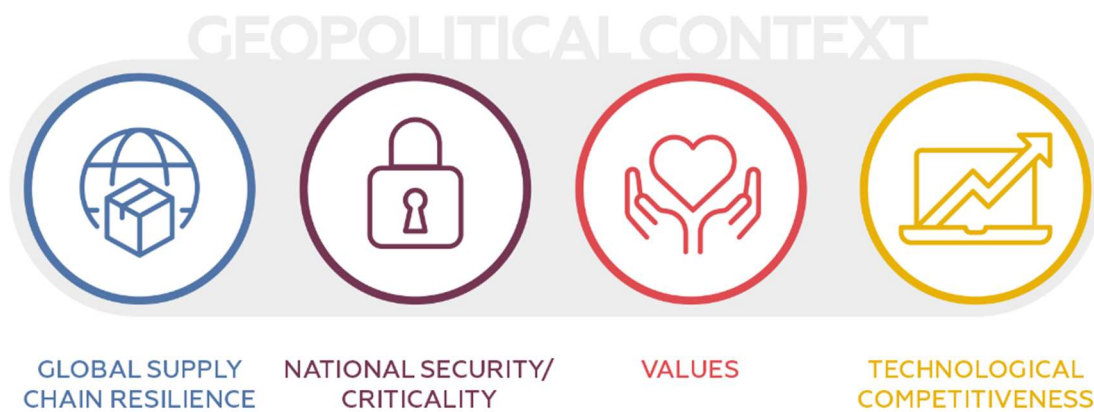


Figure 1.1 – Summary of the four dimensions of Open Strategic Autonomy

¹⁴ Optics.org, “Netherlands group claims €1.1BN for photonic chip scale-up”, 20 April 2022, <<https://optics.org/news/13/4/26>>.

¹⁵ Hideki Uno, “Japanese Semiconductor Industrial Policymaking in the Twenty-First Century”, Center for

Strategic and International Studies, Washington, DC, 19 September 2022, <<https://www.csis.org/blogs/perspectives-innovation/japanese-semiconductor-industrial-policymaking-twenty-first-century>>.



The complexity of navigating the four dimensions of Open Strategic Autonomy: three examples

This operationalization does not make Open Strategic Autonomy any less complex. Instead, the four dimensions should help to identify the weaknesses that the EU should strive to address in its attempt to gain Open Strategic Autonomy in any given foundational or emerging technology. In some cases, tensions exist between the dimensions. The three examples below illustrate the relationships between the dimensions.

Semiconductor front-end manufacturing

Semiconductor front-end manufacturing and the extent to which fabrication plants (“fabs”) should be given substantial subsidies are two issues currently receiving considerable attention from EU policymakers. A key element of the proposed EU Chips Act is a new subsidy strategy for “first-of-a-kind” fabs in Europe. The goal is to become less dependent on semiconductor manufacturing in Asia, especially Taiwan and South Korea which are currently the only places in the world with cutting-edge (5 nanometer, nm) manufacturing capacity.¹⁶ The problem is that Europe’s strongest semiconductor end-customer industries (industrial applications and medical equipment) predominantly rely and will continue to rely on older

manufacturing technologies (40nm, 90nm or even 180nm).¹⁷

Globally, most of the new fab launches by companies such as TSMC, Samsung, Intel and others are on cutting-edge capacity at 10nm and below. China is already an important location for “trailing-edge” fabs (20–45nm) and manufacturing on “mature nodes” (>45nm). Moreover, China has outspent every other region on manufacturing equipment: more than US\$ 92 billion worth of manufacturing equipment was shipped to China between Q1 2017 and Q1 2022.¹⁸ US export restrictions mean that this is almost entirely trailing-edge equipment. China spent over five times more on equipment than Europe in the same timeframe.

What does this mean? In the future, especially for older manufacturing technology, European companies will be more dependent than today on fabs in China, whether operated by Chinese or foreign companies. As there is a shortage of these older fabs globally, this strengthens *supply chain resilience*—giving European companies access to more manufacturing capacity than before. From a *national security* perspective, however, being dependent on a “systemic rival” for chip manu-

¹⁶ Jan-Peter Kleinhans, “The Lack of Semiconductor Manufacturing in Europe: Why the 2nm Fab is a Bad Investment”, Policy Brief, *Stiftung Neue Verantwortung*, 8 April 2021, <<https://www.stiftung-nv.de/en/node/3045>>.

¹⁷ ASML, “EU Chips Act: Position Paper”, February 2022, <<https://www.asml.com/-/media/asml/files/>

[news/2022/asml-position-paper-on-eu-chips-act.pdf?rev=cc4554892d7a4304bee8b056b96e4dee](https://www.asml.com/-/media/asml/files/news/2022/asml-position-paper-on-eu-chips-act.pdf?rev=cc4554892d7a4304bee8b056b96e4dee)>.

¹⁸ Jan-Peter Kleinhans, Testimony before the US–China Economic and Security Review Commission, US Congress, Hearing on US–China Competition in Global Supply Chains, *Stiftung Neue Verantwortung*, 9 June 2022, <https://www.uscc.gov/sites/default/files/2022-06/Jan-Peter_Kleinhans_Testimony.pdf>.



facturing may not be in Europe's best interest. Finally, regarding *technological competitiveness*, these older manufacturing technologies are still important and are being innovated for a variety of chips, from sensors to micro-controllers, power semiconductors and radio frequency applications. In a nutshell, China's investment spree in trailing-edge fabs is good for *global supply chain resilience* but poses very real *national security* and *technological competitiveness challenges* for Europe. This should encourage Europe to invest in its own manufacturing capabilities in these "older" technologies.

Technical standardization of 5G technology

5G infrastructure is a critical digital infrastructure that is foundational in a broad range of use cases. Mobile infrastructure is highly standardized and relies mostly on global standards developed by the International Telecommunications Union (ITU) and the Third Generation Partnership Project (3GPP). Whoever sets the technical standards in these institutions defines the technological parameters of the backbone of global critical digital infrastructure. These technical standards have a wide range of implications, not least the network security of the critical digital infrastructure.¹⁹

China's influence on the ITU and the 3GPP has grown significantly in recent years. Given the potential national security concerns and the criticality of 5G standardization, the rapid growth of China's influence in relevant standard-developing organizations should be of concern to the EU.²⁰ From a national security perspective, China's strength in these institutions could lead Europeans to advocate ignoring the technical standards developed based on Chinese contributions or even withdrawal from these international institutions.

What may sound like a logical solution from a national security perspective misses the very nature of technical standard setting. Technical standards are effective only if they achieve a broad consensus and are accepted by the market. Wireless infrastructure technology is global and no country can dominate the standard-setting process. From this perspective, neither exclusion nor withdrawal but a strengthening of European capacities coupled with continuous cooperation is necessary to boost European competitiveness.

In sum, although the national security perspective might suggest an isolation strategy, investment in Europe's own capabilities to better position cooperation

¹⁹ Tim Rühlig, *China, Europe and the New Power Competition over Technical Standards*, UI Brief 1/2021 (Stockholm: Swedish Institute of International Affairs, 2021), <<https://www.ui.se/globalassets/ui.se-eng/publications/ui-publications/2021/ui-brief-no.-1-2021.pdf>>.

²⁰ In the ITU-T, the most influential branch of the ITU in standardization, China has the second largest number of members, falling only slightly short of the United States. In the ongoing study period, China holds the

most technical leadership positions in the ITU-T study groups, focus groups and work programmes. In 3GPP, China has the highest share of individual members and technical leadership positions in technical specification groups and work programmes. Accordingly, China's share of 5G standard contributions has increased more than that of any other state compared to the previous mobile generation, 4G/LTE. China has also declared the most patent families to be standard essential.



is preferable from a technological competitiveness perspective.

Artificial Intelligence for facial recognition

The global market for facial recognition technology is projected to grow from US\$5 billion in 2022 to almost US\$13 billion by 2027.²¹ Facial recognition is alleged to increase security but it also challenges fundamental values, as it is based on enormous quantities of personal data in capturing the physiognomy of faces. AI algorithms are being trained and refined by collecting sensitive data without the consent of citizens. Surveillance, privacy, algorithmic biases and discrimination coupled with unresolved accuracy issues form the core of values-based concerns. However, facial recognition technology is deemed critical to societal and national security. Facial recognition is integral to many smart city solutions, which are now part of critical infrastructure. The vulnerabilities in facial recognition technology recently demonstrated by two Chinese companies operating in Switzerland provide actors with bad intentions with easy access to critical information, compromising

national security.²² Strikingly, Chinese firms have a legal obligation to report vulnerabilities to the PRC government within two days of their detection.²³

Some values-based challenges can be mitigated with effective regulation, such as the AI Act, the Digital Markets Act (DMA) and the General Data Protection Regulation (GDPR). However, regulations cannot resolve security vulnerabilities, and Europe does not provide an example of how a sensitive use case of AI, such as facial recognition, can be developed and refined in line with EU norms.

Strikingly, Europe is not technologically competitive in facial recognition. The industrial leader is Hikvision, a Chinese state-owned firm involved in human rights violations in Xinjiang. Until 2021, Hikvision cameras were still being used in the European Parliament building, among many other places in Europe.²⁴

This case illustrates another facet of the four dimensions of Open Strategic Autonomy. Although Europe does not need to be technologically competitive in all fields of emerging and foundational technologies,

²¹ Grand View Research, "Facial Recognition Market Size, Share & Trends Analysis Report By Technology (2D, 3D, Facial Analytics), By Application (Access Control, Security & Surveillance), By End-use, By Region, and Segment Forecasts, 2021–2028", accessed 16 December 2022 at, <<https://www.grandviewresearch.com/industry-analysis/facial-recognition-market#:~:text=The%20global%20facial%20recognition%20market,15.4%25%20from%202021%20to%202028>>.

²² Bernd Heubl and Christian Schürer, "Schweizer Behörden setzen auf chinesische Sicherheitskameras" [Swiss authorities rely on Chinese security cameras], SFR, 19 May 2022, <<https://www.srf.ch/news/>

[schweiz/sicherheitsmaengel-schweizer-behoerden-setzen-auf-chinesische-sicherheitskameras](https://www.srf.ch/news/schweiz/sicherheitsmaengel-schweizer-behoerden-setzen-auf-chinesische-sicherheitskameras)>.

²³ Cyber Administration of China, "工业和信息化部 国家互联网信息办公室 公安部关于印发网络产品安全漏洞管理规定的通知" [Notice of the Ministry of Industry and Information Technology, the State Internet Information Office, and the Ministry of Public Security on Issuing the Regulations on the Administration of Network Product Security Vulnerabilities], 13 July 2021, <http://www.cac.gov.cn/2021-07/13/c_1627761607640342.htm>.

²⁴ Charles Rollet, "EU Parliament removes Hikvision, citing human rights abuses", IPVM, 29 April 2021, <<https://ipvm.com/reports/hik-eu>>.



the challenges to European values and national security dimensions make Europe’s lack of technological competitiveness a serious problem.

Conclusions: How can Open Strategic Autonomy be achieved?

Although operationalizing Open Strategic Autonomy is necessarily complex, differentiating among the four dimensions helps to identify the EU’s goals and potential trade-offs between the different dimensions in any given technological field.

The case studies in this volume indicate that the urgency and severity of the four dimensions of Open Strategic Autonomy vary across technologies and their applications. Figure 1.2 summarizes the findings

		DIMENSION OF OPEN STRATEGIC AUTONOMY			
TECHNOLOGY		Resilience of supply chains	Criticality/national security	Defence of universal values/sustainability	Technological competitiveness
	Chip design	●	●	●	●
	6G development	●	●	●	●
	Blockchain technology	●●	●●	●	●●
	Introduction of central bank e-currency	●●	●●	●	●●●
	Artificial Intelligence in automotive applications	●	●	●	●
	Artificial intelligence in smart city applications	●	●	●	●
	Artificial intelligence ethics	●	●	●	●

- very high degree of threat
- high degree of threat
- moderate degree of threat
- low degree of threat
- not applicable

Figure 1.2 – Degree of challenge to the four dimensions of European Open Strategic Autonomy presented by China in emerging and foundational technologies and their applications



To navigate this complexity, we suggest a four-step process that helps to identify the challenges along the lines of the four dimensions and directs the EU to the right tools for addressing them.

- *First step: Ecosystem analysis.* A long-term, institutionalized and continual ecosystem analysis should form the backbone and analytical basis of Europe's Open Strategic Autonomy Strategy. Identifying and assessing inter-dependencies within technology ecosystems, such as semiconductors, cannot be meaningfully achieved with single reports such as the Staff Working Document.²⁵ These are too superficial to inform long-term policy planning and can only be a starting point. Europe needs to invest in its own capacity to assess and track a variety of technology ecosystems. To manage strategic dependencies and meaningfully inform trade, security, industrial or research policy, government units will need a robust understanding of each specific technology ecosystem. For example, neon, xenon, argon and krypton are important gases for semiconductor manufacturing. To assess whether Europe should invest in its own noble gas supply, policy-makers would need to understand the role these noble gases play in semiconductor manufacturing, the extent

to which fabs can store these gases and what the global supplier market looks like, among other things. This would only be achievable with dedicated units in government mapping technology ecosystems.²⁶ This would also enable governments to shape forward-looking policy by identifying potential future strategic dependencies.²⁷

The result of this first step should be a clear identification of the EU's dependencies.

- *Second step: Assessing Europe's position in terms of the four dimensions of Open Strategic Autonomy.* Based on a proper understanding of the ecosystem, the EU should assess the challenges that result from these dependencies in terms of the four dimensions of Open Strategic Autonomy: the resilience of its supply chains; the criticality of the technology, including potential implications for national security; potential threats to universal values promoted by the EU; and European technological competitiveness. These dimensions can also be in conflict with each other, as is the case with dependence on China for trailing-edge semiconductor manufacturing. Heavily subsidized trailing-edge fabs in China strengthen supply chain resilience because these fabs are currently globally in short

²⁵ European Commission, Strategic dependencies and capacities, SWD(2021) 352 final, Commission Staff Working Document, 5 May 2021, <[https://www.eu.dk/samling/20211/kommissionsforslag/kom\(2021\)0350/forslag/1779363/2388551.pdf](https://www.eu.dk/samling/20211/kommissionsforslag/kom(2021)0350/forslag/1779363/2388551.pdf)>.

²⁶ Julia Hess and Jan-Peter Kleinhans, "Recommendation for the EU Chips Act: A long-term government value

chain mapping", *Stiftung Neue Verantwortung*, 6 July 2022, <<https://www.stiftung-nv.de/en/publication/eca-mapping>>.

²⁷ Martijn Boerkamp, "Netherlands invests €1.1bn in the photonic-chip industry", *Physics World*, 19 May 2022, <<https://physicsworld.com/a/netherlands-invests-e1-1bn-in-the-photonic-chip-industry/>>.



supply and are desperately needed for many automotive and industrial microcontrollers. Becoming increasingly dependent on Chinese semiconductor manufacturing, however, comes with potential national security and political costs. Such an assessment would inform EU policymakers whether state aid for trailing-edge fabs in Europe is ultimately justifiable due to overriding interests in connection with Europe's Open Strategic Autonomy.

The result of this step should be a clear understanding of what achieving Open Strategic Autonomy in a given field of emerging or foundational technology means.

- *Third step: Geopolitical contextualization.* Next, the EU would need to identify the geopolitical context of these challenges. Whether Europe is reliant on supplies from geopolitical partners or systemic rivals matters because the likelihood of an acute crisis or even a military confrontation varies. This is not to say that the EU cannot accept any dependence on systemic rivals, but the threshold that the EU should tolerate differs in at least some dimensions (e.g., national security) of Open Strategic Autonomy. Instead of simply trying to reduce strategic dependencies in transnational value chains, a more pragmatic strategy might be to ensure inter-dependence within the same technology ecosystem. While Europe is dependent on Chinese and Taiwanese semiconductor

manufacturing, fabs in China and Taiwan heavily depend on European semiconductor manufacturing equipment and the chemicals required to produce these chips.

The result of this step should be an understanding of the geopolitics of the EU's Open Strategic Autonomy in a given emerging or foundational technology.

- *Fourth step: Use the available toolkit* Based on the three previous steps, the EU will be able to identify the appropriate policy tools. These tools range from an active industrial policy to trade and investment agreements, regulation, protection of critical sectors, tariffs and sanctions, and export controls. The chosen tools should fit the analyses of the three previous steps. For example, where technological competitiveness is the main concern, the reshoring of capabilities through an active industrial policy would be most appropriate. If national security concerns dominate, and geopolitical contextualization has identified a high dependence on potential adversary diversification, preferential conditions for diversification through trade and investment instruments would be a better fit.

The case studies in this volume provide a first indication that certain policy tools tend to be more appropriate for addressing any given specific dimension of Open Strategic Autonomy. Figure 1.3 provides an overview.







DIMENSION OF OPEN STRATEGIC AUTONOMY	PREDOMINANT POLICY GOAL	TYPE OF POLICY INSTRUMENTS THAT TEND TO BE MOST EFFECTIVE
 Resilience of supply chains	Diversification	<ul style="list-style-type: none">• Transparency measures• Diversification incentives, e.g. procurement• Cooperation with third parties, e.g. Free Trade Agreements• Protection of indispensable actors
 Criticality/national security	Technical and vendor trustworthiness	<ul style="list-style-type: none">• Regulation• Certification• Standardization• Like-minded sourcing
 Defence of values/sustainability	Like-minded coordination	<ul style="list-style-type: none">• Regulation• Like-minded cooperation
 Technological competitiveness	Strengthening of innovation and industrial base	<ul style="list-style-type: none">• Industrial policy• R&D investment• Protection of indispensable actors

Figure 1.3. – Policy goals and instruments of the four dimensions of Open Strategic Autonomy

These four steps illustrate the complexity of achieving Open Strategic Autonomy. They require knowledge of various fields, as well as technical and country-specific political expertise. Only interdisciplinary

analyses will provide a solid basis for policymaking that brings the European Union and its member states closer to Open Strategic Autonomy.

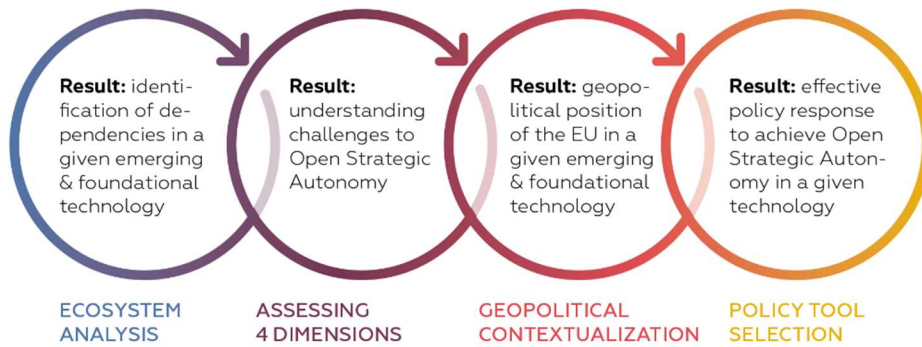


Figure 1.4. – The four-step process for identifying appropriate tools for addressing the challenges to Europe’s Open Strategic Autonomy

Authors:

Jan-Peter Kleinhaus is Head of Technology and Geopolitics at Stiftung Neue Verantwortung e.V. in Berlin, Germany. Contact: jkleinhans@stiftung-nv.de

Tim Rühlig is a Senior Research Fellow at the German Council on Foreign Relation and an Associate Research Fellow in the Swedish Institution of International Affairs’ Europe program. He is based in Germany. Contact: ruehlig@dgap.org



Challenges of a rising Chinese chip design ecosystem

Jan-Peter Kleinhans, John Lee

Abstract

The growing competitiveness of Chinese chip design companies has so far been neglected by policymakers in Europe. Despite the recent US export controls targeting China's semiconductor industry, it is highly likely that Chinese chip design companies will gain global market share in a range of industry sectors in this decade. This presents challenges across the dimensions of national security, supply chain resilience and technological competitiveness for Europe, its end-customer industries and semiconductor companies. Importantly, most of these challenges are not currently addressed by the proposed European Chips Act and will require different and tailored policy responses. Europe must: (a) invest in its own chip design capabilities; (b) strengthen the "strategic indispensability" of its semiconductor companies and technology providers through policy interventions; (c) engage with national and industry actors in discussions on the international structure of the semiconductor value chain and managing conflicting interests, including among the US-allied community; and (d) map the risk profile of increasing reliance on Chinese chip design across different sectors and industry verticals.

Semiconductors are a foundational technology and critical inputs in almost every other industry. Their production can be divided into three distinct steps: chip design, front-end manufacturing (wafer fabrication) and back-end manufacturing (assembly, test and packaging). Since 2020, spurred by global chip shortages, policymakers in Europe, the United States, Japan, South Korea, India and elsewhere

have scrutinized their national dependency on foreign semiconductor manufacturing. This has resulted in substantial subsidy packages, such as the proposed European Chips Act, to incentivize the construction of domestic fabrication plants or "fabs".²⁸ In many ways, policymakers now increasingly care about where chips are manufactured rather than where chips are designed. This has also shaped the

²⁸ Jan-Peter Kleinhans, Julia Hess and Wiebke Denkena, "Analysis of the EU Chips Act: Challenges of government monitoring of the supply chain",

Stiftung Neue Verantwortung, 7 June 2022, <<https://www.stiftung-nv.de/en/publication/eca-monitoring>>.



way in which policymakers look at China's ambitions and growing importance in the global semiconductor ecosystem. The achievements of China's indigenous semiconductor manufacturing ecosystem, from foundries (such as Semiconductor Manufacturing International Corporation, SMIC) to memory chip manufacturers (such as Yangtze Memory Technologies, YMTC), receive regular media attention but the same is not the case for advances in chip design by Chinese companies, even though this is one of the most notable areas of Chinese progress in recent years.

China's chip design ecosystem has made rapid advances, in some areas such as machine learning accelerators (or "AI chips") even reaching the global cutting-edge. If rigorously enforced, the US export controls instituted in October 2022 will make it highly unlikely that Chinese chip design companies can increase their international competitiveness in high-performance processors, cloud AI accelerators and cutting-edge memory chips. However, most types of semiconductors are not addressed by the new US restrictions.²⁹ In the areas not targeted by US export controls, Chinese chip design companies will probably continue to strengthen their capabilities and compete internationally. In doing so, they will benefit from China's strength in adjacent industries, such as internet and computing service platforms,

consumer electronics and electric vehicles, for which innovation in semiconductors provides a competitive advantage. A globally competitive Chinese chip design ecosystem therefore strengthens the global competitive position of many Chinese companies in other verticals.³⁰

This also creates new dependencies and potential challenges for European industries, regarding their long-term technological competitiveness if they come to rely on chips that are "designed in China". The dual-use nature of specific types of chips also means that Chinese chip design capabilities could have defence- and espionage-related implications, which potentially pose national security challenges. These are increasingly of concern to US policymakers in particular, who are already taking unilateral actions in response that directly impact European interests, most notably in the October 2022 export controls.

This chapter provides an overview of the foundation for and long-term potential of China's domestic ecosystem for chip design and examines the impacts on this ecosystem of the October 2022 US export controls. We then analyse the challenges and path-dependencies of China's chip design ecosystem and the implications for Europe along the four dimensions of technology autonomy as outlined in the introduction. We conclude with four policy recommendations on a European response.

²⁹ US Government, US Industry and Security Bureau, "Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification", 13 October 2022, <<https://www.federalregister.gov/d/2022-21658>>.

³⁰ John Lee and Jan-Peter Kleinhans, *Mapping China's Semiconductor Ecosystem in Global Context: Strategic Dimensions and Conclusions*, MERICS and SNV Policy Brief, June 2021, <https://www.stiftung-nv.de/sites/default/files/chinas_semiconductor_ecosystem.pdf>.



Foundations and long-term potential of China's chip design ecosystem

The first factor driving development of China's chip design sector is the concentration and rapid development of end-user industries in China. The semiconductor industry is a supplier market and chips are inputs to countless end-products. This also means that in verticals such as smartphone consumer electronics companies, cloud providers (hyperscalers) and electric vehicle manufacturers, competition increasingly takes place not just at the software level, but also at the hardware level. This virtuous circle of development between verticals that increasingly rely on innovation in chips and the chip design ecosystem creates long-term advantages for China's chip design capabilities.

This is not just about Chinese hyperscalers, such as Alibaba or Tencent, investing in in-house chip design. It is also about a growing number of fabless start-ups, such as Biren Technologies, Black Sesame or Horizon Robotics, designing AI chips and power semiconductors, among many other types of chips, not just to serve domestic companies, but to strengthen their competitiveness on international markets as well. The virtuous circle also means that domestic chip designers can learn and improve through cooperation with domestic and international end-customer industries. This will provide European firms with increasing incentives to partner with Chinese entities. One such example is Volkswagen's new joint venture with the Chinese

chip design firm, Horizon Robotics, to develop a System-on-Chip (SoC) for autonomous driving that will be available only in China.³¹ Another is the partnership between the Japanese leader in electronics components, Rohm, and Chinese firms like UAES to apply silicon-carbide (SiC) power devices in new energy vehicles.

A second factor supporting the long-term potential of China's chip design sector is China's massive talent pool. Chip design is mainly skill-intensive and thus heavily reliant on highly skilled labour. China has been developing its tertiary education institutions to produce workers for the semiconductor industry, while its chip design sector has benefited from Chinese nationals who have gained work experience with foreign, especially US, firms. However, access to foreign and foreign-trained talent has been put under pressure by China's zero-Covid policy and US government restrictions: the "US persons" provisions in the most recent US export controls impose restrictions on many executives and other important personnel in China's leading semiconductor companies who hold US citizenship or green cards. Chinese industry insiders also see the semiconductor sector as having difficulties competing for university graduates, and the general level of labour force expertise in China as lagging behind that of other countries, although this is more pronounced for electronic design automation (EDA)

³¹ Victoria Waldersee, "Volkswagen to take 60% stake in \$2 bln tech JV with China's Horizon Robotics", Reuters, 13 October 2022, <<https://www.reuters.com/business/autos-transportation/volkswagen-take-60-stake-tech-joint-venture-with-chinas-horizon-robotics-2022-10-13/>>.

[com/business/autos-transportation/volkswagen-take-60-stake-tech-joint-venture-with-chinas-horizon-robotics-2022-10-13/](https://www.reuters.com/business/autos-transportation/volkswagen-take-60-stake-tech-joint-venture-with-chinas-horizon-robotics-2022-10-13/)>.



software and manufacturing than for chip design.³²

There are objective indicators of the increasing quality of China's skilled workforce in this industry. For the first time, a majority of the accepted submissions to the 2023 International Solid-State Circuits Conference (ISSCC), one of the most prestigious academic semiconductor conferences, for example, were authored by Chinese institutions. Of the 629 submitted research papers, 198 passed screening of which 59 were from China, 42 from the US and 32 from South Korea.³³ So while the "US persons provisions" are certainly a blow to China's chip design ecosystem in the short- to medium-term, China is able to draw on an increasingly competitive academic ecosystem and thus a rich homegrown talent pool. By the Chinese authorities' own judgment, however, effectively linking research with applications for industry will remain a key challenge. China's semiconductor ecosystem has benefited from the practical experience of large numbers of foreign (especially Taiwanese) industry veterans working in Chinese firms and training up local staff. It will take time for large numbers of Chinese personnel to acquire enough applied knowledge from "sitting ten years on the cold bench", to use a local phrase about

the necessity for hard-earned experience in the industry.

A third enabling condition for China's chip design sector is state support. In the 1990s, the Chinese authorities were still taking a command-style approach to developing industry champions, but this has evolved over the past two decades into so-called grand steerage, whereby the state channels resources through indirect, market-conforming instruments to "steer" the economy towards broadly defined goals.³⁴ Among the main instruments of this approach are "government guidance funds", notably the "Big Fund" set up in 2014 for dedicated investment in the integrated circuits industry. Policy support for a given industry also encourages investment by the private sector, including foreign actors. In mid-2022, the Shanghai Stock Exchange established a "STAR Chip Index" for leading firms by market capitalization in China's semiconductor industry.³⁵

For many years, Chinese industry policy has made chip design a priority and chip design firms have been notable recipients of investment from the Big Fund. The chip design sector's relatively low barriers to entry and upstream position in the value chain make it an "easy pick" for state officials and fund managers who hope that

³² Coco Feng, "China's semiconductor self-sufficiency drive needs to strengthen development of talent and skills, education agency executive says", *South China Morning Post*, 5 October 2022, <<https://sc.mp/ti4q>>.

³³ Michael Herh, "China distinguishing itself at ISSCC 2023", *Business Korea*, 17 November 2022, <<http://www.businesskorea.co.kr/news/articleView.html?idxno=104260>>.

³⁴ Barry Naughton, "Grand Steerage as the New Paradigm for State-Economy Relations", in Frank N. Pieke and Bert Hofman (eds), *CPC Futures: The New Era of Socialism with Chinese Characteristics*, NUS Press, 7 September 2022.

³⁵ Shanghai Stock Exchange, "Release of SSE STAR Chip Index: Spotlight for Demonstration Effect of Key Technology", 20 May 2022, <<http://english.sse.com.cn/news/newsrelease/c/5702887.shtml>>.



it will drag along development of downstream value chain steps and end-user industries. Subnational governments in China promote chip design through basic measures such as designating zones for semiconductor-related technology clusters.

In Shanghai's Lingang Special Area, for example, design firms such as Cambricon and Horizon Robotics are co-located with firms operating in other steps of the value chain, all of which benefit from import duty exemptions on their inputs.

Impacts of the October 2022 US export controls

A major constraint on China's chip design sector was introduced by the sweeping US export controls instituted in October 2022, which restrict supply of various semiconductor-related technologies to China. These controls are so extensive that they have been described by many analysts as amounting to a strategy of "technological containment" of China. This framing has been reinforced by recent comments on US technology and trade policy by senior officials in the Biden administration.³⁶

While these controls do not directly target chip design, their negative effects on the wider Chinese semiconductor sector and the industries that depend on it are likely to dampen demand and investment in Chinese fabless firms, and the in-house design units of Chinese technology majors, at least in the short term. Promulgation of the new controls immediately triggered a stock market fall of around \$US 8.6 billion for Chinese firms involved in

the semiconductor sector, such as Cambricon and Horizon Robotics.³⁷ Additional US government controls are expected to follow to restrict outbound investment in China, much of which has been in Chinese chip design firms.

The new controls restrict the involvement of US persons (citizens or permanent residents) in China's semiconductor sector, which will also hamper the development of chip design capability. Many important figures in Chinese EDA software and chip design start-ups are reportedly in this category. The new controls will force such individuals to choose between working in China and their US residence rights, while also making it impossible to attract much of the foreign and possibly Chinese expatriate talent that might otherwise have been ready to work for or with Chinese firms. The US persons provisions are also likely to be a strong deterrent to US semiconductor firms doing business with

³⁶ The White House, "Remarks by National Security Advisor Jake Sullivan at the Special Competitive Studies Project Global Emerging Technologies Summit", 16 September 2022, <<https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/09/16/remarks-by-national-security-advisor-jake-sullivan-at-the-special-competitive-studies-project-global-emerging-technologies-summit/>>; Office of the US Trade Representative, "Remarks by Ambassador Katherine Tai at the Roosevelt Institute's Progressive

Industrial Policy Conference", October 2022, <<https://ustr.gov/about-us/policy-offices/press-office/speeches-and-remarks/2022/october/remarks-ambassador-katherine-tai-roosevelt-institutes-progressive-industrial-policy-conference>>.

³⁷ Hudson Lockett, "China chip stocks lose \$8.6bn in wipeout due to US export controls", *Financial Times*, 10 October 2022, <<https://www.ft.com/content/63a408cf-b4cc-4825-a6aa-ad829142e335>>.



Chinese entities through shell companies and other clandestine means. This is probably by design, given that one of the “big three” EDA vendors is reportedly under investigation for selling to Huawei and SMIC in breach of older export controls targeted at those individual entities.³⁸

Much will depend on enforcement of the new US export controls, which could be revised or expanded in the coming months. If their application is limited to the four areas addressed in the current regulation – high-performance and supercomputing, cloud AI acceleration, advanced semiconductor manufacturing and manufacturing equipment – this is likely to have

limited impacts on Chinese chip design companies serving other sectors, such as automotive, mobile chipsets, internet of things (IoT) and industrial applications, at least until the general requirements for computing power in these sectors increase significantly. At the time of writing, however, some new rules have been drafted in terms that potentially allow them to be used to restrict Chinese industry’s access to less sophisticated chips. If this is the case, the other sectors mentioned above could be significantly impacted, with negative follow-on effects for Chinese chip design firms. That said, this is not the US government’s current intention according to official statements.³⁹

Challenges and path-dependencies of China’s chip design ecosystem

Notwithstanding the long-term potential of China’s chip design ecosystem, it also faces significant challenges. The intensifying US–China technology rivalry essentially means that Chinese chip design companies could be cut off from upstream suppliers (EDA tools and semiconductor intellectual property, IP, vendors) and downstream front-end manufacturing (equipment vendors and fabrication providers) within a matter of months, or potentially even days.

A key challenge for China’s chip design ecosystem is its dependence on the US-origin *electronic design automation* tools that are essential for designing semiconductors. Access to EDA tools is essential in order to design chips and the leading EDA tool suppliers, Cadence, Synopsys and Mentor (acquired by Siemens in 2017), are all US-based. While there have been several initial public offerings in China’s homegrown EDA ecosystem since 2021, and Chinese EDA start-ups receive a lot of attention from public and private investors, this is still in its infancy.

³⁸ Ian King and Jenny Leonard, “Synopsys probed on allegations it gave tech to Huawei, SMIC”, Bloomberg, 13 April 2022, <<https://www.bloomberg.com/news/articles/2022-04-13/synopsys-probed-on-allegations-it-gave-chip-tech-to-huawei-smic>>.

³⁹ Martin Rajser, “A Conversation with Under Secretary of Commerce Alan F. Estevez”, Center for a New American Security, 27 October 2022, <<https://www.cnas.org/publications/transcript/a-conversation-with-under-secretary-of-commerce-alan-f-estevez>>.













ACTOR TYPE	NAME OF KEY ACTOR	DESCRIPTION	KEY TASK	PRIORITY
'Government guidance fund' (state-linked sectoral investment fund)	 National Integrated Circuit Industry Investment Fund (Big Fund) 国家集成电路产业投资基金	Supervised by Ministry of Industry and Information Technology (MIIT)	Investment in semiconductor sector in line with policy priorities	●
'Leading Small Group' (interagency steering body)	 IC Industry Development Leading Small Group (国家集成电路产业发展领导小组)	At time of establishment, vice-chair was Director of MIIT	Policy oversight for the IC sector	◐
Industry R&D consortium	 IC Industry Technical Innovation Strategic Alliance (集成电路产业技术创新战略联盟)	Ministry of Science and Technology is registrar (holds authoritative copy of body's constitution)	Integrated R&D across the IC sector and facilitating collaborative innovation	◐
Industry representative body	 China Semiconductor Industry Association (中国半导体行业协会)	MIIT (supervision and guidance of activities)	Industry assessments and data collection, information exchange, policy implementation, international exchanges, member representation	◐
Industry consortium	 China RISC-V Industry Consortium (中国RISC-V产业联盟)	Led by Verisilicon (publicly listed company)	Development of RISC-V based technology	◐
Industry R&D consortium	 China Open Instruction Ecosystem Alliance (中国开放指令生态)	Chinese Academy of Sciences (Institute of Computing Technology)	Development of RISC-V based technology	◐
R&D institute	 Beijing Open Source Chip Research Institute (北京开源芯片研究院)	Chinese Academy of Sciences (Institute of Computing Technology)	Development of RISC-V based technology, especially Xiangshan HPC open-source processor project	◐
Company (Foundry provides chip manufacturing services)	 Semiconductor Manufacturing International Corporation (SMIC) (中芯国际集成电路制造有限公司 (中芯国际))	Publicly listed company, partially state-owned	China's most advanced fabrication provider	●
Company (Equipment maker and systems integrator)	 Shanghai Microelectronics Equipment (SMEE) (上海微电子装备(集团)股份有限公司)	State-owned	China's leading producer of photolithography systems	◐
Company (Memory chip maker)	 Yangtze Memory Technology Corporation (YMTC) (长江存储科技有限责任公司)	Holding company-owned	Technologically leading memory chip manufacturer	◐

Figure 2.1 – An overview of the technical and political actors driving China's 6G development



Like EDA, *semiconductor IP* is another critical input to chip design. Since China is a “fast follower” in the semiconductor ecosystem, having joined the globalized value chain late and in lower value-added steps, there is a relative lack of domestic semiconductor IP. This makes Chinese chip design activities heavily reliant on foreign, especially US, semiconductor IP for core functionalities such as input/output (I/O), memory and compute.

Dependence on foreign providers for *front-end manufacturing (fabrication)* poses another challenge for the growth of China’s chip design ecosystem. Most, if not all, globally competitive chips “designed in

China” rely on cutting-edge front-end manufacturing in Taiwan. Like the rest of the world, Chinese fabless companies depend on manufacturing by TSMC in Taiwan, specifically for cutting-edge logic chips such as processors, AI accelerators and System-on-Chips. TSMC’s dependence on US-origin manufacturing equipment and fab technology means that the US government can always apply the foreign direct product rule to use export controls to block Chinese fabless companies’ access to TSMC’s fabrication services, leaving them unable to have their leading-edge chip designs manufactured into products.

Implications for Europe

China’s chip design ecosystem has a lot of long-term potential even in the light of the latest US restrictions. China already has globally competitive companies in many verticals that directly benefit from innovation in semiconductors, such as hyperscalers (Alibaba, Tencent, Baidu), electric vehicles (BYD, Nio), consumer electronics (Xiaomi), smartphones (OPPO, Vivo, OnePlus) and mobile infrastructure (Huawei, ZTE). A few Chinese firms (most notably Haier) have also become competitive in “smart manufacturing” and “industrial internet” systems, which also benefit from chip design to optimize various functions within these technological ecosystems.⁴⁰ The Chinese state encourages the development of all these fields and

probably has the resources to further increase effective subsidy levels, especially if this is seen as necessary to compensate for the negative impacts of foreign measures such as US export controls or to support critical import substitution efforts.

Very few, if any, European companies are present in many of these end-customer markets. Consequently, Europe will be increasingly confronted not just with end-products assembled in China, but chips designed in China at the core of these products. The above-mentioned virtuous circle between end-customer industries and chip design capabilities will also enable Chinese chip design companies to enter other verticals, to compete internationally and potentially to supply European

⁴⁰ Rebecca Arcesati et al., “China’s digital platform economy: Assessing developments towards Industry 4.0”, MERICS, 29 May 2020, <<https://merics.org/en/>

[report/chinas-digital-platform-economy-assessing-developments-towards-industry-40](https://merics.org/en/report/chinas-digital-platform-economy-assessing-developments-towards-industry-40)>.



end-customer industries. Over time, this will create new dependencies among European end-customer industries on chips “designed in China”. In the example of Volkswagen’s cooperation with Horizon Robotics mentioned above, even if the products of this collaboration serve only the Chinese market, this reinforces Volkswagen’s dependence on access to China to remain profitable and a global technological leader.

This prospect of growing European dependence on China’s chip design ecosystem, and chips designed in China, will have impacts on Europe’s Open Strategic Autonomy. We assessed Open Strategic Autonomy across the four dimensions of supply chain resilience and security of supply, national security, values and sustainability, and technological competitiveness, and offer the following evaluation of each of these dimensions.

Supply chain resilience and security of supply

For the most part, chip design does not depend on physical inputs in the way semiconductor manufacturing does. Thus, generally speaking, an increasingly competitive Chinese chip design ecosystem will have little impact on Europe’s security of supply of chips or overall supply chain resilience. If in the long-term European end-customer industries come to increasingly depend on Chinese-origin chips,

however, and if the Chinese government implements similar crisis response measures to those currently envisaged in the EU Chips Act (priority-rated orders and export authorizations), Europe’s supply of Chinese-origin chips could be disrupted during a future chip shortage due to interventions by the Chinese government.⁴¹ The extent of such impacts would be influenced not only by China’s strength in semiconductor design, but also by the share of global semiconductor manufacturing located in China, even if not necessarily owned by Chinese firms.

National security

Increasing dependency on chips designed in China could have negative impacts on national security in EU member states for two main reasons. First, as the US government argues in its justification for its October 2022 export controls, chips used in supercomputers and machine learning have direct military utility in simulating and enhancing preparedness for future armed conflict.⁴² The greater national capacity that China has in chip design, the higher the potential strategic advantage to the Chinese military. Second, the threat of hidden hardware backdoors and “kill switches” grows with the increasing complexity of chips.⁴³ The rise of chiplets and heterogeneous integration as approaches to packaging semiconductors into their end-use form means that the threat of so-called

⁴¹ Jan-Peter Kleinhans and Julia Hess, *Analysis of the EU Chips Act: The Crisis Response Toolbox*, Stiftung Neue Verantwortung, September 2022, <https://www.stiftung-nv.de/sites/default/files/governments_role_in_the_global_semiconductor_value_chain_3_0.pdf>.

⁴² US Government, US Industry and Security Bureau (note 299).

⁴³ Jeff Goldman, “Chip Backdoors: Assessing the Threat”, Semiconductor Engineering, 4 August 2022, <<https://semiengineering.com/chip-backdoors-assessing-the-threat/>>.



hardware hacks must already be considered when implementing a single Chinese chiplet as part of a non-Chinese chip design.⁴⁴ These threats are very similar to those that stem from the deployment in Europe of mobile network equipment manufactured by Chinese entities such as Huawei and ZTE.⁴⁵ Depending on the type of chip and the use scenario, the trustworthiness of the chip design company and the fab might also be relevant. The increasing presence of Chinese equipment in the rapidly expanding global IoT further amplifies this security risk.⁴⁶

Values and sustainability

A growing dependence on chips from Chinese companies does not pose any challenges to Europe's Open Strategic Autonomy in terms of values. This emerges as an issue once software runs on these systems, such as facial recognition algorithms or other forms of data analysis. At the hardware level, however, there are negligible impacts. Compared to the challenges that stem from the other three dimensions, sustainability issues are also of little concern when assessing Europe's growing dependence on Chinese-origin chips. The Chinese authorities are themselves conscious of the imperative to increase energy efficiency and reduce resource consumption, and these priorities are written into China's various policies on develop-

ment of the digital industries that depend on semiconductors and chip design.

Technological competitiveness

Next to national security challenges, Europe's long-term technological competitiveness is potentially affected most by the growing Chinese chip design ecosystem. Many products in which European companies have had historically strong positions, such as cars and robotics, increasingly compete at the level of hardware- and software-innovation, as well as optimization of the interactions between the two. These "cyber-physical systems" make up a growing share of economic activity and national infrastructure as a result of the expanding IoT.⁴⁷ Even if European companies continue to excel in the traditional electrical and mechanical engineering aspects of these products, Chinese companies might be able to out-compete their European counterparts due to innovation in chip design. Chip design capabilities will reinforce Chinese strengths in other supply chain segments, as is already evident in the electric vehicle sector where Chinese carmakers benefit from Chinese minerals processing and battery making suppliers.

When assessing the impact on Europe's Open Strategic Autonomy in these four dimensions, the effects of the sweeping

⁴⁴ Ed Sperling, "Security Risks Widen With Commercial Chiplets", *Semiconductor Engineering*, 7 July 2022, <<https://semiengineering.com/security-risks-widen-with-commercial-chiplets/>>.

⁴⁵ Jan-Peter Kleinhans, "Whom to trust in a 5G world?", *Stiftung Neue Verantwortung*, December 2019, <https://www.stiftung-nv.de/sites/default/files/whom_to_trust_in_a_5g_world.pdf>.

⁴⁶ Alexi Drew, "Chinese technology in the 'Internet of Things' poses a new threat to the west", *Financial Times*, 10 October 2022, <<https://www.ft.com/content/cd81e231-a8d3-4bc0-820a-13f525a76117>>.

⁴⁷ John Lee, "The Connection of Everything: China and the Internet of Things", *MERICs*, 24 June 2021, <<https://meric.org/en/report/connection-everything-china-and-internet-things>>.



US export controls of October 2022 must be taken into account. These restrictions have made the task of balancing the risks and benefits of engaging with China’s semiconductor sector and related end-user industries far more difficult. The clear objective of the controls is to completely cut-off China’s access to cutting-edge and next-generation computer processors,

whether imported or domestically produced. These are the very products that Chinese chip design firms are primarily working on, and this is where their value primarily lies as partners for European firms in end-user industries such as car making, and potentially in more wide-ranging fields such as intelligent manufacturing systems.

DIMENSION OF STRATEGIC AUTONOMY	SHORT DESCRIPTION OF CHALLENGE IN KEYWORDS	RELATIVE IMPORTANCE OF CHALLENGE ON A SCALE OF 1 TO 4	POLICY INSTRUMENTS FOR TACKLING CHALLENGE IN KEYWORDS
 Resilience of supply chains	Mitigating risks of interruptions to supply associated with rising dependence on chips designed and manufactured in China	2	Integrated discussions across the US-allied community; mapping and domain-specific risk assessment of dependence on chips of Chinese origin
 National security	Constraining China’s access to leading-edge military capabilities; guarding against Chinese hardware-enabled espionage & sabotage	3	Integrated discussions across the US-allied community; mapping and domain-specific risk assessment of dependence on chips of Chinese origin
 Values and sustainability	Ensuring that the semiconductor industry’s development and end-uses are sustainable and in line with European values	1	Coordinated cross-sectoral approach with end-user industries; mapping and domain-specific risk assessment of dependence on chips of Chinese origin
 Technological competitiveness	Ensuring that Europe maintains and builds world leading firms that occupy indispensable roles in the global semiconductor supply chain, thereby also providing a foundation for competitiveness in end-user industries	4	EU Chips Act; coordinated cross-sectoral approach with end user industries; focus on sustaining leverage in the global value chain by protecting European firms that are “indispensable” technology providers

Figure 2.2 – Main Chinese semiconductor technology-related risks

Recommendations for European Policymakers

For Europe, these issues are therefore tied to the macro question of Europe’s international positioning between the US and China, particularly as the EU itself currently

has limited chip design capabilities. In the context of chip design, China’s relative position in the global semiconductor industry means that the choice is not between



dependence on either the US or China. Instead, it is probably between maintaining access to both US and Chinese technology ecosystems (with a bias towards the former), on the one hand, and the high degree of dependence on US industry that would probably be implied by severing links with Chinese industry, on the other.

The US is pursuing other international cooperative initiatives on semiconductors, notably the so-called Chip 4 Alliance with Taiwan, Japan and South Korea. It is not evident that European interests are being adequately considered in these discussions, and there is already concern in various EU quarters about the implications for European firms' future competitiveness vis-a-vis companies from the US and its East Asian allies. Specifically, it is not clear what consideration is being given to ASML's long-term competitiveness and the consequences for supplier firms such as Trumpf and Zeiss, particularly as the US appears to be dealing with this issue through bilateral discussions with the Netherlands. Nor is it clear that the significant exposure to China of STMicroelectronics, Infineon, NXP and other European firms in the semiconductor sector, or of major semiconductor end-user industries, is being taken into account in discussions on supply chain restructuring.

Conversely, even before accounting for the new US export controls and US political pressure to align against China, integration with China's chip design ecosystem brings significant political risks. China's

government recently proved ready to weaponize economic relations against an EU country (Lithuania) over its relations with Taiwan, with consequences also for firms in other EU member states. The intrusive data regulatory regime imposed by the Chinese state means that operating in China will continue to create problems of data security and intellectual property protection for European businesses. The Chinese state is increasingly arming itself with "counter-sanctions"-type instruments in retaliation for foreign measures seen as discriminating against Chinese interests, and Beijing may choose to use these cross-sectorally and disproportionately. Above all, the general advance of Chinese firms' capabilities will increasingly make them effective competitors not only in China, but in third party markets and even the EU itself.

In view of these multifaceted challenges, and of Europe's difficult balancing act amid the intensifying US–Chinese technology rivalry, we make recommendations below on how Europe can mitigate some of the risks of increasing dependence on chips designed in China.

Invest in European chip design through end-customer industries and in technology trends

It is an increasingly severe shortcoming of Europe's semiconductor strategy that, at the time of writing, the Industrial Alliance on Processors and Semiconductor Technologies has still not been launched⁴⁸

⁴⁸ European Commission, "Alliance on Processors and Semiconductor technologies", 2022, accessed 5 December 2022, at <https://digital-strategy.ec.europa.eu/en/policies/alliance-processors-and-semiconductor-technologies>

[eu/en/policies/alliance-processors-and-semiconductor-technologies](https://digital-strategy.ec.europa.eu/en/policies/alliance-processors-and-semiconductor-technologies)



more than 18 months after its envisaged start date.⁴⁹ The alliance and its working groups could provide a suitable forum for European end-customer sectors, such as the automotive, telecommunications, health and manufacturing sectors, to jointly develop technology roadmaps for future chip designs that serve their industries. If Europe wants to strengthen its chip design ecosystem in the long-term, European end-customer industries need to perceive chips as a strategic input and competitive differentiator in their own end-products, in order to justify the necessary investments in in-house chip design units and cooperation with European chip design companies. This is key to European *technological competitiveness* not only in semiconductors, but also in various end-customer industries.

Ensure sustained leverage in other parts on the semiconductor value chain in the long-term

Despite the recent US export controls, China's chip design ecosystem has several systemic advantages compared to Europe's that make it almost certain that European industries will depend more on chips designed in China at the end of this decade than they do today. To strengthen Europe's Open Strategic Autonomy despite growing dependence on China's semiconductor ecosystem, European policymakers must support the preservation and creation of European technology

providers that are indispensable to the global semiconductor value chain. The fact that no fab in the world can move beyond 7nm process technology without access to ASML's Extreme Ultra-Violet lithography machines creates geopolitical leverage. This "strategic indispensability" of domestic semiconductor firms to the international ecosystem is a key pillar of Japan's semiconductor strategy.⁵⁰

European semiconductor manufacturing equipment and chemical suppliers have globally competitive, in some cases market-leading, positions in their fields. One aspect of Europe's semiconductor strategy should therefore be to support the continued indispensability of these technology providers not only against Chinese competitors, but also in relation to firms from the US and its East Asian allies. This policy objective should inform assessments of US export controls, even if these only target China, and their potential impacts on European firms.

Such indispensable and market-leading firms are key to Europe's *technological competitiveness* not just in the semiconductor sector, but in many other end-user industries. Their existence also boosts *supply chain resilience* and *national security* by providing points of leverage that Europe can use to counter weaponized interdependence in the semiconductor supply chain.

⁴⁹ European Commission, "Updating the 2020 New Industrial Strategy: Building a Stronger Single Market for Europe's recovery", SWD(2021) 350 final, 2021, <https://ec.europa.eu/info/sites/default/files/communication-industrial-strategy-update-2020_en.pdf>.

⁵⁰ Hideki Uno, "Japanese Semiconductor Industrial Policymaking in the Twenty-First Century", CSIS, 19 September 2022, <<https://www.csis.org/blogs/perspectives-innovation/japanese-semiconductor-industrial-policymaking-twenty-first-century>>.



Engage in EU-level dialogue with other key actors in the semiconductor value chain

At the same time, cooperation with the US and its East Asian allies is important to the sustainable development of a competitive European semiconductor sector. There is no prospect of Europe ever “onshoring” the entire semiconductor supply chain: *supply chain resilience* must be managed, in so far as is possible, through international cooperation and information exchange. The TSMC-Samsung duopoly on leading edge fabrication is only the most prominent example of why comprehensive onshoring is unrealistic. Europe must build “strategically indispensable” niches in the context of dependence on technology provided by other countries. Within the US allied community, it should be possible to discuss these issues in combined forums where all parties’ interests can be addressed. Dependencies on China cannot be handled in the same way for political reasons, but they are also best managed by maximizing communication with Chinese parties on the basis of reciprocity (i.e. not providing information without receiving equivalent information).

Map and assess the domain-specific risks that stem from the use of Chinese-origin chips

While certain market dependencies on Chinese firms are relatively easily identified, the rapid growth of the global IoT and in Chinese industrial capabilities requires extensive and continuing risk assessments differentiated by sector and vertical. Not all Chinese-designed chips and the products they support present an equal risk profile, although common risk factors stem from the Chinese state’s political priorities and its intrusive data regulatory regime.

Enabling such comprehensive and detailed risk assessments is another reason why cross-sectoral cooperative forums such as the above-mentioned alliance are important. Without deep visibility of the structure of Europe’s digitalized industries and their interdependencies with China – and indeed with other states in the US-allied community – policymakers cannot make informed decisions on risk management for national security, on supporting Europe’s future prosperity or on maximizing Europe’s Open Strategic Autonomy.

Authors:

Jan-Peter Kleinhans is the Head of Technology and Geopolitics at Stiftung Neue Verantwortung e.V. in Berlin, Germany. Contact: jkleinhans@stiftung-nv.de

John Lee is Director of East West Futures in Berlin, Germany. Contact: johnlee@eastwestfutures.com



In political and technological harmony or disharmony? How Europe and China advance towards 6G

Tim Rühlig, Liesbet Van der Perre

Abstract

As the world rolls out 5G technology, advances are also being made in the development of the next generation of wireless networks: 6G. Although in its infancy, 6G already carries the hope of new and strategic use cases that could fulfil promises that 5G has not yet been able to accomplish. Just as with 5G, China and Europe are leading the development of 6G. Without underestimating Europe's own strengths, careful monitoring of Chinese policy and technological developments will be crucial for European policymakers. This chapter identifies which actors should be monitored. China's strength also has implications for European strategic autonomy in terms of supply chain resilience, national security, values protection and technological competitiveness. The EU has increased its supply chain resilience but dependencies remain and national security is still the greatest concern. Differences in values are particularly stark with regard to privacy and sustainability. Although still well positioned, Europe should bolster its technological competitiveness and pay particular attention to patenting.

From global 5G roll-out to 6G definition

While some countries in Europe were still in the phase of granting licences in 2022,⁵¹ the global rollout and adoption of 5G continues at high speed; 5G is scaling faster than any previous mobile generation and the number of 5G subscriptions was expected to reach 1 billion by the end of 2022.⁵² Asian countries such as India, South

Korea and the People's Republic of China (PRC) have all been early adopters.

By late 2022, China had built 1.85 million 5G base stations, ranking it first in absolute numbers but not per capita. The European Union's 5G Observatory puts the number of 5G base stations deployed in the EU at 256,074. Germany has less than

⁵¹ European 5G Observatory, "European 5G scoreboard", accessed 18 December 2022 at <<https://5gobservatory.eu/observatory-overview/eu-scoreboard/#menu-mobile>>.

⁵² Ericsson, "Ericsson Mobility report", November 2022, accessed 2 January 2023, <<https://www.ericsson.com/en/reports-and-papers/mobility-report>>.



52,000 such stations,⁵³ although methods for calculating deployment vary. Europe counts cell sites while Chinese operators report base stations and sometimes count different spectrum bands as separate “logical” base stations even if they partly use the same hardware.⁵⁴ However, even if numbers are adjusted, China has deployed almost twice as many base stations as the EU. It is true that China needs to service far more people – China Mobile alone has more mobile subscribers than there are people living in the US and the EU combined – but the race for technological leadership in the wireless sector is also one of scale.

China’s deployment is not just faster than but different from Europe’s. The PRC is rolling out stand-alone 5G (SA 5G), which frees up capacity in the mid- and low-band spectrum. By contrast, Europe deploys non-stand-alone 5G (NSA 5G), which does not require a new Core Network like SA 5G. While NSA 5G offers largely the same applications for most consumers, SA 5G has interesting potential for a wide range of applications in manufacturing, healthcare and mobility, to name just a few examples. Experts disagree on the practical relevance of the different deployment strategies and on when new

use cases will become a reality. In common with all other states, China is yet to tap the full potential of SA 5G. For the time being, NSA 5G is sufficient and more cost-effective, not least since it supports legacy networks. In private conversations, however, representatives of European 5G vendors are concerned that their de facto exclusion from the Chinese market is cutting them out of the largest market for the most advanced version of 5G. This could provide Chinese manufacturers with the advantage of experimenting with applications that might steer the way to the development of 6G. Instead of prioritizing 6G, the US-EU Trade and Technology Council (TTC) is stalled over the technologically premature Open RAN, which the US is pushing in order to support its industry.⁵⁵

China’s vendors develop and manufacture high quality equipment and profit from party-state support. The PRC government has instructed state-run operators to roll out stand-alone 5G at high speed, provides subsidies and instructs operators to offer low-cost subscriptions to consumers. China’s 14th Five-Year Plan sets China’s ambitious 5G deployment targets, which aim for market penetration of 56%.⁵⁶

⁵³ European 5G Observatory, “International 5G scoreboard”, November 2022, accessed 18 December 2022 at <https://5gobservatory.eu/observatory-overview/international-5g-scoreboard/>.

⁵⁴ Doug Brake and Alexandra Bruer, “The great 5G race: Is China really beating the United States?”, Information Technology and Innovation Foundation, 30 November 2022, <<https://itif.org/publications/2020/11/30/great-5g-race-china-really-beating-united-states/>>.

⁵⁵ Julian Ringhof, “Setting the tone: The value of the EU-US Trade and Technology Council”, European

Council on Foreign Relations, 9 December 2022, <<https://ecfr.eu/article/setting-the-tone-the-value-of-the-eu-us-trade-and-technology-council/>>.

⁵⁶ National Development and Reform Commission, “中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要” [The Fourteenth Five-Year Plan for the National Economic and Social Development of the People’s Republic of China and Outline of Long-term Goals for 2035], *Xinhua*, accessed 18 December 2022 at <http://www.gov.cn/xinwen/2021-03/13/content_5592681.htm>.



Further development of wireless infrastructure continues in parallel. In the coming years, new Third Generation Partnership Project (3GPP) releases of 5G standards are planned (5G-advanced). Global harmonization is ongoing, and the Global 5G Event series is discussing regulation, security, trust and prospects for 5G and beyond, among other issues.

Since new generations of mobile networks typically occur every ten years, many expect 6G in 2030. Prior to standardization in the 3GPP, the world has reached the stage of crucial research and development (R&D) initiatives exploring and developing these new technologies. Europe and China are heavily investing in 6G research and remain in the lead. The PRC 14th Five-Year Plan envisages a mobile infrastructure that integrates space and earth, with enhanced data perception, transmission, storage and computing capabilities as central features.⁵⁷ China's National Informatization Plan makes clarification of requirements for 6G and the development of technologies to support 6G among its main targets.⁵⁸

⁵⁷ National Development and Reform Commission (note 56).

⁵⁸ Central Commission for Cybersecurity and Informatization, “十四五”国家信息化规划 [14th Five-Year Plan for national Informatization] (in Chinese), Chinese State Council, accessed 18 December 2022 at <<http://www.gov.cn/xinwen/2021-12/28/5664873/files/1760823a103e4d75ac681564fe481af4.pdf>>.

⁵⁹ University of Oulu, 6G Flagship, “We are 6G Flagship: Welcome aboard”, accessed 18 December 2022 at <https://www.6gflagship.com/>.

⁶⁰ 6G IA, “6G Smart Networks and Services Industry Association”, accessed 18 December 2022 at <<https://6g-ia.eu/>>

Europe is also taking the initiative. Finland launched a flagship project to envisage and define 6G in 2018.⁵⁹ At the European level, the 6G Smart Networks and Services Industry Association (6G-IA) has been established as the voice of European industry and research on next generation networks and services. Among its more than 200 members are Nokia and Ericsson as well as many academic institutes, semiconductor companies (NXP, Infineon), small and medium-sized enterprises and operators (e.g., Orange, Deutsche Telecom, Telefonica, Telenor). The association is also open to non-European actors such as Samsung, Huawei, ZTE, Vodafone or Interdigital.⁶⁰

Several EU-funded projects, particularly those part of the Horizon 2020 ICT-52 call such as HEXA-X and REINDEER, have generated vision documents on what 6G should be.⁶¹ For the same purpose, China formed the IMT-2030 (6G) Promotion Group in June 2019 led by the China Academy of Information and Communication Technology (CAICT) under the guidance of the Ministry of Industry and Information Technology. The group set out its 6G vision in a White Paper in June 2021.⁶² Individual companies such as Nokia, Ericsson, Huawei

⁶¹ HEXA-X, “Deliverable D1.2: Expanded 6G vision, use cases and societal values”, accessed 18 December 2022 at https://hexa-x.eu/wp-content/uploads/2022/04/Hexa-X_D1.2_Edited.pdf. REINDEER, “Deliverable D1.1: Use case-driven specifications and technical requirements and initial channel model”, accessed 18 December 2022 at <https://reindeer-project.eu/public-deliverables/>.

⁶² IMT-2030 (6G) Promotion Group, “White Paper on 6G Vision and Candidate Technologies”, CAICT, accessed 18 December 2022 at <http://www.caict.ac.cn/english/news/202106/P020210608349616163475.pdf>.



and Samsung are also expected to drive 6G innovation and have published their own vision papers on the new generation of mobile technology.⁶³

Just as in previous generations of mobile technology, the development of 6G remains transnational. Almost all the technology leaders continue to operate R&D centres throughout the world and Huawei's US subsidiary, Futurewei, is a member of the Next G alliance. A partial separation of Western and Chinese innovation efforts is obvious, however, as Futurewei is the only Chinese company in the Next G alliance and two other Western research alliances, HEXA-X and IOWNGF, feature no Chinese companies among their members.

Our quantitative analysis of European and Chinese contributions to two particularly important academic conferences, the IEEE International Conference on Communications (ICC) in Seoul in May 2022 and the IEEE Global Communications Conference (Globecom) in Rio de Janeiro in December 2022, confirms that Europe and China remain in the technology lead. Both were hybrid conferences, which evens out the distorting effects of travel restrictions. Figures 3.1 and 3.2 show that in terms of the technical symposium contributions,

which undergo particularly strict peer review, neither Europe nor China dominate but both hold strong positions.

Analysis of the technical tutorials at the same conferences puts presenters from the EU ahead of the US and China, which were the second and third most important contributors, respectively. Chinese-led tutorials often engage with Artificial Intelligence and machine learning for wireless while EU-based researchers lead in many of the most theoretical contributions. Keynote speakers from Chinese companies were prominent at both conferences, in recognition of the amount of sponsorship they provide to the events.

This is not to ignore, however, that many papers and presentations stem from groups of researchers that cut across nationalities and world regions. Our analysis assigned these to the respective shares of their contributions. Which of these research efforts will translate into contributions on or adopted standards remains to be seen. The findings on these two conferences show that many European and Chinese experts have significant editorial responsibilities in the IEEE community, which publishes journals of that provide the main reference for the communication domain.

⁶³ Nokia, "White papers", accessed 18 December 2022 at <<https://www.bell-labs.com/institute/everything/white-papers/#gref>>; Ericsson, "6G: Connecting a cyber-physical world", accessed 18 December 2022 at <<https://www.ericsson.com/4927de/assets/local/reports-papers/white-papers/6g--connecting-a-cyber-physical-world.pdf>>; Samsung, "Next generation communications", accessed 18 December 2022

at <<https://research.samsung.com/next-generation-communications>>; Huawei, "6G: The next horizon. From connecting people and things to connecting intelligence", accessed 18 December 2022 at <<https://www-file.huawei.com/-/media/corp2020/pdf/tech-insights/1/6g-white-paper-en.pdf?la=en>>.

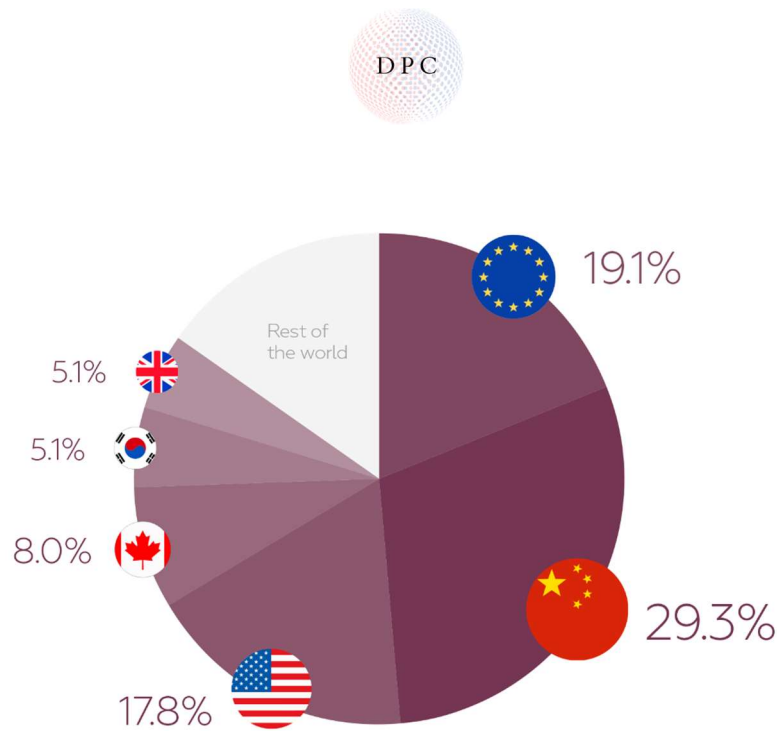


Figure 3.1 – Origin of contributors to Technical Symposiums at the 2022 ICC

What’s new in 6G and does it matter?

Anticipated technological trends as expressed in Chinese and European White Papers and technical documents are strongly aligned. These will require significant upgrades from 5G to 6G to continue the improvements initiated by 5G in mobile data volume, greater reliability and reduced latency, and mass device use; and to support new features, in particular

to provide precise positioning information, sensing,⁶⁴ and Wireless Power Transfer (WPT).

These new requirements increase the need for suitable technology and available spectrum. Among the current trends and proposed solutions are:

⁶⁴ Henk Wymeersch et al., “Integration of communication and sensing in 6G: A joint industrial and academic perspective”, 2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile

Radio Communications (PIMRC), accessed 18 December 2022 at <<https://ieeexplore.ieee.org/document/9569364>>.

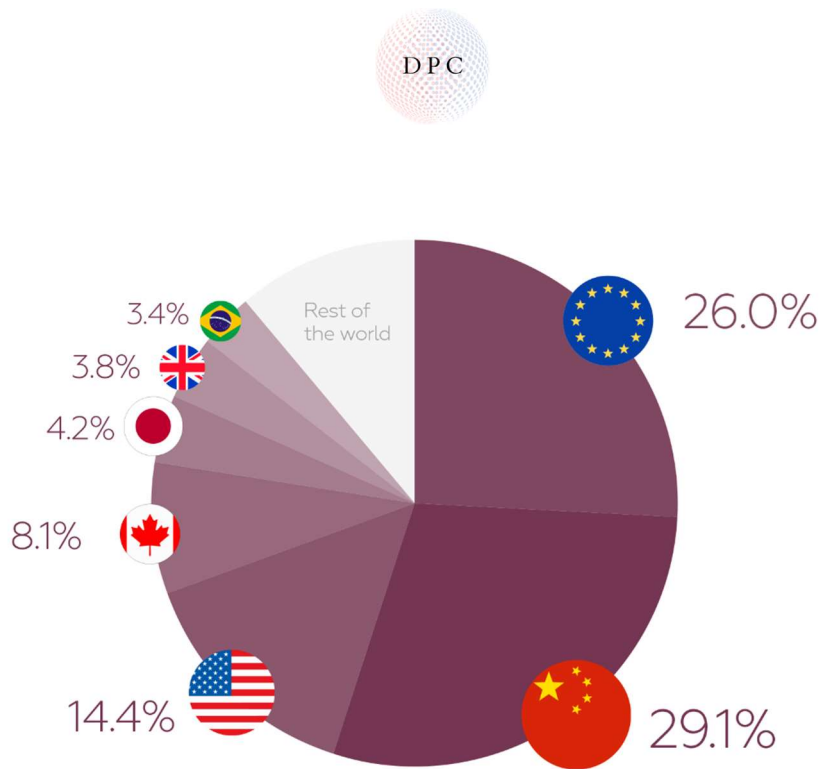


Figure 3.2 – Origins of contributors to Technical Symposiums at the 2022 Globecom, percentage

- An evolution towards “everything in the cloud”, with RAN continuing but technical reasons, such as latency and energy efficiency, as well as other reasons (privacy or security concerns) for movement in the opposite direction. In this context, heterogeneous 6G infrastructure is expected to include distributed smart connectivity/computation platforms and to merge communication, computation, navigation and sensing.
- To provide ubiquitous support for applications and services, it is anticipated that future 6G networks will deploy with “global and deeper coverage”.⁶⁵ To establish global coverage, integration with non-terrestrial network segments is proposed, in particular Low Earth Orbit (LEO) satellite communications.
- Spatial multiplexing is key to increasing capacity and service levels. This can be achieved with massive antenna systems that will be deployed in distributed topologies and could operate in cell-free networks.
- In order to establish very high-capacity areas, exploitation of higher operating frequencies up to sub-THz spectrum is being studied.
- The complexity of 6G systems will require use of AI technology. AI already shows promise in addressing diverse challenges in the networks.

⁶⁵ Shanzhi Chen et al., “Vision, requirements, and technology trend of 6G: How to tackle the challenges of system coverage, capacity, user data-rate and movement

speed,” *IEEE Wireless Communications*, vol. 27, no. 2 (April 2020), pp. 218–228, <doi: 10.1109/MWC.001.1900333>.



Many questions remain, however, such as the testability of AI-enhanced functions.

- ‘Reconfigurable Intelligent Surfaces’ (RIS) are being studied as a new technological component for providing consistent coverage, which is especially challenging at mmwave frequencies and above.

The candidate technologies for 6G mentioned in the IMT-2030 Promotion Group White Paper align with the above list. The paper lists as key innovations the introduction of distributed antennas, AI in the network, merging positioning/sensing and communication, exploitation of higher frequencies and integration of non-terrestrial networks. Non-orthogonal multiple access (NOMA) is mentioned as an approach to multiple access, which is a logical proposal given that so much R&D in this domain is happening in China. However, there is an unexpected section on Orbital Angular Momentum (OAM)-based radio communication, which is contested as a new term for a special case of what is a well-known technology among European researchers. In addition, but of lesser importance, interest in Europe in Visible Light Communications (VLC) has been declining and it is not widely advocated for 6G. R&D on all of the above topics has gained momentum in recent years in all regions of the world, but with China and Europe often taking the lead (see above).

⁶⁶ HEXA-X, “Deliverable D1.2: Expanded 6G vision, use cases and societal values”, accessed 18 December 2022 at <https://hexa-x.eu/wp-content/uploads/2022/04/Hexa-X_D1.2_Edited.pdf>.

It is not just traditional key performance indicators that are being set in the development of 6G. A new type of indicator has been proposed to reflect other key parameters: Key Value Indicators (KVIs). Among the components of KVIs are sustainability, digital inclusiveness and trustworthiness.⁶⁶ The 6G-IA has established a Security Working Group and a Vision and Societal Challenges Working Group, and the latter hosts a dedicated Societal Needs and Value Creation Sub-Group. The latter two have published a white paper, *What societal values will 6G address?*⁶⁷ The jury is still out on whether KVIs will have a major impact, but there are arguments for reasonable doubt.

The importance of the above summary of innovation lies in the enormous potential of new use cases. It is mainly on new functionality that European and Chinese visions diverge. A challenging class is proposed in “mixed reality” applications, and potentially holographic interactions, where the physical and virtual worlds could merge. This requires both worlds to be able to work in the same temporal and spatial reference frames, and hence asks for (quasi) real-time wireless connectivity and precise positioning information. It is in this context that China envisages use of more precise and timely information for the sake of further broadening political control over society and the economy, a trend that is euphemistically referred to as “social governance”.⁶⁸ Applications

⁶⁷ Gustav Wikström et al., “What societal values will 6G address?”, *Zenodo*, 17 May 2022, <<https://doi.org/10.5281/zenodo.6557534>>.

⁶⁸ IMT-2030 (6G) Promotion Group, “White Paper on 6G Vision and Candidate Technologies”, CAICT, accessed



where both sides broadly align include highly “dependable” applications, such as in wireless connectivity-enabled robotized factories, and interaction with

many more and diverse IoT nodes such as energy-neutral devices that enable an envisaged ‘internet-of-tags’.

Actors to watch

A multitude of technical and political actors are driving China’s 6G development. Broadly speaking, the members of the IMT 2030 6G Promotion Group are the most

decisive actors that Europe needs to watch when seeking to understand technological and policy developments in the PRC. Figure 3.3 provides an overview.

Implications for strategic autonomy

1. *Global supply chain resilience and second- and third-order effects*

Following various attempts in different parts of the world to define distinct ICT technical standards, a broad consensus has emerged that there is no viable alternative to a single global wireless standard. While 6G standardization has not yet begun, it is anything but a bold prediction that Chinese and European entities will account for the vast majority of adopted contributions. Given the high degree of standardized technology in the wireless sector and the importance of patented standard contributions, it is no secret that the share of successful contributions will also be decisive in the influence and revenue that European, Chinese, US and other entities will accrue. The state of research contributions points to a leading position for European and Chinese entities (see the quantitative analysis above) but it is too early to determine the exact share of

Chinese and European contributions to the 6G standard or whether Chinese influence will increase as much as it did from 4G to 5G. It is unlikely, however, that either Europe or China will be marginalized.

During its development, and in the expected 6G supply chain, a high degree of a transnational division of labour is likely. No region is in control of all the production steps and supplier markets: both Europe and China face challenges. A prime example is that of semiconductors. If comprehensively enforced, the October 2022 US export controls will prevent Chinese chip manufacturers from producing $\leq 14\text{nm}$ logic, $\leq 18\text{nm}$ half-pitch DRAM and $> 128\text{L}$ NAND chips. This would also mean that no person with US resident permit could service equipment on Chinese chip manufacturer SMIC’s 7nm/ 14nm nodes and no US equipment vendor could sell machines for SMIC’s $\leq 14\text{nm}$ process nodes, which

18 December 2022 at <http://www.caict.ac.cn/english/news/202106/P020210608349616163475.pdf>.














ACTOR TYPE	NAME OF KEY ACTOR	DESCRIPTION	KEY TASK	PRIORITY
Research institution/policy institution	 China Academy of Information and Communications Technology (CAICT) (中国信息通信研究院)	Research institution that is an integral part of the Ministry of Industry and Information Technology (MIIT)	Heading the IMT 2030 (6G) Coordination Group; bridging policy and technical layers	●
Research institution	 Purple Mountain Laboratories (紫金山实验室)	State-backed research institute	Famous for a successful trial of a 6G chip at an unprecedented transmission speed of 206.25 gigabits in early 2022	◐
Company	 Huawei & Huawei Cloud (华为云)	Private company with close ties to the party-state	Lead developer and manufacturer of wireless infrastructure equipment, large cloud provider	●
Company	 Alibaba Cloud (阿里云)	Private company	China's leading cloud provider	◐
Company	 ZTE (中兴通讯股份有限公司)	State-owned enterprise under the guidance of the State-owned Assets Supervision and Administration Commission of the State Council (SASAC)	One of China's leading developers and manufacturers of wireless infrastructure equipment	◐
Company	 Tencent Cloud (腾讯云)	Private company	One of China's leading cloud providers	◐
Policy institution	 Central Cyberspace Affairs Commission (中央网络安全和信息化委员会)	Body under the Central Committee of the Chinese Communist Party	Main task: supra-ministerial policy coordination	●
Policy institution/standards body	 China Electronics Standardization Institute (CESI) (中国电子技术标准化研究院)	non-profit organization under the guidance of MIIT	Steering of standardization work, secretariat of TC 260, China's National information security standardization technical committee	◐
Policy institution	 Ministry of Industry and Information Technology (MIIT) (中华人民共和国工业和信息化部)	Ministry of the State Council	Political steering of 6G development	●
Policy institution	 Ministry of Science and Technology (MOST) (中华人民共和国科学技术部)	Ministry of the State Council	Responsibility for state-funding under the Broadband Communications and New Type of Networks Special project	◐
Policy institution	 Department of High-technology and the State Information Center of the National Development and Reform Commission (NDRC) (中华人民共和国国家发展和改革委员会)	Departments of the State Council's macro-economic planning institution	State planning of 6G development under the 14th Five-Year Plan	◐

Figure 3.3 – An overview of the technical and political actors driving China's 6G development



would severely limit China's ability to do anything remotely leading-edge in chips. All this calls into question China's ability to develop and later produce cutting-edge 6G technology. 6G is likely to integrate a number of cutting-edge technologies, including AI, that require highly specialized chips, which China may not have access to in future. Three dimensions need to be considered:

First, the recent past suggests that waivers of US export controls are not a rare exception. Whether the most recent export controls will be comprehensively enforced remains to be seen. If the United States gets serious, it has all the means necessary to comprehensively enforce the measures. TSMC and Samsung Foundry's customers are mostly US fabless companies, but they are crucial for China too. Neither firm will risk its revenues to accommodate the limited business it has with Chinese fabless companies.

Second, China's indigenous chip industry has developed in the recent past. Some experts believe that China's SMIC can *process* 7nm chips even without EUV (i.e. lithography machinery that is necessary for the fabrication of cutting edge chips), but it will not be able to *competitively produce* 7nm chips without EUV, and thus its products might not be as reliable as those of TSMC, which European 6G vendors will be able to use. However, competitive disadvantages could, at least to some degree, be financially compensated for by the Chinese state. The US October 2022 export controls also cut China's access to critical deposition equipment.

Third, many mobile chips do not need the latest semiconductor technology. Several chips, such as mobile chipset or base station ASICs, probably do not fall under the new US export restrictions. If comprehensively implemented, however, developing very high frequency 6G technology in China might be most affected. The mmwave bands are not yet the most commonly used in 5G, but R&D on 6G is considering low THz, and these higher frequencies will probably be used in some 6G applications. This will most likely be for use cases that draw on 'fixed Wireless Access', so smartphone applications would be less likely to be affected, unless precise localization and sensing functionalities require the high frequencies. Huawei's production of 5G equipment provides some indication that the industry is not currently experiencing the anticipated demand, since production of high-frequency equipment fell significantly in 2021–2022.

Generally speaking, it appears that the new export controls follow a logic whereby Chinese chip design companies in wireless technology will not be fully cut off from Western supply, but China is constrained and remains dependent on foreign manufacturing, providing leverage to the US and its allies.

However, dependencies are mutual. Western companies rely on raw materials supplied by the PRC. Reports indicate that China controls around 85% of the global rare earth processing capacity and 60%



of global mined production.⁶⁹ While the country possesses only one-third of the world's rare earth reserves, it could take up to a decade to untap reserves in other parts of the world. For 6G, Europe will continue to rely on raw material supply from China.

China will also remain a site for wireless infrastructure R&D and manufacturing, as well as software development. European supply chain dependency is comparatively low and has decreased in recent years. European vendors have reduced their exposure to sourcing from the PRC. For example, Ericsson has growing manufacturing locations in Estonia, Brazil, India and Mexico, has opened new facilities in the United States and Poland, and has additional contractual capacities in Malaysia. At the time of writing, manufacturing capacities in Poland and Estonia have reached a state where all base station manufacturing for Europe can be carried out in Europe. Nonetheless, that some components rely on Chinese supply chains cannot be circumvented. Ericsson does not directly source components from companies headquartered in the PRC. Application-specific integrated circuits are designed by Ericsson and production is contracted to Ireland. The company's production in China is for the Chinese market or for third markets that do not have an issue with sourcing from the PRC. Ironically, China is well positioned in the Open RAN ecosystem, which is often falsely considered a concept that could reduce dependency on Chinese vendors,

while single vendors are drastically reducing their reliance on sourcing from the PRC. While Ericsson maintains its research in China, 60% of its development is in Europe.

Despite best efforts, some limited dependencies remain. Some devices, such as filters required for a wide array of products, are exclusively manufactured in the PRC, although enlarging what is kept in stock helps mitigate supply chain vulnerabilities. More importantly, however, a significant proportion of software development takes place in the PRC. To mitigate cybersecurity risks, all product management and control, including source code review, is carried out predominantly in Europe. If China were to cut software supply, improvements in functionality would be delayed. Ericsson is not expanding its software development in China but instead increasingly building up capacity in other countries. For example, Ericsson's CloudRAN, which is essential to Open RAN, is being developed in Canada.

Mitigation of supply chain risks is more difficult for smaller vendors. One example is the use of Open Source software. A recent study has identified that China has a growing percentage of Open Source software, which is also frequently used in wireless infrastructure equipment. This requires European vendors to carefully review their due diligence because of the widespread assumption that the "many eyes principles" does not create sufficient security in Open Source code. In fact, only

⁶⁹ Xianbin Yao, "China is moving rapidly up the rare earth value chain", *Brink*, 7 August 2022, <[https://](https://www.brinknews.com/china-is-moving-rapidly-up-the-rare-earth-value-chain/)

www.brinknews.com/china-is-moving-rapidly-up-the-rare-earth-value-chain/>.



a very small proportion of Open Source work is on security.⁷⁰ Small European vendors in particular cannot afford the necessary source code review.

2. National security/criticality

The discussion on whether the inclusion of Huawei equipment poses a security risk to Europe has exposed that a minimum level of vendor and supplier trustworthiness is essential. A recent DPC study demonstrates that trust remains a serious challenge in Open RAN solutions. This is particularly crucial with the software pillar of the O-RAN Alliance.⁷¹ Even beyond software-defined components, sourcing from China carries risks. One example is Europe's increasing dependence on Chinese back-end manufacturing (the last step of semiconductor manufacturing), which could be utilized to compromise a chip and implement hardware backdoors or kill switches.⁷²

Trust is becoming an increasingly important and even crucial characteristic in many of the envisaged 6G applications, which rely on wireless connectivity for their correct and safe operation. The risks are most

obvious when software-defined components are sourced from China, since these require a comprehensive source code review. More pertinently, if continuous updating of the source code is needed, a comprehensive review of source code is unrealistic which makes trustworthiness essential. Autonomous vehicles present a clear case, but mobile e-health applications, for example, will also require great care. How 6G security will differ from 5G networks, and whether dedicated features such as PHY-layer security will be implemented, remains to be seen. A particular question is whether providing joint communication and positioning can be achieved while preserving the privacy of users.

In addition to the lack of trustworthiness of Chinese vendors, which continues to be an issue, the development of 6G also needs to consider potential military use cases. Chinese-language sources provide proof that the People's Liberation Army (PLA) is considering 6G's potential for its own capabilities, ranging from the rapid and reliable transmission of information to competition in outer space and modelling the predictability of threats.⁷³

⁷⁰ Rebecca Arcesati and Caroline Meinhardt, "China's open-source tech development: Insights into a growing ecosystem", MERICS, May 2021, <https://merics.org/sites/default/files/2021-05/MERICS%20Primer%20Open%20Source%202021_0.pdf>.

⁷¹ Jan-Peter Kleinhans and Tim Rühlig, *The False Promise of Open RAN: Why Open RAN Does not Solve the "5G China Challenge"*, Berlin, Digital Power China, August 2022, <https://timruhlig.eu/ctf/assets/x93kiko5rt7l/2VmWvuXxKdqdTuwkLSWUSQ/b48a2ffe9e42dc3a3b09d4c35b1c802e/DPC-Open_RAN_-_FULL_REPORT_-_FINAL.pdf>.

⁷² Jan-Peter Kleinhans and John Lee, "Europe's dependence on Chinese semiconductor manufacturing", in Tim Rühlig (ed.), *China's Digital Power*:

Assessing the Implications for the EU, Berlin, Digital Power China, January 2022, pp. 21–32, accessed 18 December 2022 at <https://timruhlig.eu/ctf/assets/x93kiko5rt7l/4uiZoNQtrkni5KfuNdrBbx/fd52e3320cfe21e6b304ad31d81279d8/DPC-full_report-FINAL.pdf>.

⁷³ PLA Daily, "智能化带来战争新变化" [Intelligence Brings New Changes to Warfare], *Military People*, accessed 18 December 2022 at <http://military.people.com.cn/n1/2021/0107/c1011-31992241.html>; Tang Weizhong, "智能化战争时代的军事高等教育" [Military Higher Education in the Age of Intelligent Warfare], Chinese Ministry of Defense, accessed 18 December 2022 at http://www.mod.gov.cn/education/2021-05/13/content_4885203.htm>; Ruikun Xie



3. Values and sustainability

As noted above, different approaches to privacy might become more crucial with the transition from 5G to 6G. It is almost certain that 6G infrastructure will provide more information on its users and a higher degree of precision of personal data, such as a user's location. Such information will be collected not only by applications, but also at the infrastructure layer. A combination of higher bandwidth and more distributed antennas will enable greater accuracy and reliability of information on the location of users and devices. An evolution towards sub-THz is advocated as a technological means for providing better sensing and positioning capabilities.

Another value difference between Europe and China could arise from the different levels of importance attributed to sustainability. This value can be considered two sides of the same coin: sustainable 6G and 6G for sustainability. On sustainable 6G, an obvious priority is to increase transmission energy efficiency to support continuous growth in mobile data volumes, where the ambition should be to improve by several orders of magnitude. Ecological concerns are broader, however, and total lifecycle assessments are required that consider both energy and materials use, including of toxic and rare earth materials. Individual research groups and organizations in Europe have recently published useful studies.⁷⁴ EU representatives also stress the importance of

focusing on sustainability. Nonetheless, in debates at the 2022 Joint European Conference on Networks and Communications & 6G Summit, among others, some companies expressed the opinion that industry could continue to operate as it did in previous mobile network generations, where new functionalities were developed first and significant energy reduction was achieved during optimization afterwards. This perspective is commonly shared by Chinese and US actors, as current practice and plans indicate. For example, the IMT 2030 White Paper mentions that 6G should address sustainability challenges, but the anticipated timetable for achieving "carbon neutrality" is decades later than the ambition expressed by Europe. However, to the extent that energy efficiency becomes a competitive advantage, sustainability goals might be more broadly adopted as a side-effect of market demand. For the time being, however, extrapolating from 5G, it is not far-fetched to conclude that 6G standard proposals put forward by Chinese actors will pay less attention to sustainability and the UN Sustainable Development Goals.

4. Technological competitiveness

Europe and China are technological front-runners in 5G and best placed to capture the same spot in 6G. In comparison with other foundational technologies, Europe is relatively well placed and needs to defend its position. Europe is strategically investing in 6G, but quantitative studies

et al., "如果 6G 运用于未来作战" [When 6G is used in future operations], *81.cn*, accessed 18 December 2022 at <http://www.81.cn/gfbmap/content/2020-04/14/content_258839.htm>.

⁷⁴ Nicolas Moreau et al., "Could unsustainable electronics support sustainability?", *Sustainability*, vol. 13, no. 12 (June 2021), pp. 6541–6547, <<https://doi.org/10.3390/su13126541>>.



highlight significant improvements in China. For example, Huawei's R&D investment in 2021 was equivalent to 15% of its revenue at an impressive US\$ 22 billion. In comparison, Ericsson invested US\$ 4.9 billion in the same year.

A widely reported investigation of 6G patents by Nikkei Asia and the Cyber Creative Institute also found Chinese entities in the lead: 40.3% of 6G patents had been filed by Chinese entities, followed by a 35.5% share by the US with Japan at 9.9% and Europe at 8.9%.⁷⁵ In the spring of 2021, China's National Intellectual Property Administration came to a similar conclusion, putting the Chinese share of patents ahead of all other countries at around 35%.⁷⁶

However, these calculations underestimate Europe's position in 6G innovation. The widespread comparison of Huawei and Ericsson R&D investment neglects the fact that Huawei's R&D covers wireless infrastructure, devices and fixed networks. Ericsson R&D, by contrast, is only on infrastructure equipment development. In addition, the number of patents provides no information on quality or whether they

will turn out to be standard essential for 6G, even if declared as such.⁷⁷ In a comparison of the quality of Qualcomm, Intel and Huawei patents, the Cyber Creative Institute put the Chinese tech giant last, indicating that almost twice as many 6G patents by Qualcomm could be considered "high quality" compared to Huawei's.⁷⁸ Only a comprehensive analysis of forward references of standard-essential patents can provide a good estimate of the value of contributions once in the advanced stage of 6G standardization. To complicate the issue further, the value of patents is currently contested since China has issued an anti-suit injunction forbidding foreign companies from taking patent disputes to courts outside the PRC. This questions whether patent rights can ever be effectively enforced. The European Commission has taken the issue to WTO dispute settlement and consultations are under way.

In short, while it remains to be seen how Europe scores relative to China it is unlikely that either side has lost technological competitiveness in the wireless sector.

⁷⁵ Naoki Watanabe, "China accounts for 40% of 6G patent applications: survey", *Nikkei Asia*, accessed 18 December 2022 at <https://asia.nikkei.com/Business/Telecommunication/China-accounts-for-40-of-6G-patent-applications-survey>.

⁷⁶ CNIPA, "6G通信技术专利发展状况报告发布：中国申请已居首位" [6G communication technology patent development status report released: China's application has ranked first], CCID, accessed 18 December

2022 at <<http://www.ccidcom.com/yunying/20210426/YCs9TCDAbBTMCVYRQ18ajwvI913nw.html>>.

⁷⁷ John Donovan, "NSTAC letter to the President on standards", CISA, 24 May 2022, <https://www.cisa.gov/sites/default/files/publications/NSTAC%20Letter%20to%20the%20President%20on%20Standards%20%285-24-22%29_508.pdf>.

⁷⁸ Naoki Watanabe (note 75).







DIMENSION OF STRATEGIC AUTONOMY	SHORT DESCRIPTION OF CHALLENGE IN KEYWORDS	RELATIVE IMPORTANCE OF CHALLENGE ON A SCALE OF 1 TO 4	POLICY INSTRUMENTS FOR TACKLING CHALLENGE IN KEYWORDS
 Resilience of supply chains	<ul style="list-style-type: none"> Continued sourcing from China 	2	<ul style="list-style-type: none"> Invest in dependency analysis, issue transparency requirements where necessary - base instruments on this analysis Incentivize diversification (e.g. by means of procurement)
 National security	<ul style="list-style-type: none"> Lack of trustworthiness of Chinese suppliers and their technology PLA plans for 6G military use cases 	4	<ul style="list-style-type: none"> Implementation of updated 5G Cybersecurity Toolbox Balanced approach to encryption and limitation of network sharing with building redundancies Track PLA ambitions and share information with like-minded partners
 Values and sustainability	<ul style="list-style-type: none"> Growing importance of privacy concerns for 6G infrastructure Different importance attributed to sustainability 	2	<ul style="list-style-type: none"> Early regulatory signalling Close academic-regulator cooperation on implementation Transparency requirements on ecological footprint of equipment deployed in Europe
 Technological competitiveness	<ul style="list-style-type: none"> Revenue from patents at risk Competitive race over tech leadership with China 	3	<ul style="list-style-type: none"> Prioritize WTO case against China's anti-suit injunction Promote research on European engagement and remove clauses favouring non-European researchers

Figure 3.4 – Main Chinese 6G technology-related risks

Conclusions and policy implications

Europe has a relatively high degree of strategic autonomy in the wireless sector. The EU is not independent of China in terms of either innovation or production, but the PRC is also significantly reliant on capabilities from the West. This is even more the case since the surprise introduction of US semiconductor controls in October 2022.

EU supply chain resilience is fairly positive. European vendors continue to source from China and to rely on critical minerals, but the exposure of large vendors has

declined drastically. To address the remaining challenges, not least those facing smaller vendors, Europe should invest in intelligence to provide a proper understanding of critical dependencies, such as second- and third-order effects. Where necessary, transparency requirements on the origin of materials and primary production of equipment deployed in Europe should be considered, but bureaucratic overburdening should be avoided. Targeted instruments should be developed based on such analysis, not least



in the context of the EU Critical Raw Materials Act, an issue that is beyond the scope of this chapter. Where diversification remains an issue, EU member states can incentivize diversification by means of procurement in cooperation with publicly owned operators.

Chinese actors will remain part of Europe's 6G ecosystem: decoupling is not an option. This makes the lack of Chinese actors' trustworthiness an issue of *national security*. Comprehensive implementation of the EU's 5G security toolbox is a precondition for mitigating network security risks. In the light of the additional information likely to be collected by 6G infrastructure, and its growing complexity, the EU toolbox will require an update.

Encryption remains the most effective way to prevent espionage while sabotage of wireless infrastructure can be made more costly for malign actors through use of network diversity and redundancy. However, strengthening encryption is claimed to hinder European law enforcement and network redundancies are costly. This means striking a balance to serve contradictory policy purposes. Network sharing is an effective tool to increase coverage in European countries, but should be limited given its inherent vulnerabilities to sabotage. Network diversity can be difficult in highly concentrated segments of the wireless infrastructure market. Open RAN is no solution given that it comes with new security risks.⁷⁹

In addition to network security, the EU and its member states should pay close attention to the PLA's exploration of military use cases. Tracking and information sharing with like-minded partners will be essential.

In terms of *values differences*, privacy and sustainability are European policy priorities. Given that European vendors produce for global markets, strong European performance in standardization will not be sufficient. The EU should therefore engage in early regulatory signalling in international standardization efforts, and publish benchmarks that set high privacy norms and requirements. This could serve as a strong incentive to develop methods that comply with European regulatory demands. A significant increase in academic engagement in standard-setting is unrealistic but EU regulators could closely cooperate with European academia on regulatory implementation.

China's participation in standardization is not problematic. Standardization is distinct from deployment or adoption of Chinese use cases. Europe must insist, however, that standardization requires adherence to WTO/TBT principles in order to protect the transparency and openness of technical standard-setting.

As a first step to achieving sustainability goals, the EU could issue transparency requirements on the ecological footprint of all equipment deployed in Europe. Such requirements need to be crafted carefully in order to avoid bureaucratic overburdening.

⁷⁹ Jan-Peter Kleinhans and Tim Rühlig (note 71).



Finally, Europe and China will remain *technologically competitive*. However, China's anti-suit injunction poses serious challenges to the monetization of European innovation. Since mobile network technology will soon penetrate a broad range of products and sectors, patent licensing will take on a significant distributary function that shapes competitiveness. The EU must prioritize the WTO case against China.

To strengthen European academic competitiveness, the EU should not cut ties with China. The PRC contributes significant innovation. However, the EU can

incentivize European engagement and remove clauses in its funding schemes that effectively favour non-European researchers. For example, the Marie Skłodowska-Curie Doctoral Networks require candidates not to have worked or studied for more than 12 months in the previous 36 months in the country of the recruiting institution. Despite its well-intentioned fostering of mobility, this excludes European citizens who want to stay in their country of residence. This has led to non-Europeans benefiting disproportionately from this particular EU funding instrument.

Authors:

Tim Rühlig is a Senior Research Fellow at the German Council on Foreign Relations and an Associate Research Fellow of the Swedish Institute of International Affairs' Europe program. He is based in Germany. Contact: ruehlig@dgap.org

Liesbet van der Perre is a Professor in the DRAMCO lab of the Electrical Engineering Department of the KU Leuven in Belgium. Contact: liesbet.vanderperre@kuleuven.be





Crypto Without the Currency: China's Blockchain Strategy

Cyrille Artho, Rogier Creemers

Abstract

Blockchain is considered a promising emerging technology of strategic importance in both Europe and China. The Chinese government is forging ahead with support for research and technological development, as well as the rollout of blockchain-based initiatives such as the Blockchain Service Network (BSN). Missing from its approach, however, is use of blockchain to underpin cryptocurrency. What will the impact of these ambitions be on European strategic interests? This chapter reviews the technical status quo for blockchain, compares Chinese and European visions and policy frameworks, and provides an overview of the different ways in which blockchain will affect elements of European strategic autonomy — from supply chain resilience to national security, values and sustainability, and technological competitiveness. It concludes with recommendations for European policymakers on responding to the Chinese blockchain challenge.

In recent years, blockchain has emerged as one of the core cutting-edge technologies in which China is seeking global leadership. Policy documents on the 14th five-year planning cycle call for greater research on components such as encryption, consensus mechanisms and smart contracts, on the introduction of secure

technology platforms and open-source communities for blockchain services and on technical standards and regulatory norms, as well as the launch of trials and demonstrations in areas ranging from fintech and supply chain services to governmental operations and regulatory oversight.⁸⁰ Blockchain infrastructure and

⁸⁰ Central Commission for Cybersecurity and Informatization, ““十四五”国家信息化规划” [Translation: 14th Five-year Plan for National Informatization, Dec. 2021], DigiChina, accessed 28 November 2022, at <<https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/>>; National Development and Reform Commission, ““十四五”推进国家政务信息化规划” [“14th Five-Year Plan to Advance the Informatization

of National Government Affairs], *Gov. cn*, accessed 28 November 2022, at <http://www.gov.cn/zhengce/zhengceku/2022-01/06/content_5666746.htm>; State Council, ““十四五”数字经济发展规划” [“14th Five-Year Plan” for the Development of the Digital Economy], *Gov. cn*, accessed 28 November 2022, at <http://www.gov.cn/xinwen/2022-01/12/content_5667840.htm>.



related data centres are now priorities, as Beijing believes that the technology enables new forms of applications and services that will reduce transaction costs, enhance economic productivity and efficiency, and provide more effective forms of verification and trust-building. This is not confined to high value-added applications; it is also considered crucial for rural development,⁸¹ and for reforming evidence handling and case management in the judiciary.⁸²

Firmly excluded from this development agenda, however, is the application for which blockchain is best known in the West: cryptocurrencies. Their use in transactions by banks was prohibited in 2015 and by the end of 2021, crypto-mining and use had also been completely outlawed. China's official digital currency, the e-CNY, does not use blockchain technology. Instead, Beijing's flagship initiative is the Blockchain Service Network (BSN), which was launched in 2020.⁸³ The aim is to build up a global infrastructure for the cloud-based operation of a wide spectrum of blockchain applications, which are discussed at greater length below. The future roadmap for the BSN indicates an intention to develop payment networks and expand in more locations, both within China and internationally. Thus, the ambitions for the BSN are connected with China's broader international agenda,

most notably around the Belt and Road Initiative (BRI).

These trends raise many questions. In China, will it be possible or realistic to achieve the ambitious goals Beijing has set? Will the impact of blockchain adoption on economic or government activities be transformational or merely evolutionary? From an international perspective, what will the impact of the internationalization of the BSN or other blockchain technologies be on policy perspectives and decisions in other countries? How will it affect the values, interests, and concerns of other governments? What might the responses be by those governments?

At the same time, it is necessary to take account of the technical aspects of blockchain technology, which still impose multiple constraints and present challenges that bely the often overly enthusiastic treatment the subject receives in popular media or policy circles. This chapter first reviews the technical state of the art in blockchain services and the state of play in the Chinese and European blockchain landscape, paying particular attention to nascent pilot projects of blockchain applications. Second, it assesses the impact of Chinese blockchain developments on the European Union's goal of Open Strategic Autonomy, focusing primarily on the integrity of global value chains, EU values,

⁸¹ Xiaowei Wang, *Blockchain Chicken Farm: And Other Stories of Tech in China's Countryside*, New York: FSG Originals, 2020.

⁸² Supreme People's Court, "最高人民法院关于加强区块链司法应用的意见" [SPC Opinions concerning Strengthening the Judicial Application of Blockchain], Gov.cn, accessed 28 November 2022, at

<<https://www.court.gov.cn/zixun-xiangqing-360281.html>>.

⁸³ Mikk Raud, "Knowledge Base: Blockchain-based Service Network (BSN, 区块链服务网络)", DigiChina, accessed 28 November 2022, at <<https://digichina.stanford.edu/work/knowledge-base-blockchain-based-service-network-bsn-区块链服务网络/>>.



national security interests and European technological competitiveness — in both home markets and third countries. Finally, it discusses the possible policy means at

the disposal of the EU and member state governance in order to respond to the challenges presented by developments in Chinese blockchain.

What is blockchain and how is it developing?

A *blockchain* is a distributed ledger that records data (transactions) in a way that ensures that historical data is immutable, so it cannot be changed retroactively. Because a cryptographic function is used to sign each block of data, a checksum only matches if the data has not been modified. Blocks are chained by including the checksum of the previous block in the next block. A blockchain as trustworthy distributed storage can therefore take on the role of a central database. Instead of storing data directly, users execute a consensus protocol so that updates are trusted by a majority, and the chaining of checksums ensures that data is tamper-proof.

Blockchains were originally used to implement electronic currencies but they are far more versatile than that. Instead of representing currency, data on the blockchain can store tokens that encode ownership of assets and reference off-chain data such as important documents or images, or be used to track inventory or business transactions. Operations on the data on the blockchain are usually implemented by *smart contracts*, which are small pieces of software that are executed on the blockchain, creating transactions that update the shared ledgers as they execute. These smart contracts are still a relatively immature technology: they are difficult to design correctly and once deployed, they

cannot be altered. In addition, programming mistakes can result in vulnerabilities that could be exploited by an unscrupulous attacker. Such attacks have in the past resulted in damage to the value of up to €300 million.

Nonetheless, the ability to fully automate and reliably store business transactions has vast potential that could not only make business operations more automatic, but also prevent fraud or other types of illegal or undesirable behaviour, such as smuggling, forgery or prescription drug abuse. This is particularly attractive in cases where different parties might not trust a central authority. Many business sectors could benefit from increased transparency and oversight by having their transactions on a blockchain. In cases of global commerce, blockchains have the potential to harmonize international transactions, and to take care of software rules and regulations in a fully automated way.

Blockchains currently have some limited commercial use in domain-specific cases such as tracking the provenance of luxury goods or gambling, albeit on a much smaller scale than online gambling using traditional technology. However, a globally used blockchain to manage real-world transactions in more diverse use cases would require agreement on a common



standard. For smart contracts, large-scale adoption is even further away and the benefits over traditional cloud software are not yet clear enough to warrant the inherent risks that come with immature technology. As the software platforms and tools for smart contracts are still evolving, it is too early to create a global standard.

Thus, the potential for global adoption of blockchain technology is restricted not only by a lack of technical maturity, but also by a lack of trust between China and the West. These issues limit the potential of blockchain technology to increase transparency and cooperation.

Visions and approaches to blockchain in China and Europe

China

In recent years, the Chinese government has come to see blockchain technology as an enabler of many of the innovative applications in its plans for economic development and modernization of the party-state system.⁸⁴ The 14th Five-Year Plan for National Informatization, published in late 2021, devotes a dedicated paragraph to blockchain with the intention of expanding its use in fintech, supply chain services, governmental services, and commercial science and technology. Related

development plans for the digital economy further encourage the exploration of blockchain-based data use authorization and tracing functionalities, and their inclusion in BRI projects. Blockchain has appeared in policy initiatives on non-fungible tokens,⁸⁵ the traceability of food and drug production,⁸⁶ the metaverse industry,⁸⁷ the criminal justice system,⁸⁸ and digital philanthropy.⁸⁹ Since 2019, blockchain has been regulated by the Cyberspace Administration of China (CAC),⁹⁰ and blockchain projects hosted in China must obtain a licence from the CAC. The

⁸⁴ Gary Sigley and Warwick Powell, "Governing the Digital Economy: An Exploration of Blockchains with Chinese Characteristics", *Journal of Contemporary Asia*, 2022, <doi: 10.1080/00472336.2022.2093774>.

⁸⁵ Wen Ning, "蚂蚁、腾讯、百度、京东等联合倡议数字藏品行业自律发展", *CN Stock*, accessed 28 November 2022, at <https://news.cnstock.com/news/bwx-202206-4911519.htm?mc_cid=4598a391bf&mc_eid=ad7c94e0d8>.

⁸⁶ Ministry of Industry and Information Technology et al., "数字化助力消费品工业"三品"行动方案 (2022—2025年)" [Action Plan for the "Three Products" in the Data-assisted Consumer Product Industry], accessed 28 November 2022, at <https://www.miit.gov.cn/zwgk/zcjd/art/2022/art_7901fe97b0ce43ffabb3bc461c802522.html?mc_cid=7e12bd13fa&mc_eid=ad7c94e0d8>.

⁸⁷ Shanghai Municipal Government, "上海市培育"元宇宙"新赛道行动方案 (2022-2025年)" [Shanghai Municipality Action Plan to Foster New Tracks for the

"Metaverse"], accessed 28 November 2022, at <https://www.shanghai.gov.cn/202214zcjd/20220720/a6a89e36eee64974a9c64998e13bdaae.html?share_token=9e33f7c9-931f-4ac7-b0b8-7024b9d2fafa>.

⁸⁸ Supreme People's Court (note 82).

⁸⁹ People's Daily, "中央网信办：推动"互联网+公益慈善"向民生服务等新场景拓展" [CAC: Promote the Expansion of "Internet + Public Interest Philanthropy" towards People's Livelihood Services and Other New Venues], *People's Daily*, accessed 28 November 2022, at <http://finance.people.com.cn/n1/2022/0829/c1004-32514151.html?mc_cid=cf9eae169&mc_eid=ad7c94e0d8>.

⁹⁰ Cyberspace Administration of China, 区块链信息服务管理规定 [Blockchain information Service Management Regulations], accessed 28 November 2022, at <<https://digichina.stanford.edu/work/translation-blockchain-information-service-management-regulations-2019/>>.



ninth and most recent batch of licences were issued in July 2022,⁹¹ bringing the number of registered projects nationwide to 2159. China is also a global leader in academic research. China-based researchers publish the most blockchain papers worldwide,⁹² and the Ministry of Industry and Information Technology (MIIT) claims that China accounts for 84% of global blockchain-related patent applications.⁹³ Researchers such as Hong Kong-based Xiapu Luo and institutions such as Zhejiang University, Wuhan University and Peking University regularly figure in the top conferences and best journals in the field (see below), while businesses such as Huawei and Ant Group collaborate with academic institutions on smart contracts and other practical applications. High-profile research on these topics is currently still at the academic level. Because the field is still immature, conferences and journals do not yet have tracks for industrial contributions, as is usual in other, more established fields of research. Moreover, industrial research is usually not published at globally leading conferences or in journals unless it has been carried out together with universities. Developments since 2017 have shown a steady rise in publications. There were more than 100 top-tier publications in 2022, of which China had at least a 30%

share, making it the biggest contributor in the field.

Perhaps China's most ambitious real-world initiative is the Blockchain Service Network, which is defined on its own website as a "cross-cloud, cross-portal, and cross-framework global public infrastructure network used to deploy and operate all types of blockchain distributed applications".⁹⁴ It was launched in April 2020 and is operated by a consortium of state and private sector actors. The lead institution is the State Information Centre, which comes under the authority of the National Development and Reform Commission. Collaborating partners include telecommunications operator China Mobile and payment provider China UnionPay. BSN's technical architect is Red Date Technology, a Hong Kong-based start-up. It functions on the basis of a domestically developed open-source platform called FISCO BCOS, built with the support of partners such as Beyondsoft, Digital China, Forms Syntron, Huawei, Shenzhen Securities Communications, Tencent, WeBank, YIBI Technology and Yuexiu Financial Holdings. This is a permissioned blockchain, where operational parameters are set by the application owners, from which potential users must obtain approval before they are able

⁹¹ Cyberspace Administration of China, "国家互联网信息办公室关于发布第九批境内区块链信息服务备案编号的公告" [CAC Announcement concerning the Publication of the 9th Batch of Blockchain Information Service Filing Numbers], accessed 28 November 2022, at <http://www.cac.gov.cn/2022-07/25/c_1660369837207693.htm?mc_cid=4ee2811e1c&mc_eid=ad7c94e0d8>.

⁹² Qiang Wang et al., "Is China the World's Blockchain Leader? Evidence, Evolution and Outlook of

China's Blockchain Research," *Journal of Cleaner Production*, vol. 264 (2020).

⁹³ Coco Feng, "China Makes up 84 Per Cent of Blockchain Applications Worldwide, State Official Says, but Only a Fifth are Approved", *South China Morning Post*, accessed 28 November 2022, at <<https://www.scmp.com/tech/policy/article/3193379/china-makes-84-cent-blockchain-applications-worldwide-state-official>>.

⁹⁴ BSN Website, accessed 28 November 2022, at <<https://bsnbase.io/g/main/index>>.



to use the application. It also has partnerships with other public blockchain providers, such as Ethereum, EOS, Tezos, Casper and Findora. BSN operates a domestic and an international wing, and the latter works through data centres owned by Google Cloud and Amazon Web Services (AWS). The domestic side is hosted on Baidu AI Cloud. Decentralized applications (DApps) are made available through city nodes, of which there are over 100 in China. International nodes are located in Singapore, Tokyo, Sydney, Johannesburg, Sao Paulo, Paris and California.⁹⁵ Its short-term outlook envisages expansion of the system across all Chinese provinces, an increase in the number of city nodes and the creation of a universalized digital payments system.⁹⁶

In September 2022, the BSN consortium announced the establishment of an international spin-off, the Spartan Network, which from the start managed to attract the custom of several large Hong Kong businesses, such as Emperor Group, HSBC, Lan Kwai Fong Group and Maxim's Group. For the time being, however, many of BSN's applications seem to be vanity projects with little impact on core business models, such as redemption of non-fungible token-based gift certificates and the creation of blockchain-based customer loyalty cards.⁹⁷ The network's aspirations are

bigger, and include the formation of blockchain infrastructure for the connectivity corridor around the Digital Silk Road. Whether this will ever materialize depends substantially on the ability of the BSN and Spartan Network to add value and convenience for users and generate sufficient trust in an infrastructure that operates under the close supervision of the Chinese leadership.

Completely absent from these blockchain ambitions is the application for which the technology is best known worldwide: cryptocurrencies. In 2013, the People's Bank of China (PBoC) prohibited the country's banks from handling bitcoin transactions. Four years later, it banned initial coin offerings. In September 2021, after further progressive limitations on crypto mining, the PBoC declared all cryptocurrency transactions illegal.⁹⁸ This ban reflected multiple concerns about the underlying technologies of cryptocurrencies and the uses to which they can be put. There are also environmental concerns: in 2019, China accounted for three-quarters of the global energy consumption linked to crypto mining. Furthermore, the PBoC sees them as speculative assets that could endanger financial stability. Lastly, cryptocurrencies are often used for illegal transactions, including unlawful capital expatriation, which Beijing intends to

⁹⁵ BSN, "节点运行情况" [Node Running Conditions], accessed 28 November 2022, at <<https://www.bsnbase.com/p/main/serviceNetworkDesc?type=RunningCondition>>.

⁹⁶ Mikko Raud (note 83).

⁹⁷ Xinmei Shen, "China's State-Backed Architect of Non-Crypto Blockchain Makes First Major Push Outside Mainland", *South China Morning Post*, accessed

28 November 2022, at <https://www.scmp.com/tech/tech-trends/article/3191553/chinas-state-backed-architect-non-crypto-blockchain-makes-first?mc_cid=113f7b04eb&mc_eid=ad7c94e0d8>.

⁹⁸ AP News, "China Says all Crypto Transactions Illegal: Bitcoin Tumbles", 24 September 2021, accessed 28 November 2022, at <<https://apnews.com/article/china-declares-cryptocurrency-bitcoin-transactions-illegal-c6e869b63af6de3d1d699ee105d602e6>>.



curb. China has moved ahead with its own central bank digital currency, the e-CNY, but this is not based on blockchain technology.⁹⁹

Europe

The EU and its member states have also identified blockchain technology as a strategic emerging technology. The European blockchain strategy aims to establish leadership in blockchain technology, foster innovation in blockchain and facilitate the emergence of leading platforms, companies and applications. The core presumption in this strategy is that blockchain will enhance trust in data, facilitating online transactions and information sharing. To this end, the EU intends to set a “gold standard” that reflects European values. This gold standard includes environmental sustainability, data protection, support for the digital identity framework, cybersecurity and interoperability.

Like China, the EU supports the construction of public blockchain infrastructure through the European Blockchain Service Infrastructure (EBSI) programme. This is a peer-to-peer network with nodes foreseen in every EU member state as well as Norway and Liechtenstein. The initial use cases of EBSI revolve around notarization, verification of diplomas and educational credentials, supporting the European digital identity and trusted data sharing. In future, it will also support the financing of small and medium-sized enterprises (SMEs), cross-border access to welfare services for EU citizens, and facilitation of cross-border asylum procedures. More broadly, the EU intends to promote legal certainty through

blockchain-enabled digital assets and smart contracts, increase funding for blockchain research, promote the use of blockchain for sustainability, support the development of interoperable technical standards, enhance blockchain skills development and create multistakeholder bodies for cooperation.

In academic research, Europe does not currently have the same level of visibility in top-tier venues as China or the US, and there are fewer highly active groups in the EU than in those two countries. Current research is still highly exploratory, and identifies new challenges and possible solutions in quick succession. It remains to be seen whether Europe’s strong tradition in formal (mathematics-based) analysis methods will increase its technology momentum in the long term by providing a crucial means for achieving robust, trustworthy software. There are some similarities in applications: both China and the EU have tended to assign a stronger coordinating role to government in comparison with the nearly entirely private sector-led US approach. At the same time, the ambitions of both actors are very different. China sees the BSN as a potentially global network while Europe’s EBSI is predominantly aimed at the internal market and bordering countries such as Ukraine and Norway. The EBSI is smaller in scale and, reflecting the often glacial pace of European policymaking, is developing far more slowly. But the EU’s commitment to transparency and inclusion is likely to be more amenable to international organizations than China’s counterpart.

⁹⁹ Martin Chorzempa, *The Cashless Revolution: China’s Reinvention of Money and the End of America’s*

Domination of Finance and Technology, Public Affairs, New York, 2022.

























ACTOR TYPE	NAME OF KEY ACTOR	DESCRIPTION	KEY TASK	PRIORITY
Leading scientist	 Xiapu Luo (罗夏朴)	Associate Professor at Hong Kong Polytechnic University, collaborator on 11 top-tier publications	Expert on software engineering, software security and smart contracts; many international collaborations on smart contracts	
Research institution	 Zhejiang University (浙江大学)	Leading Chinese university	Leading research groups on smart contract and blockchain security, each with eight top-tier publications (a few collaboratively between Zhejiang and Peking University)	
Research institution	 Wuhan University (武汉大学)	Leading Chinese university	Leading research groups on smart contract and blockchain security, each with eight top-tier publications	
Research institution	 Peking University (北京大学)	Leading Chinese university	Leading research groups on smart contract and blockchain security, each with eight top-tier publications (a few collaboratively between Zhejiang and Peking University)	
Corporation	 Huawei (华为)	Large technology corporation	Industrial partner in academic research	
Corporation	 Ant Group (蚂蚁集团)	Large technology corporation	Industrial partner in academic research	
Policy Institution	 National Development and Reform Commission (NDRC) (国家发展和改革委员会)	In overall charge of planning on economic development	Oversees the inclusion of blockchain into the digital economy	
Policy Institution	 Cyberspace Administration of China (国家互联网信息办公室)	Digital regulator and coordinating body	Regulates blockchain information services and coordinates blockchain rollout	
Policy Institution	 Supreme People's Court (最高人民法院)	Highest judicial body	Operates judicial blockchain	
Policy Institution	 State Information Centre (国家信息中心)	Policy think tank under the NDRC	Member of the Blockchain Service Network (BSN) Consortium	
Corporation	 Red Date Technology (红枣科技有限公司)	Hong Kong-based corporation	In technical charge of the BSN Consortium	

Figure 4.1. – Actors to watch



Impact on strategic autonomy

As blockchain technology is still embryonic, it is difficult to predict its long-term impact. Nonetheless, it is useful to formulate possible future scenarios to assist with the creation of policy analysis frameworks and the identification of signifiers that might require a response. In an overall sense, it is important to understand these impacts on two levels. First, there is the broad adoption of Chinese blockchains in bilateral interactions and in third countries more broadly, which European actors would have to use. Second, there is the possible impact of technological non-compatibility between blockchain applications developed in Europe and those developed in China.

Supply chain resilience

The EU has developed a number of policies to increase domestic capacity, diversify product sources and suppliers, and maintain the integrity of multilateral trading systems in response to the challenges to product supply chains that arose in the Covid-19 pandemic, as well as from the Russian invasion of Ukraine and growing geopolitical tensions with China.¹⁰⁰ If blockchain technologies become important enablers of supply chains, the EU will need to consider the extent to which this might create leverage for Chinese actors over European private and public sector entities. In the case of use of Chinese-run

blockchain apps, for instance, it might be possible for the Chinese government to leverage dependence on these services by denying service, or to obtain data and information to which it would not otherwise have access. In the case of multiple incompatible blockchain services, however, EU players might be confronted with increased costs of global trade and supply chain maintenance.

National security

The immediate impact of China's blockchain agenda on traditional core elements of national security is relatively limited. The People's Liberation Army is exploring the use of blockchain-enabled systems to manage information about soldiers, including data on their training, career paths and mission history, and to evaluate their performance, provide rewards or impose sanctions.¹⁰¹ More specifically, the use of blockchain applications may have cybersecurity consequences, as a China-dominated infrastructure could theoretically be compromised by having all Chinese actors collude against the underlying security assumptions.¹⁰²

Another concern relates to the geopolitical impact of China's blockchain strategy. Blockchain introduces a further form of technological interaction, and thereby dependence and vulnerability, into a deeply

¹⁰⁰ Marcin Szczepeński, "Resilience of Global Supply Chains: Challenges and Solutions", European Parliament Briefing, Members' Research Service, November 2021, accessed 28 November 2022, at <[https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698815/EPRS_BRI\(2021\)698815_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698815/EPRS_BRI(2021)698815_EN.pdf)>.

¹⁰¹ Xuanzun Liu, "Chinese Military Could Deploy Blockchain Management", *Global Times*, 18 November 2019, accessed 28 November 2022, at <<https://www.globaltimes.cn/content/1170370.shtml>>.

¹⁰² Arati Baliaga, "Understanding Blockchain Consensus Models", *Persistent*, vol. 4, no. 1 (2017).



interdependent world that has started to fray. For instance, the US might sanction suppliers to BSN, or collaborative partners in the Network inside the US. This might, in turn, affect relationships with third countries with significant exposure to the BSN. Most importantly, however, is the BSN's role in the Digital Silk Road. If China is a first mover there, it might gain enough traction to become a tool for China to wield strategic economic leverage.¹⁰³ BSN's value proposition is not only based on technological functionality and feature sets, but also on ease of use, low cost and broad interoperability. This combination of factors would be very attractive to less well-off countries that do not have significant geopolitical concerns about China's rise. The counterpoint to this would be a scenario under which businesses and governments would be wary of becoming too reliant on initiatives closely connected to the Chinese state, in which case the BSN and other initiatives would not achieve widespread adoption.

Values and sustainability

China's technological ambitions and its growing international footprint have had a significant ideational impact on Western perceptions and, increasingly, concerns.

China has defied widespread impressions that it is a non-innovative country,¹⁰⁴ and foreign observers and NGOs now sound warnings about the potentially repressive impact of Chinese "techno-authoritarianism" at home and abroad.¹⁰⁵ The Digital Silk Road, for instance, is seen as a platform for the spread of Chinese hardware, software and online services with architectures more amenable to Beijing's control-oriented, government-led view of digital affairs.¹⁰⁶ The emergence of blockchain applications therefore raises questions about the extent to which they may be used in ongoing Chinese social control programmes or might find root elsewhere in the world.

It is certainly true that the set-up of platforms such as the BSN dilutes the possible transparency, privacy and immutability of data stored on blockchains, which makes them more susceptible to government intervention or manipulation. At the same time, however, the Chinese authorities would face trade-offs: intervention and manipulation would run counter to the assurances that need to be given to global BSN users that their data and privacy will be appropriately protected. Red Date has addressed such privacy concerns, claiming that "no private user data is stored

¹⁰³ RWR Advisory, "The Emergence of China's State-Backed Blockchain Platform: The Risks and Geopolitical Implications of China's State-Backed Blockchain Platform", June 2021, accessed 28 November 2022, at <<https://www.rwradvisory.com/wp-content/uploads/2021/06/RWR-Report-Blockchain-6-2021.pdf>>.

¹⁰⁴ Regina Abrami et al., "Why China Can't Innovate", *Harvard Business Review*, March 2014, accessed 28 November 2022, at <<https://hbr.org/2014/03/why-china-cant-innovate>>.

¹⁰⁵ Jonathan Hillman, "Techno-Authoritarianism: Platform for Repression in China and Abroad", CSIS,

accessed 28 November 2022, at <<https://www.csis.org/analysis/techno-authoritarianism-platform-repression-china-and-abroad>>.

¹⁰⁶ Jon Bateman, "Denying Support for Chinese and China-enabled Authoritarianism and Repression", *Carnegie Endowment for International Peace*, 25 April 2022, accessed 28 November 2022, at <<https://carnegieendowment.org/2022/04/25/denying-support-for-chinese-and-china-enabled-authoritarianism-and-repression-pub-86924>>.



on the BSN or within the platform”, and that “there is no API [application programming interface] to personal private data on the empowerment platform used within portals, and personal information of all developers and DApp users is managed independently by each BSN portal”.¹⁰⁷ Even so, much will depend on the encryption standards used by the network. If these are Chinese standards, there will always be a possibility that backdoors exist.¹⁰⁸ The risk of backdoors may be comparable to early web browsers in the late 1990s, where the US only allowed legal exports of versions that were known to have extremely weak encryption.¹⁰⁹

Domestically, China’s judiciary has been an early adopter of blockchain in the litigation process. In May 2022, the Supreme People’s Court announced that over 2.6 billion pieces of judicially relevant information, including documentary evidence and judicial certificates, were already being stored on the blockchain. It intends that blockchain will enhance the efficiency of the judicial process, particularly in relation to complex and cross-regional cases. Moreover, the court plans to collaborate more closely with blockchain platforms and private sector entities to enhance intellectual property protection and the overall

business environment, better manage corporate bankruptcy and reorganization, and consolidate the social credit system.¹¹⁰ The latter is an example of how concerns about China can be exaggerated. The social credit system is not after all a technologically empowered Orwellian behemoth quantitatively scoring each Chinese individual in real time.¹¹¹ The new draft Social Credit System Construction Law does not mention blockchain,¹¹² and related policy documents only perfunctorily refer to it as a particular kind of technology, use of which can be explored. If introduced, blockchain would not significantly affect the functioning of the system, merely offer new technical processes for its operation.

Technological competitiveness

The extent to which China’s blockchain capabilities affect the technological competitiveness of the EU will be decided largely by the extent to which blockchain delivers the transformational economic impact its proponents claim. Moreover, if the impact of blockchain is largely incremental, many areas of its adoption will not necessarily have a significant bearing on Europe’s technological competitiveness with China. The adoption of blockchain in domestic governance systems, for instance, might

¹⁰⁷ RWR Advisory (note 103).

¹⁰⁸ Shuyao Kong, “BSN’s ‘ChinaChain’ Launches Globally”, *Decrypt*, 26 April 2020, accessed 28 November 2022, at <<https://decrypt.co/26693/bsns-chinain-launches-globally>>.

¹⁰⁹ Robert Sanders, “The Only Legally Exportable Cryptography Level is Totally Insecure: UC Berkeley Grad Student Breaks Challenge Cipher in Hours”, UC Berkeley, 29 January 1997, accessed 28 November 2022, at <<https://www.berkeley.edu/news/media/releases/97legacy/code.html>>.

¹¹⁰ Supreme People’s Court (note 82).

¹¹¹ Vincent Brussee, “China’s Social Credit System is Actually Quite Boring”, *Foreign Policy*, 15 September 2021, <<https://foreignpolicy.com/2021/09/15/china-social-credit-system-authoritarian/>>.

¹¹² National People’s Congress, “中华人民共和国社会信用体系建设法（向社会公开征求意见稿）”, [Social Credit System Construction Law of the People’s Republic of China (Public Opinion Solicitation Draft)], China Law Translate, accessed 29 November 2022, at <<https://www.chinalawtranslate.com/en/social-credit-law/>>.



provide slightly more efficient interactions between government and citizen or private business, but would not generate meaningful differences in comparative productivity.

If blockchain does become a transformational technology, however, Europe will have to contend with a China that has been at the forefront of research and real-life experimentation with blockchain and has attempted to internationalize it. Thus far,

the degree of international cooperation in the region is extremely limited. There is a BSN portal in Singapore, and one in South Korea is planned.¹¹³ There is little evidence to suggest significant levels of interaction beyond that. International adoption would have multiple advantages, creating established markets where late arrivals face significant thresholds to entry, as well as efficiencies of scale that would enable the amortization of R&D expenses across a larger user base.





DIMENSION OF STRATEGIC AUTONOMY	SHORT DESCRIPTION OF CHALLENGE IN KEYWORDS	RELATIVE IMPORTANCE OF CHALLENGE ON A SCALE OF 1 TO 4	POLICY INSTRUMENTS FOR TACKLING CHALLENGE IN KEYWORDS
 Resilience of supply chains	<ul style="list-style-type: none"> • Use of Chinese blockchains creates leverage for China over European companies and governments; • Incompatibility between European and Chinese blockchains leads to higher business costs 	<p>2</p> <p>1</p>	<ul style="list-style-type: none"> • Diplomatic engagement with third countries; • Develop leadership in international standardization processes
 National security	<ul style="list-style-type: none"> • Blockchain-related cybersecurity concerns • Geopolitical impact of blockchain in connection with Belt and Road Initiative 	<p>2</p> <p>3</p>	<ul style="list-style-type: none"> • Develop cybersecurity regulation for blockchain-using entities; • Diplomatic engagement with third countries, support for trusted alternative to BSN
 Values and sustainability	<ul style="list-style-type: none"> • Energy use of blockchain technology • Privacy concerns around storing sensitive information on BSN 	<p>3</p> <p>3</p>	<ul style="list-style-type: none"> • Mandate the inclusion of blockchain-generated carbon costs into pricing; • Implement GDPR requirements for BSN services as appropriate
 Technological competitiveness	<ul style="list-style-type: none"> • Chinese leadership in blockchain technology • Deepening regional collaboration between China and other Asian countries 	<p>4</p> <p>3</p>	<ul style="list-style-type: none"> • Invest in blockchain research and broad industrialization/application; • Leverage existing partnerships and create more attractive offerings

Figure 4.2. – Recommendations

¹¹³ Timmy Shen, “China’s State-backed Blockchain Network to Expand to South Korea”, *Forkast*, 1 September 2021, accessed 28 November 2022, at <<https://>

forkast.news/china-blockchain-network-expand-south-korea/>.



Recommendations

As noted above, blockchain technologies and their applications are still in their infancy, and much about their eventual impact on economic, political and social processes remains to be seen. Consequently, to avoid excessive speculation, the specific recommendations emerging from this chapter are largely aimed at enhancing monitoring capabilities and consultation with other countries, implementing fundamental legislative and regulatory requirements for blockchain-enabled systems, and investing in future-oriented research and implementation projects. To address the four dimensions of strategic autonomy the EU should consider the following measures, which are summarized in Figure 4.2.

Supply chain resilience: Blockchain technology depends on specialized hardware chips for energy efficiency and on cutting-edge software. The chip supply chains are currently highly dependent on Taiwan but are being diversified. Software platforms are mostly based on open-source software, which alleviates concerns about their availability but still requires good practice in overall IT supply chain management.¹¹⁴ Diplomatic engagement with third countries and developing leadership in international standardization processes will therefore be essential.

National security: the EU should be proactive in research to identify the potential technical and non-technical security

risks emerging from blockchain applications and start to develop cybersecurity regulation. Ideally, this would entail working together with third countries. Moreover, particularly in relation to third countries, Europe should take initiatives to develop or support trusted alternatives to BSN and other Chinese technologies.

Values: General Data Protection Regulation (GDPR) compliance will require technologies that make it possible to “forget” data. This can be a way to deal with potentially flawed off-chain input data and to comply with the GDPR.¹¹⁵ Energy-limiting policies may also determine which blockchain platforms will be used in the EU.

Technological competitiveness: Smart contracts are currently relatively unreliable due to the lack of strong verification. Europe is traditionally strong on formal methods, which leverage mathematical methods for strong verification. Promoting formally verified blockchain and smart contract platforms could leverage Europe's strengths and promote the acceptance of such new platforms, which are currently mostly used as research tools.

Moreover, it is important that the EU does not go it alone in the implementation of blockchain technology: it needs to expand consultation with third countries on both technological interoperability and

¹¹⁴ Sandor Boyson, “Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems”, *Technovation*, vol. 34, no. 7 (2014), 342–353.

¹¹⁵ Simon Farshid, Andreas Reitz and Peter Roßbach, “Design of a forgetting blockchain: A possible way to accomplish GDPR compatibility”, Proceedings of the 52nd Hawaii International Conference on System Sciences, 2019.



establishing benchmarks for what constitute trusted blockchain systems.

These specific recommendations can only be realized by a broader shift in attitude that affects the way policymakers understand and respond to the potential challenges emerging from China. First, European actors should keep calm. Precisely because so much about blockchain is still unproven, it is tempting to give in to alarmist scenarios and unfounded fears. The remedy for this is better information and knowledge. Europe should develop a comprehensive understanding of the technological parameters and constraints that affect blockchain development, the political questions and trade-offs that are necessary for its internationalization and the measures necessary for its acceptance in broader markets. This will enable a far more targeted and accurate response to potential Chinese challenges than amorphous references to “digital authoritarianism”. China has, after all, been perfectly capable of imposing strict control on the virtual realm without blockchain technology. The EU should continuously monitor the moves that China is making internationally and develop frameworks for assessing their impact and importance. This will assist with prioritization and distinguishing core concerns from others.

Second, Europe should not primarily base policy on responses to Chinese actions and initiatives. The EU has already developed a comprehensive blockchain

strategy, which can serve as a basis for the development of competitive technologies, products and services for the European and global markets. This will require considerable investment, as well as exploration of models that integrate public and private sector actors and bypass the glacial pace of bureaucratic processes for which Brussels is renowned. The EU should also fully exploit its position as a regulatory superpower to develop the frameworks and rules necessary to protect its interests and values.

Third, particularly in its dealings with other countries, Europe should lead by example, not by statement. For instance, even though the BRI and the associated Digital Silk Road have raised concerns about greater Chinese influence in the Global South, the EU and its partners are still being slow to develop alternatives that are more attractive than the Chinese proposition. Perhaps counterintuitively, engagement with third countries should centre on them rather than China. European entreaties are unlikely to gain a warm welcome in African or South Asian capitals if this is merely seen as a bid to resolve Europe’s “China problem”. More broadly, as a conglomeration of small and mid-level states, maintenance of a universally respected rules-based order for both political and economic concerns is one of the EU’s core interests. It should therefore ensure that this order remains stable and attractive to small and medium-sized entities elsewhere in the world.



Authors:

Cyrille Artho is an associate professor in software engineering at KTH Royal Institute of Technology, Stockholm, Sweden. Contact: artho@kth.se

Rogier Creemers is a university lecturer in politics and governance of modern China at Leiden University, the Netherlands. Contact: r.j.e.h.creemers@hum.leidenuniv.nl



Assessing the Financial and Geoeconomic Implications of China's Digital Currency

Amir Elalouf, Maximilian Mayer

Abstract

The digital yuan (e-CNY) is an example of a field in which China is ahead of its global peers. It is the first major advanced economy to implement a digital currency, and this fast-paced development mirrors its ambitions as a financial power. The e-CNY is a form of central bank digital currency that aims to replace cash in circulation. It is a digitized version of China's legal (fiat) currency. Although functionally, e-CNY is similar to online payment platforms, it makes up a proportion of the country's money supply. Moreover, the digital yuan is not confined to the domestic market. Its ultimate objective is to go global to improve cross-border payments. It is therefore important to understand the relevance of the e-CNY from a European point of view with regard to three issues: (a) the similarities and differences between the digital yuan and the digital euro; (b) the domestic and international actors developing the digital yuan; and (c) the impact of the e-CNY on the four dimensions of Europe's strategic autonomy. The paper highlights the possible effects of the e-CNY on European security, values and competitiveness, and recommends steps to improve Europe's economic and technological stance.

Digital currencies in China and Europe

Developments regarding digital currencies, from cryptocurrencies to stablecoins and Central Bank Digital Currencies (CBDCs), have been rapid and tumultuous in recent years. The market cap for the two most prominent cryptocurrencies has reached almost US\$ 540 billion. Many central banks, including the European Central Bank, are working on digital fiat currencies, but the People's Bank of China (PBOC) has been the frontrunner. The e-CNY is not a decentralized cryptocurrency like bitcoin but

a digitized version of China's legal (fiat) currency – the renminbi (RMB). The PBOC controls and issues the e-CNY. Digital currencies could provide alternatives to the global influence of the US dollar. Their future is intertwined with China's ambition to become a financial power and the inevitable geopolitical tension with the



United States that this course implies.¹¹⁶ Evolving payment systems, developing financial infrastructures, and the digitization of money are key to monetary sovereignty and economic power.¹¹⁷ Chinese advances in these areas are highly relevant for the European Union from the perspective of geoeconomics and geopolitics.

From the perspective of the Chinese party state, digital money poses a challenge that has the potential to undermine monetary sovereignty and capital controls. However, it also provides an opportunity to create new, transnational digital payment infrastructures that are more China-centric.¹¹⁸ Initially, cryptocurrencies, like other fintech, flourished in a largely unregulated environment in China. However, they are now perceived by the PBOC as a potential threat to financial security.¹¹⁹ Chinese laws and regulations have been progressively tightened, finally leading to a ban on crypto-

currencies and even the criminalization of mining operations.¹²⁰ In contrast, the e-CNY has been consistently viewed as a secure and controllable option designed to serve as a digital analog to cash and part of China's monetary base (M0).¹²¹

Central bank money has unique advantages in terms of safety, finality, liquidity, and integrity. The e-CNY aims to serve as retail "digital cash". It seeks to replace electronic payments rather than bank accounts, thereby ensuring that commercial banks will not be disintermediated. The e-CNY is a digitized version of China's legal currency with the same value as the physical RMB. The widespread use of Alipay and WeChatPay links users' bank accounts to a digital wallet, making a large share of transactions in China cashless. From a financial perspective, the Chinese central bank believes that the e-CNY can make payments less costly, more efficient, and more inclusive. It is commonly assumed

¹¹⁶ Martin Chorzempa, "China, the United States, and Central Bank Digital Currencies: How Important is it to be First?", *China Economic Journal*, vol. 14, no. 1 (January 2021), pp. 102–115, <doi: 10.1080/17538963.2020.1870278>.

¹¹⁷ Ying Huang and Maximilian Mayer, "Digital Currencies, Monetary Sovereignty, and US–China Power Competition", *Policy & Internet*, vol. 14, no. 2 (June 2022), pp. 324–347; Johannes Petry, "Beyond Ports, Roads and Railways: Chinese Economic Statecraft, the Belt and Road Initiative and the Politics of Financial Infrastructures", *European Journal of International Relations* (October 2022), <https://doi.org/10.1177/13540661221126>; Marieke de Goede and Carola Westermeier, "Infrastructural Geopolitics", *International Studies Quarterly*, vol. 66, no. 3 (September 2022), <https://doi.org/10.1093/isq/sqac033>.

¹¹⁸ On the nexus of the digital yuan and blockchain technologies see Gary Sigley and Warwick Powell, "Governing the Digital Economy: An Exploration of Blockchains with Chinese Characteristics", *Journal of*

Contemporary Asia, 1 August 2022, <doi: 10.1080/00472336.2022.2093774>.

¹¹⁹ Sara Hsu and Jianjun Li, *China's Fintech Explosion: Disruption, Innovation, and Survival*, New York, Columbia University Press, 2020; Martin Chorzempa and Yiping Huang, "Chinese Fintech Innovation and Regulation", *Asian Economic Policy Review*, vol. 17, no. 2 (February 2022), pp. 274–292, <doi: https://doi.org/10.1111/aepr.12384>.

¹²⁰ Between September 2019 and July 2021, China's share of the global "hashrate" shrank from 75% to zero. After a short hiatus, however, it was back to around 21% in January 2022 despite a harsh regulatory crackdown. See Cambridge Centre for Alternative Finance, Bitcoin Mining Map, "Evolution of network hashrate", accessed 5 December 2022 at <https://ccaf.io/cbeci/mining_map>.

¹²¹ Arendse Huld, "China Launches Digital Yuan App: All You Need to Know", *China Briefing*, 22 September 2022, <https://www.china-briefing.com/news/china-launches-digital-yuan-app-what-you-need-to-know/>.



that the e-CNY will contribute to financial stability through a system of “controllable anonymity”, in which payments are largely anonymous but still allow the data analysis tools of the central banks to detect illegal activity and prosecute financial crime. Chinese regulators are seeking to increase competition in the payments space while reducing systemic risk.¹²² The design of the e-CNY merges the features of the physical RMB, such as settlement upon payment and anonymity, with the characteristics of electronic payment instruments, which are less costly, highly portable and efficient, and hard to counterfeit.

The key advantage of the e-CNY over the RMB is the international digital currency infrastructure it could potentially provide to serve diverse payment needs. It delivers more efficient financial services, can include smart contracts and other blockchain applications, warrants more straightforward conversion, and simplifies bank and peer-to-peer settlement.¹²³ In line with improving economic connectivity through the Belt and Road Initiative, China is participating in the mBridge, a CBDC project that brings together central banks from the Middle East, Southeast Asia, and Greater China. Its pilot phase “demonstrated the

platform’s ability to improve cross-border payment speed and efficiency and to reduce settlement risks in a real-world setting”.¹²⁴ The e-CNY also offers a novel technological monetary instrument. Digital money can be programmed to function as “consumption coupons” to push domestic consumption, which will be a key priority of post-Zero-covid economic policies.

The e-CNY circulates via a “two-tier” system of distribution and expenditure, wherein the PBOC authorizes partner institutions, such as state-owned commercial banks and the financial arms of Tencent and the Alibaba-affiliated Ant Group, to distribute currency to consumers. Consumers store and spend the e-CNY using “wallet” apps operated by these companies or specialized devices called “hardware wallets”. The e-CNY, therefore, offers the public a cash-like digital payment method that is ostensibly accessible to all. To ensure the system’s reliability and soundness, the e-CNY implements a distributed and platform-based design using a mix of technologies, such as trusted computing and special encryption based on hardware and software integration.¹²⁵

¹²² See Working Group on E-CNY Research and Development of the People’s Bank of China, “Progress of Research & Development of E-CNY in China”, July 2021, accessed 5 December 2022 at <<http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf>>. The cost of cash management is relatively high.

¹²³ Elijah J. Fullerton and Peter J. Morgan. “The People’s Republic of China’s Digital Yuan: Its Environment, Design, and Implications.” *ADB Discussion Paper* 1306, Asian Development Bank Institute, February

2022, <<https://www.adb.org/publications/the-peoples-republic-of-chinas-digital-yuan-its-environment-design-and-implications>>; Working Group on E-CNY Research and Development of the People’s Bank of China (note 122).

¹²⁴ Bank for International Settlement Innovation Hub, “Project mBridge connecting economies through CBDC”, October 2022, <<https://www.bis.org/publ/othp59.pdf>>.

¹²⁵ Working Group on E-CNY Research and Development of the People’s Bank of China (note 122).



CRITERIA	THE DIGITAL YUAN/ 数字人民币	THE DIGITAL EURO
Objective	The digital yuan will ultimately replace the physical yuan	The digital euro will only complement the physical euro
System	A two-tier system that is not reliant on distributed ledger technology	A two-tier system that is not reliant on distributed ledger technology
Implementation	Large-scale pilot schemes since 2020, 261 million users (2022), 360 million transactions (in 2022), transaction value 12.7 billion RMB (Jan. to Aug. 2022)	No pilots thus far
Features	Cash-like features; the ability to make or receive payments without going online or being connected to telephone networks	Cash-like features; the ability to make or receive payments without going online or being connected to telephone networks
Technological configuration	A bank account is needed and payment is by phone/app.	A pre-paid device or card; payment is via an app.
Technological features	Digital currencies and associated wallets are interoperable with current and future payment services and platforms	Digital currencies and associated wallets are interoperable with current and future payment services and platforms

Figure 5.1. – e-CNY vs. the digital euro

The e-CNY and the digital euro share strategic and technological similarities but diverge in crucial respects (Figure 5.1). The PBOC and the European Central Bank (ECB) are both pursuing a two-tier system that is interoperable with existing digital payment services but not reliant on distributed ledger technology. Both currencies are stored in digital wallets. This feature allows central banks to have a remunerative

policy (i.e., payment of interest) on CBDC holdings not possible with banknotes and coins. Nonetheless, it is envisaged that the PBOC will completely replace cash while the ECB seeks to complement the physical euro.¹²⁶ Another critical difference is that the e-CNY is pegged with the RMB to a currency basket, while the digital euro would be a free-floating currency.

Main actors in the development of the digital yuan

The Chinese government aims to create a new monetary digital instrument across platform payment systems. The associated private-public governance architecture will consist of “consortium chains”,

entailing a “multiplicity of actors, coalescing around a shared technical infrastructure and operational protocols”.¹²⁷ The Chinese government views the e-CNY as a “dynamic, evolving system”

¹²⁶ See Joachim Nagel, “Digital euro: Opportunities and risks”, CFS-IMFS Special Lecture, Goethe University, Bundesbank, 11 July 2022, <<https://www.bundesbank.de/en/press/speeches/digital-euro-opportunities-and-risks-894326>>; and Hung Tran, “The digital yuan, digital euro, and the diem: Key issues

for public debate”, Atlantic Council, 6 April 2021, <<https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-digital-yuan-digital-euro-and-the-diem-key-issues-for-public-debate/>>.

¹²⁷ Gary Sigley and Warwick Powell (note 118).



and wants to prevent monopolies “which could pose barriers to new technological paths”.¹²⁸ The three main financial actors responsible for promoting the implementation of the e-CNY are the PBOC and its branches, state-owned commercial banks, and the large private e-commerce platforms (see Figure 5.2).

The PBOC began its research into digital currencies in 2014. Following a small pilot programme in 2019, the initiative greatly expanded in 2021 and 2022 when 23 Chinese mainland cities accounting for nearly one-fifth of the mainland’s population adopted the e-CNY. Pilot schemes for the e-CNY were also introduced in other settings, such as the Beijing Winter Olympics in February 2022.¹²⁹ The e-CNY has been used in over 8.08 million individual transactions.¹³⁰ The value of total transactions reached approximately 100 billion yuan (\$13.9 billion) by the end of August 2022, a sizeable percentage of global e-

currency transactions.¹³¹ This uptake is in line with China’s staggering adoption rate of new financial technology. For example, mobile wallet payments in China in 2019 were almost 1.5 times the total value of credit card transactions outside China. The most prominent payment apps in the country have a user base of 872 million people.¹³²

Although the new digital currency is still a marginal component of China’s financial structure, there has been impressive growth and huge growth potential. Existing digital payment ecosystems are predominantly owned by private companies. Currently, the e-CNY market is small relative to China’s population, and the e-CNY still has a lower favourability rating (60%) than Alipay and WechatPay (84% and 83%, respectively).¹³³ However, when the market cap becomes a hundred times bigger, as happened to the digital dollar (USDC, see Figure 5.3), it will become important in China and globally.¹³⁴

¹²⁸ Zhou Xiaochuan, “Understanding China’s Central Bank Digital Currency”, China Finance 40 Forum, 13 December 2020, <http://www.cf40.com/en/news_detail/11481.html>.

¹²⁹ Rajesh Bansal and Somya Singh, “China’s digital yuan: An alternative to the dollar-dominated financial system”, *Carnegie Endowment for International Peace*, 2021, <<https://carnegieindia.org/2021/08/31/china-s-digital-yuan-alternative-to-dollar-dominated-financial-system-pub-85203>>; Citic Securities 2022 “数字人民币专题研究报告：数字经济时代支付基础设施” [“Digital RMB Special Research Report: Payment Infrastructure in the Digital Economy Era”], <<https://www.vzkoo.com/document/20220315bd9a6621cc625ecd7fd04f57.html?keyword=%E6%95%B0%E5%AD%97%E4%BA%BA%E6%B0%91%E5%B8%81>>.

¹³⁰ Lian Cheng, “Will China Open the Era of Sovereign Digital Currency?”, *China Watch*, vol. 2, no. 12 (March 2022), <<https://china-cee.eu/2022/03/28/will-china-open-the-era-of-sovereign-digital-currency/>>.










¹³¹ Zhang Tianyuan, “Digital yuan to spread its wings”, *China Daily*, 11 November 2022, <<https://www.chinadaily.com.cn/a/202211/11/WS636de7bfa3104917543292e4.html>>.

¹³² Kalina Tonkovska, “Digital yuan: The financial revolution of the east”, *Industria*, 9 February 2022, <<https://www.industria.tech/blog/digital-yuan-the-financial-revolution-of-the-east/>>; Jaime Toplin, “China continues expanding and incentivizing digital yuan”, *Insider Intelligence*, 20 July 2022, <<https://www.insiderintelligence.com/content/china-continues-expanding-incentivizing-digital-yuan>>.

¹³³ Ryan Heath, “Watch out for China’s digital yuan”, *Politico*, 13 May 2022, <<https://www.politico.com/newsletters/digital-future-daily/2022/05/13/watch-out-for-chinas-digital-yuan-00032475>>; Jaime Toplin (note 132).

¹³⁴ E-CNY and USDC are stablecoins and have similar numbers of potential users. Since historical data on the e-CNY are quite limited, we use the digital dollar as a proxy. USDC daily volume was 230 million after less than one year in the market, which is the daily volume of e-CNY today. Today, after 3 years in the market, the USDC has a \$4 billion daily trading volume, and we forecast a similar future for the e-CNY by 2026.



ACTOR TYPE*	NAME OF KEY ACTOR	DESCRIPTION	KEY TASK	PRIORITY
Policy Institution	 The People's Bank of China (PBOC) 中国人民银行 and its branches	Central actor in the design, implementation and regulation of CBDCs	Coordinates the issuance and cancellation of e-CNY, inter-institutional networking and wallet ecology management, cooperation with central banks in other countries; Supervises exchange and circulation services	●
Research Institution	 Digital Currency Research Institute of the People's Bank of China 中国人民银行数字货币研究所	Part of the PBC; Central research facility and hub for cooperation with other central banks on developing CBDCs	Research on design of e-CNY	◐
Commercial bank	 Industrial and Commercial Bank of China (ICBC) 中国工商银行	Technology & service implementation with users	Responsible for e-CNY exchange and circulation services, such as opening e-CNY accounts/digital wallets, promoting use of the e-CNY and e-CNY marketing campaigns; Investment in hardware and software infrastructure for retail e-CNY	◐
Commercial bank	 Agricultural Bank of China (ABC) 中国农业银行	Technology & service implementation with users	Responsible for e-CNY exchange and circulation services, such as opening e-CNY accounts/digital wallets, promoting use of the e-CNY and e-CNY marketing campaigns; Investment in hardware and software infrastructure for retail e-CNY	◐
Commercial bank	 Bank of China (BOC) 中国银行	Technology & service implementation with users	Responsible for e-CNY exchange and circulation services, such as opening e-CNY accounts/digital wallets, promoting use of the e-CNY and e-CNY marketing campaigns; Investment in hardware and software infrastructure for retail e-CNY	◐
Commercial bank	 China Construction Bank (CCB) 中国建设银行	Technology & service implementation with users	Responsible for e-CNY exchange and circulation services, such as opening e-CNY accounts/digital wallets, promoting use of the e-CNY and e-CNY marketing campaigns; Investment in hardware and software infrastructure for retail e-CNY	◐
Commercial bank	 Postal Savings Bank of China (PSBC) 中国邮政储蓄银行	Technology & service implementation with users	Responsible for e-CNY exchange and circulation services, such as opening e-CNY accounts/digital wallets, promoting use of the e-CNY and e-CNY marketing campaigns; Investment in hardware and software infrastructure for retail e-CNY	◐
Commercial bank	 Bank of Communications (BOCOM) 中国交通银行	Technology & service implementation with users	Responsible for e-CNY exchange and circulation services, such as opening e-CNY accounts/digital wallets, promoting use of the e-CNY and e-CNY marketing campaigns; Investment in hardware and software infrastructure for retail e-CNY	◐
Commercial bank	 China Merchants Bank (CBM) 中国招商银行	Technology & service implementation with users	Responsible for e-CNY exchange and circulation services, such as opening e-CNY accounts/digital wallets, promoting use of the e-CNY and e-CNY marketing campaigns; Investment in hardware and software infrastructure for retail e-CNY	◐

















ACTOR TYPE*	NAME OF KEY ACTOR	DESCRIPTION	KEY TASK	PRIORITY
Commercial bank	 MYbank 蚂蚁金服网商银行	Technology & service implementation with users	Responsible for e-CNY exchange and circulation services, such as opening e-CNY accounts/digital wallets, promoting use of the e-CNY and e-CNY marketing campaigns; Investment in hardware and software infrastructure for retail e-CNY	
Commercial bank	 WeBank 腾讯微众银行	Technology & service implementation with users	Responsible for e-CNY exchange and circulation services, such as opening e-CNY accounts/digital wallets, promoting use of the e-CNY and e-CNY marketing campaigns; Investment in hardware and software infrastructure for retail e-CNY	
Commercial bank	 Industrial Bank 兴业银行	Technology & service implementation with users	Responsible for e-CNY exchange and circulation services, such as opening e-CNY accounts/digital wallets, promoting use of the e-CNY and e-CNY marketing campaigns; Investment in hardware and software infrastructure for retail e-CNY	
Corporation	 JD 京东	Internet service platform	Collaborate with certain operating institutions to jointly provide e- CNY circulation services; Provide a rich consumption scenario for the e-CNY trough their own large user bases; Promote the e-CNY by issuing online consumption vouchers	
Corporation	 Meituan 美团	Internet service platform	Collaborate with certain operating institutions to jointly provide e- CNY circulation services; Provide a rich consumption scenario for the e-CNY trough their own large user bases; Promote the e-CNY by issuing online consumption vouchers	
Corporation	 DiDi 滴滴	Internet service platform	Collaborate with certain operating institutions to jointly provide e- CNY circulation services; Provide a rich consumption scenario for the e-CNY trough their own large user bases; Promote the e-CNY by issuing online consumption vouchers	
Corporation	 Vipshop 唯品会	Internet service platform	Collaborate with certain operating institutions to jointly provide e- CNY circulation services; Provide a rich consumption scenario for the e-CNY trough their own large user bases; Promote the e-CNY by issuing online consumption vouchers	

Figure 5.2. – Actors to watch

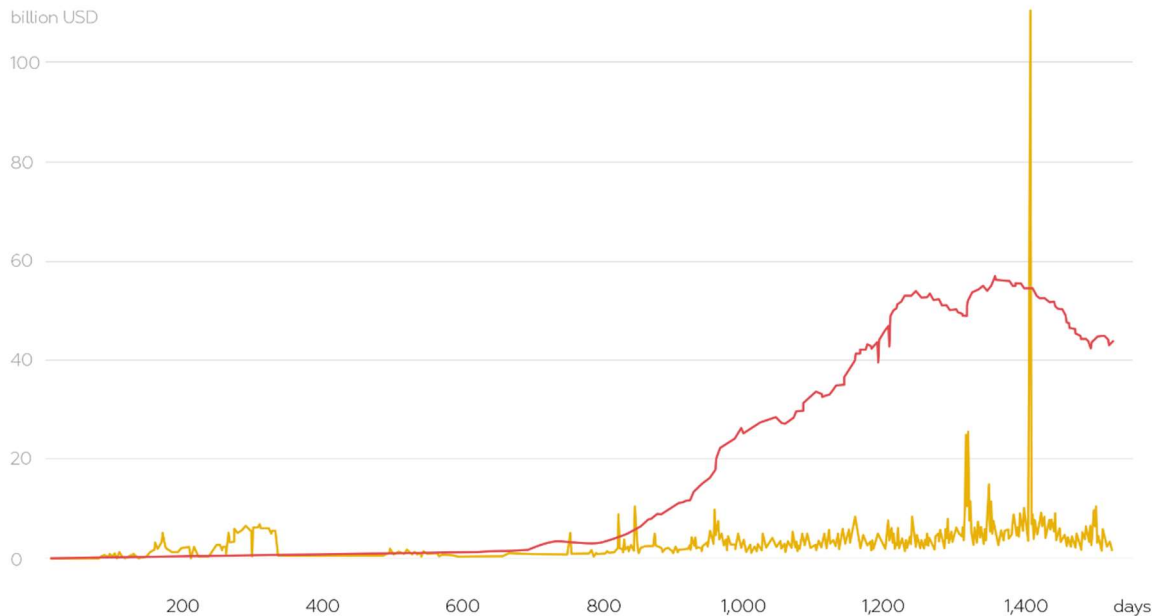


Figure 5.3. – USDC market cap (red) and volume trading (yellow)

The e-CNY's ultimate objectives are global in scope: it is intended to boost the RMB's adoption of cross-border payments. China's major cities will play a decisive role in implementing transnational financial ecosystems and promoting the e-CNY internationally.¹³⁵ The megacity Chong Qing, for example, features a crucial transnational link with the Chongqing (China-Singapore) Demonstration Initiative on Strategic Connectivity, which involves business travel, talent training, medical care and shopping malls using the digital RMB. The goal is

to use the digital RMB for "trade and exchanges between western China and Southeast Asian countries to improve cross-border settlement efficiency".¹³⁶ Hong Kong, the international financial centre in the middle of the Greater Bay Area, with its population of 70 million and gross domestic product of US\$ 1.7 trillion in 2019, could also become a significant promotion hub for the e-CNY. Given the restrictions inside China, Hong Kong is poised to become a vibrant centre for the use of the e-CNY in international settlements.¹³⁷

¹³⁵ Chinese cities became crucial global actors in promoting transnational technological, trade, and other linkages. See e.g. Dominik Mierzejewski, "The role of Guangdong and Guangzhou's Subnational Diplomacy in China's Belt and Road Initiative", *China: An International Journal*, vol. 18, no. 2 (May 2020), pp. 99–119, <doi: 10.1353/chn.2020.0018>; Yonghui Han et al., "The Belt and Road Initiative, Sister-city Partnership and Chinese Outward FDI", *Economic Research-Ekonomska Istraživanja*, vol. 35, no. 1 (November 2021), pp. 3416–3436, <doi: 10.1080/1331677X.2021.1997618>; Helen Wei Zheng et al., "Interrogating

China's global urban presence", *Geopolitics*, March 2021, <doi: 10.1080/14650045.2021.1901084>.

¹³⁶ Ran Zheng, "Chongqing activates more than one million digital RMB wallets", *Chongqing International Communication Center (for Culture and Tourism)*, 21 May 2022, <<https://www.ichongqing.info/2022/05/21/chongqing-activates-more-than-one-million-digital-rmb-wallets/>>.

¹³⁷ Kelly Le, "Hong Kong may be first global 'sandbox' for China's DCEP digital yuan", *forkast*, 17 December 2020, <<https://forkast.news/hong-kong-pilot-test-china-dcep-digital-currency/>>; Zhang Tianyuan (note 131).



The e-CNY and the four dimensions of Open Strategic Autonomy

Growing international use of the e-CNY would affect all four dimensions of Europe's Open Strategic Autonomy.

The resilience of value chains

China is striving not only to make the digital yuan an effective domestic tool for consumers' retail payments but also to integrate the yuan as a payment currency into the global financial system. The world's largest cross-border multi-country payment trial, the mBridge project, which concluded in October 2022, indicated that CBDCs are a viable means of making real-time cross-border payments and foreign exchange transactions at low cost and high speed, and in a less complex, more transparent manner.¹³⁸ At first glance, a stronger e-CNY would not directly affect the security and resilience of supply chains. Ideally, the e-CNY strengthens the Chinese government's ability to monitor capital flight and money laundering, thereby improving international supply chain sustainability. If the ECB maintains its sluggish approach to developing the digital euro, European companies might come under increasing pressure to use non-European CBDCs, not least for trading with Chinese companies. This approach could weaken their position in evolving supply chains, as they would suffer from a loss of efficiency and higher cost of business operations. If more of China's international trading partners were to adopt the digital

yuan, this scenario would become far from unrealistic.

National security

The broader national security concerns around the e-CNY are connected with the future of the euro and Europe's monetary sovereignty, and the potential for detrimental changes to the international political economy. China is powering ahead with its CBDC at a time when the rest of the world is just starting to explore future opportunities for economic systems. Internationally, it aims to convert a share of US dollar-denominated exports into RMB-based exports. Combined with the global presence of Chinese e-commerce platforms, the e-CNY could promote a more expeditious transition than is often assumed. Widespread adoption of the e-CNY could give rise to global financial transactions and settlements, circumnavigating the US monetary system.¹³⁹ Hence, the e-CNY as a financial tool could promote considerable change within the global financial system that might weaken the influence of economies in the transatlantic region. Many countries, especially in Southeast Asia, are already considering diversifying their foreign currency reserves, offering opportunities for RMB internationalization. In addition, states are accelerating their efforts to reduce their use of the US dollar by setting up RMB clearing arrangements.¹⁴⁰

¹³⁸ Bank for International Settlement Innovation Hub (note 124).

¹³⁹ Nicola Bilotta, "An international digital yuan: (Vane) ambitions, (Excessive) alarmism and (pragmatic)

expectations", IAI Commentaries 21/44, Istituto Affari Internazionali, Rome, 2021; Rajesh Bansal and Somya Singh (note 130); Ryan Heath (note 133).

¹⁴⁰ Zhang Tianyuan (note 131).



The official policy goal behind the e-CNY is not to supplant the US dollar as the dominant global currency,¹⁴¹ but to reduce dollar dependence by establishing an alternative payment architecture. The e-CNY is a deft technological move by the Chinese government to gain increased autonomy and minimize the political risks associated with US dollar intermediation, as well as the potential impact of US sanctions. Whereas China's Cross-Border Inter-Bank Payments System (CIPS) has thus far failed to establish a genuine alternative to the western-centric Society for Worldwide Interbank Financial Telecommunication (SWIFT), several multi-CBDC arrangements "may spur the adoption of the CIPS by implementing the e-CNY",¹⁴² allowing China to bypass SWIFT. Ultimately, if a sufficient number of banks accept international payments in e-CNY, the Chinese government could pre-emptively undermine the effectiveness of US primary and secondary sanctions.¹⁴³

Europe's aim of Open Strategic Autonomy makes developing an effective response to the e-CNY without impeding vital trade relations essential. The euro's popularity is currently increasing as countries search for alternatives to the US dollar in order to gain greater independence from the US. However, rapid and mass adoption of the e-CNY could threaten the financial position and popularity of the euro as the second most traded currency. It should be noted that the SWIFT system, based in

Belgium, is arguably the only infrastructure node of global relevance located in Europe. If the e-CNY becomes an alternative payment system with hundreds of millions of wallet holders, Europe will lose its single financial "choke point" and financial data security will be weakened. The PBOC's capacity to gather information on financial flows – including international financial transfers from China-Europe trade and other third parties using the e-CNY – would considerably increase.

Values and Sustainability

The success of digital currencies depends on the strength of institutions and the level of trust in public policy, particularly the legal and regulatory environment in the areas of currency convertibility and capital account liberalization, as well as the sophistication of financial ecosystems and the robustness of legal and regulatory frameworks. Individual users value key attributes such as safety, security, reliability and ease of use when interacting with the CBDC system. Hence, apprehension is mounting about the ownership and use of personal financial data arising from transactions in digital currencies. On the digital euro, the EU must decide to what extent personal data can be collected, for how long this can be retained, how such data can be used and for whose benefit, and what safeguards will be put in place to protect against abuses.¹⁴⁴

¹⁴¹ Nicola Bilotta (note 139).

¹⁴² Elijah J. Fullerton and Peter J. Morgan (note 123).

¹⁴³ Jan Knoerich, "China's new digital currency: Implications for yuan internationalization and the US dollar", in Nicola Bilotta and Fabrizio Botti (eds), *The*

(Near) Future of Central Bank Digital Currencies: Risks and Opportunities for the Global Economy and Society, Bern, Peter Lang, 2021, pp. 145–166, p. 160.

¹⁴⁴ Hung Tran (note 126).



Privacy is a core value for EU citizens and a central driver of the acceptability of and trust in currencies. However, privacy conflicts with other, equally valid policy objectives on which the EU is a world leader, such as the fight against money laundering and the financing of terrorism, as well as tax evasion. Moreover, concerns about using personal transaction data correlate with securing personal data privacy in an increasingly digitalized world. For example, a Chinese-centred digital currency system would confer panoptical power over personal financial data on the Chinese Communist Party. Similarly, the design and governance of blockchain applications are typically “embedded institutionally within a frame of public utility service infrastructure and national strategic objectives”.¹⁴⁵ Europe has robust legal and regulatory safeguards in place to protect against abuses of personal data by companies and governments, but digital currencies pose a new challenge to the General Data Protection Regulation, the Digital Markets Law and the Digital Services Law.¹⁴⁶

The e-CNY and the digital euro are based on similar technological features but rooted in divergent political, legal and regulatory regimes and underlying visions. Globally, the differences between a stakeholder model and a state-centric model are less

apparent than in the case of Internet governance. The centralized technical structure of CBDCs cuts out intermediaries in a manner that differs from decentralized cryptocurrencies and advantages governments and central banks. The current lack of global norms surrounding CBDCs, for example, regarding privacy standards for international e-currency transactions and the absence of regulatory competition from the US and the EU enable China to engage with governments and banks on piloting technical interfaces and standards by building on ample domestic experience with the e-CNY.¹⁴⁷

Technological competitiveness

Implementation of the e-CNY has various ramifications for Europe’s technological competitiveness. First, China is in a leadership position thanks to the expertise gained from experimenting with new forms of digital money and payment systems. China’s experience offers a rich set of examples and insights into how a balance between fintech innovation and regulation might be pursued, including the thorny issue of technology choices as detailed in the 2021 White Paper published by the PBOC.¹⁴⁸ The right policy mix is a critical ingredient in the successful digitalization of money.¹⁴⁹ Moreover, because various private and public sector actors with

¹⁴⁵ Gary Sigley and Warwick Powell (note 118). See also Steven-Jiawei Hai and Robyn Klingler-Vidra, “Chinese blockchain: Convergence around a Beijing-aligned strategy”, *Global Policy*, King’s College, London, August 2022, <<https://www.globalpolicyjournal.com/sites/default/files/pdf/Hai%20and%20Klingler-Vidra%20-%20Chinese%20blockchain%2C%20convergence%20around%20a%20Beijing-aligned%20strategy.pdf>>.

¹⁴⁶ Hung Tran (note 126); Markus K. Brunnermeier and Jean-Pierre Landau, “The digital euro: Policy implications and perspectives”, European Parliament, Committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, Luxembourg, 2022.

¹⁴⁷ Ryan Heath (note 133).

¹⁴⁸ Working Group on E-CNY Research and Development of the People’s Bank of China (note 122).

¹⁴⁹ Martin Chorzempa and Yiping Huang (note 119).



cryptography and computer science expertise can create money, currency competition could develop inside and across borders. Some countries use their digital networks to circulate their currencies/stablecoins in other jurisdictions. Hence, the primary rationale for developing a national digital currency is to preserve the role of public money in a digital economy.¹⁵⁰

Second, the PBOC has gained visible leadership in the global landscape of CBDCs. China has leveraged its economic power to shape and foster practices and standards constituting the multilateral CBDC space. The synchronized development of

several national CBDCs could advance a new payment network based on multi-CBDC arrangements in which nodes are more independent of the US dollar.¹⁵¹ Based on this supposition, the PBOC has established international cooperation and trials around its CBDC (see Figure 5.4).¹⁵² In addition, the bank has proposed global rules to empower essential interoperability between CBDCs issued by different jurisdictions.¹⁵³ China is following a known pattern of seeking “*portfolio diversification*, not the replacement of institutions and systems”.¹⁵⁴ In so doing, China can build on its existing web of currency swaps of RMB 3.54 billion with more than 40 states.

NAME	MULTIPLE CBDC	HONG KONG PILOT COOPERATION	CHINA-SINGAPORE (CHONGQING) DEMONSTRATION INITIATIVE ON STRATEGIC CONNECTIVITY (CCI)
Partners	Bank for International Settlements Innovation Hub in Hong Kong, together with the Hong Kong Monetary Authority, Bank of Thailand, Central Bank of the United Arab Emirates and the Digital Currency Institute of the People's Bank of China	Hong Kong Monetary Authority, Digital Currency Institute, Research Unit of the PBOC	Industrial and Commercial Bank of China (ICBC), Agricultural Bank of China (ABC), Bank of China (BOC), SASSEUR Group, Sino-Singapore Cancer Center (SSCC), New Land-sea Corridor Operation Co., Ltd., China-Singapore (Chongqing) Fintech Cooperation Demonstration Zone
Time	2021–2022	2021–	2022–

Figure 5.4 – International pilot projects on cross-border transactions

¹⁵⁰ Markus K. Brunnermeier and Jean-Pierre Landau (note 146).

¹⁵¹ Nicola Bilotta (note 139).

¹⁵² Eliza Gkritski, “China, Hong Kong enter second phase of cross-border digital Yuan trials: Report”, *Coindesk*, 9 December 2021, <<https://www.coindesk.com/policy/2021/12/09/china-hong-kong-enter-second-phase-of-cross-border-digital-yuan-trials-report/>>.

¹⁵³ Tom Wilson and Marc Jones, “China proposes global rules for Central Bank digital currencies”, Reuters, 25 March 2021, <<https://reut.rs/3si5OH4>>; Martin Chorzenia (note 116).

¹⁵⁴ Evan A. Feigenbaum, “Reluctant stakeholder: Why China’s highly strategic brand of revisionism is more challenging than Washington thinks”, in Damien Ma (ed.), *China’s Economic Arrival*, Singapore, Palgrave Macmillan, pp. 117, 2020. (Emphasis in original).



Third, the Chinese government believes that the e-CNY has the potential to contribute to one of its crucial policy objectives and ambitions: the internationalization of the RMB.¹⁵⁵ However, the monetary and financial interlinkage between China and global markets has a complicated history.¹⁵⁶ Given the size of the Chinese economy and its role in world trade, the RMB continues to underperform as an international currency.¹⁵⁷ Consequently, the Chinese economy remains highly dependent on the US dollar for global trade and investment.¹⁵⁸ Because of the possibility of monitoring, digital networks and multi-CBDC arrangements could ease the internationalization of the currency as a means of payment in trade links. However, the e-CNY is unlikely to lead to a sea change in the RMB's stalled internationalization as capital

Policy recommendations

China has gained a first-mover advantage by implementing a central bank digital currency while Europe plays catch-up and

controls will be maintained and international trust in the institutions governing the RMB remains low.

Finally, the e-CNY could become a vehicle for extending Chinese blockchain infrastructures globally. In 2020, Zhou Xiaochuan, the former governor of the PBOC, stated that: "Blockchains and DLT have always been part of the PBOC's toolkit to establish a digital currency system".¹⁵⁹ As the Chinese government systematically promotes blockchain technologies,¹⁶⁰ they will likely be employed in multiple ways to facilitate the new payment architecture and its embedding within China's "smart society".¹⁶¹ For instance, blockchain servers can manage digital currency wallet addresses, supervision of transaction information and the transaction supervision of digital bills.¹⁶²

assesses the risks, opportunities and national security implications of creating such a currency. Importantly, the e-CNY in

¹⁵⁵ Yuan Zhang, "A review of the impact of Central Bank Digital Currency on Currency Internationalization", *Proceedings of the International Conference on Urban Planning and Regional Economy (UPRE 2022)*, 2022, <doi: 10.2991/aebmr.k.220502.089>; Shen, Chunming, "Digital RMB, RMB Internationalization and Sustainable Development of the International Monetary System", *Sustainability*, vol. 14, no. 10 (May 2022), <doi: 10.3390/su14106228>.

¹⁵⁶ Ho-fung Hung, *The China Boom: Why China Will Not Rule the World*, New York, Columbia University Press, 2015.

¹⁵⁷ Vita Spivak, "Can the yuan ever replace the dollar for Russia?", *Carnegie Endowment for International Peace*, 2021, <<https://carnegiemoscow.org/commentary/85069>>.

¹⁵⁸ See Hofung Hung, "China: Saviour or Challenger of the Dollar Hegemony?", *Development and Change*, vol. 44, no. 6 (November 2013), pp. 1341–1361, <doi: 10.1111/dech.12063>.

¹⁵⁹ Zhou Xiaochuan (note 128).

¹⁶⁰ Mike Knapp, "The United States is Behind the Curve on Blockchain", *War on the Rocks* <<https://warontherocks.com/2022/08/the-united-states-is-behind-the-curve-on-blockchain/>>.

¹⁶¹ Xiaohong Chen et al., "Digital technology-driven smart society governance mechanism and practice exploration", *Frontiers of Engineering Management*, 12 September 2022, <doi: 10.1007/s42524-022-0200-x>.

¹⁶² See Fintech Research Feature: Detailed Explanation of Digital RMB, "金融科技研究专题：详解数字人民币、三个关键问题解答和投资机会分析" ["Fintech Research Special: Detailed Explanation of Digital RMB, Three Key Questions Answered and Investment Opportunity Analysis"], SINA, <https://stock.finance.sina.com.cn/stock/go.php/vReport_Show/kind/search/rpt/id/692140407978/index.phtml>.



- To protect the resilience of its value chains, Europe should speed up the development of its digital euro and issue it to protect the EU's financial/monetary autonomy and avoid a rival digital currency controlled by a non-European country or big tech company taking hold in Europe.
- To safeguard national security, the ECB should monitor the effects of domestic and international e-CNY developments on tech, policy and regulations. Perhaps a scenario for after 2030, the EU should prepare for a growing tide of countries engaging in e-CNY cooperation, and a possible progressive switch away from the US dollar for certain types of transactions, such as oil and gas.
- To maintain technological competitiveness, Europe should begin pilot projects between the European Central Bank, the PBOC and the Hong Kong Monetary Authority, as well as other central banks. Moreover, a European understanding of Chinese capacities, design choices and approaches to standard setting will be paramount in enabling fast exchanges/settlements between the e-CNY and the e-euro for companies.
- To defend its values, Europe should lead international efforts to foster

norms on central bank digital currencies around security, financial data privacy and the rule of law.

Despite mounting anxieties about China's digital power, it is worth stressing that the RMB's lack of progress on internationalization stems from the fact that it is not freely convertible and is subject to capital controls. The e-CNY could boost the internationalization of the RMB but currency digitalization does not make up for its original flaws, such as policies that deliberately reduce foreign access to e-CNY-denominated investments.¹⁶³ The attractiveness of an international currency depends on macroeconomic conditions, the openness and transparency of financial markets, and the credibility of the issuing country's political institutions. These factors currently limit the RMB's international status.¹⁶⁴ While the fast progress of the e-CNY should inspire the ECB to advance its own CBDC project more quickly, the yuan's long-lasting disadvantages will not disappear overnight. These shortcomings will allow Europe to consider a more comprehensive response. However, even though the e-CNY is unlikely to replace the US dollar as a world reserve currency any time soon, the tensions between the US and China around financial infrastructures and payment systems are likely to grow and significantly impact European companies.

¹⁶³ Vita Spivak (note 157); Maximilian Kärfelt, "The Digital Yuan Will Only Lend a Minor Boost to Internationalization of the Currency", MERICS, 16 November 2020, <<https://merics.org/de/kurzanalyse/digital-yuan-will-only-lend-minor-boost-internationalization-currency>>.

¹⁶⁴ Rajesh Bansal and Somya Singh (note 130); Yiping Huang et al., "Paths to a Reserve Currency: Interna-

tionalization of the Renminbi and its Implications", *ADB Working Papers* no. 482, Asian Development Bank, 2014; Jimmy Choi, "RCEP and renminbi's role as a reserve currency", *Central Banking*, 8 December 2022, <<https://www.centralbanking.com/central-banks/reserves/foreign-exchange/7953921/rcep-and-renminbis-role-as-a-reserve-currency>>



Authors:

Amir Elalouf is Head of the Technology Management Program and a lecturer and researcher in the department of management at Bar-Ilan University, Israel. Contact: amir.elalouf@biu.ac.il

Maximilian Mayer is an Assistant Professor of International Relations and Global Politics of Technology at the Center for Advanced Security, Strategic and Integration Studies (CASSIS), University of Bonn, Germany. Contact: maximilian.mayer@uni-bonn.de





Chinese Vehicle-to-Everything (V2X) Technology and the European Car Industry

Sanne van der Lugt, Raúl Rojas and Frans-Paul van der Putten

Abstract

The European Union car manufacturing industry does not currently appear to be dependent on Chinese suppliers of vehicle-to-everything (V2X) technology. But given the scale and pace of application of V2X in China, it is possible that Chinese companies could eventually become highly competitive internationally. This could present various risks for EU strategic autonomy, in particular with regard to supply chain resilience and technological competitiveness. National security and values-related risks also require serious attention. That said, the evolution of Chinese V2X technology could also provide opportunities for the EU to strengthen its strategic autonomy. Provided that Chinese suppliers do not become dominant, that Chinese standards are open and developed jointly with non-Chinese actors and that EU car user data is protected from access by the Chinese government, the EU could benefit from European-Chinese cooperation on accelerating the transition to electric driving and smart mobility, maintain an innovative and competitive car industry, and mitigate strategic dependence on US technology firms.

Traditional carmakers worldwide are under pressure to reinvent themselves. They need to become software-driven companies capable of competing in a fast-changing market shaped by four megatrends: next-generation connectivity, autonomous technologies, electrification and novel shared mobility concepts. In the highly interconnected automotive sector, European carmakers partner with technology companies from various parts of the world, including China. A recent study found that

German carmakers are likely to increasingly switch to Chinese suppliers in order to remain globally competitive. Batteries, autonomous driving and car software are fields that are developing rapidly in China.¹⁶⁵ Chinese battery manufacturers already play a leading role in electric driving.

Artificial Intelligence (AI) and the internet-of-things (IoT) are becoming increasingly

¹⁶⁵ Gregor Sebastian, "The Bumpy Road Ahead in China for Germany's Carmakers", MERICS, 27 October 2022,

<<https://merics.org/en/report/bumpy-road-ahead-china-germanys-carmakers>>.



important to the car industry.¹⁶⁶ While the IoT enables vehicles to communicate with each other and with their physical environment, AI aims to make it possible for cars and roadside equipment to mine that interaction in order to reach decisions autonomously of human operators. Both AI and the IoT are required for vehicle-to-

everything (V2X) systems,¹⁶⁷ which enable connected automated driving and smart mobility. This chapter provides a preliminary assessment of the relevance of Chinese V2X technology to the automotive industry in the EU, and how it could affect European strategic autonomy.

European and Chinese Approaches to Artificial Intelligence and the internet-of-things, and vehicles

Increasingly, vehicles on the road collect all kinds of data. This aspect of V2X helps to improve autonomous driving technologies but V2X could also play a significant role improving traffic efficiency, saving resources, reducing pollution, reducing the frequency of accidents and improving traffic management – especially in combination with advanced driver-assistance systems (ADAS). State-of-the-art ADAS technology can assist drivers while driving, changing lanes, handling obstacles on the road and parking. It relies on video cameras, radar/lidar and ultrasonic sensors to detect obstacles and assist path planning. V2X as an interaction technology relies on messages sent from other entities, such as

other vehicles or infrastructure. ADAS and V2X are steadily evolving from just issuing warnings to the driver, who can then react, to taking partial or full control of the vehicle.

Any V2X system is essentially limited by network economies: it relies on adoption of the technology by a critical mass of users in order to develop its full potency.¹⁶⁸ A basic common standard is also needed to ensure that all new vehicles and services can share critical information. For V2X, two major technology directions have been widely adopted: Dedicated Short Range Communications (DSRC), derived from Wi-Fi,¹⁶⁹ and cellular V2X (also known as

¹⁶⁶ While AI refers to a set of methods and algorithms that can be implemented by software to perform operations, IoT refers to the information and communications methods, algorithms and software, as well as the physical infrastructure that allow devices to be connected to cloud servers or internet access points, often through wireless communications. Carlo Fischione, Sanne van der Lugt and Frans-Paul van der Putten, "AI and IoT Developments in China and the Relevance for EU Policy: A scoping study", *Digital Power China*, January 2022, pp. 47–64.

¹⁶⁷ The letter V stands for vehicles and X for anything that interacts with them. Currently, the X mainly comprises other vehicles (V2V), people (V2P and P2V), roadside infrastructure (V2I and I2V) and networks

(V2N, V2N2V and N2V). V2N refers to the connection between the on-board device in a vehicle and the cloud platform through a network. The cloud platform interacts with the vehicle. It also stores and processes the acquired data, and provides remote traffic information, entertainment, business services and vehicle management. V2N/V2C is mainly applied to vehicle navigation, vehicle remote monitoring, emergency rescue, information entertainment services, etc.

¹⁶⁸ Graham Jarvis, "Limitations of ADAS, V2V and V2X Communications", *Urgent Communications*, 19 April 2022, <<https://urgentcomm.com/2022/04/19/limitations-of-adas-v2v-and-v2x-communications/>>.

¹⁶⁹ Using the IEEE 802.11p standard for wireless access in vehicular environments.



C-V2X), derived from cellular modem technology.¹⁷⁰

These technologies target a global solution with a unified series of short-range communication protocol designs, but they constitute different standards. The main advantage of DSRC is that it is based on widely used technologies that are already deployed and have been thoroughly tested. C-V2X cannot be fully implemented yet because of a lack of 5G networks. In addition, C-V2X is expected to be more expensive as cellular carriers will charge for the use of their networks. However, the higher bandwidth and ultra-low latency capabilities on which autonomous driving relies will only be provided by 5G infrastructure, and therefore C-V2X, which is rolling out across the world but will not be ubiquitous or even widely available, let alone embedded in vehicles, for many years. It is possible that the full potential of mobile infrastructure for the automotive sector will be realized only with the introduction of 6G (see chapter 3 in this volume). The arrival of national 5G coverage in some markets, however, has resulted in car makers moving forward with the development of technologies and solutions that rely on 5G connectivity.¹⁷¹

¹⁷⁰ Using 3GPP standardized 4G LTE or 5G mobile cellular connectivity. On DSRC and C-V2X see Mikael Fallgren et al., "Introduction", in Fallgren et. al. (eds), *Cellular V2X for Connected Automated Driving*, Hoboken: John Wiley & Sons, 2021, p. 10.

¹⁷¹ "From here to Autonomy: How to fulfil the requirements of the next generation connected car", *Quectel*, 2021, accessed 13 December 2022 at

European Union

In April 2019, the European Commission issued a Delegated Act that identified DSRC as the standard for automotive communication. The act defines a hybrid approach: endorsing the ITS-G5 (DSRC-related) standard as the baseline technology for direct vehicle-to-vehicle and vehicle-to-infrastructure communication, while using long-term evolution (LTE), a standard for wireless broadband communication, and 5G cellular technology for additional communication to remote infrastructure and cloud services. In Europe, initial 5G applications will address logistics, medical and fixed broadband markets, but not smartphone users. This makes the connected car industry critical for 5G stakeholders. While most smartphone users will wait a few years to get a 5G enabled handset, car makers are a huge and exciting market for the new networks.¹⁷²

According to the 2025 road map of the European New Car Assessment Programme (Euro NCAP), an organization that conducts safety tests on vehicles, V2X features will be necessary to achieve an NCAP 5-star rating after 2024, just as airbags, ABS and driver-assistance systems are today. Currently, 97% of the new vehicles sold in Europe are Euro NCAP rated, and 89% of new vehicles have 4- or 5-star ratings. Any technology added to Euro NCAP reaches

<<https://www.quectel.com/wp-content/uploads/2021/08/Quectel-Auto-WPFINAL.pdf>>.

¹⁷² Pablo Valerio, "The 5G lobby wins: EU Council stops WiFi standard for V2X", *IoT Times*, 15 July 2019, accessed 13 December 2022 at <<https://iot.eetimes.com/the-5g-lobby-wins-eu-council-stops-wifi-standard-for-v2x/>>.



nearly all new vehicles within a few years of receiving a rating. It is likely that the same outcome will be replicated for V2X. All carmakers with brands on the European market would then need to include V2X in their vehicles to achieve the highest ratings.¹⁷³

China

China is the world's largest car market. Moreover, one in four new cars sold in China is either an electric vehicle or a hybrid, and the number of electric car sales in China in 2022 is expected to be higher than in the rest of the world combined.¹⁷⁴ China currently has a larger number of V2X-equipped cars than any other market, including the EU.¹⁷⁵ Although China's entry into the global automotive market has not been meteoric, it has progressed swiftly in recent decades. The country's car exports are growing fast but Chinese brands still play only a limited role abroad. Instead of promoting their own vehicles on the European market, Chinese carmakers have bought struggling European

companies. For instance, Zhejiang Geely Holding Group, which has an AI company dedicated to the automotive sector,¹⁷⁶ owns Volvo and Lotus. It also has a 10% stake in Daimler Benz.

Domestically, the Chinese government has embarked on mass-deployment of C-V2X.¹⁷⁷ China's national strategy (the 14th Five-year Plan, 2021–2025) calls for national V2X coverage by 2025, with a spectrum allocated specifically to LTE-V2X. This provides the conditions for rapid local industrial development moving towards commercialization. The aim of the strategy is that China should lead the world in intelligent connected vehicles within 15 years by providing full coverage spatio-temporal information and transportation perception.¹⁷⁸ The 'New Infrastructure' campaign, launched by the Chinese government to boost local economies, promotes substantial growth in V2X-enabled infrastructure across the country. C-V2X is the technology of choice in China. As the world's largest automotive market, this could have an impact on other regions

¹⁷³ Onn Haran and Ram Shallom, "V2X Technology Trends and Market Evolution in Europe and China", Autotalks, no date, accessed 13 December 2022 at <<https://auto-talks.com/v2x-technology-trends-and-market-evolution-in-europe-and-china/>>.

¹⁷⁴ Daisuke Wakabayashi and Claire Fu, "For China's auto market, Electric isn't the future, it's the present", *New York Times*, 26 September 2022, <<https://www.nytimes.com/2022/09/26/business/china-electric-vehicles.html>>.

¹⁷⁵ Quectel, (note 171).

¹⁷⁶ Guangyu Mingdao Digital Technology Co, based in Qingdao.

¹⁷⁷ C-V2X was developed within the 3rd Generation Partnership Project (3GPP) as an alternative to the US Dedicated Short-Range Communications (DSRC). C-V2X can function without network assistance. Murray Slovick, "DSRC vs. C-V2X: Looking to impress the regulators", *Electronic Design*, 6 October 2017,

<<https://www.electronicdesign.com/markets/automotive/article/21805671/dsrc-vs-cv2x-looking-to-impress-the-regulators>>. After months of debate, in November 2020 the US Federal Communications Commission (FCC) voted to allocate 75MHz of the spectrum band (5.850-5.925GHz), which had previously been reserved for DSRC services, to Wi-Fi and C-V2X uses, which means the US has given up DSRC and turned to C-V2X. Research and Marketing, "Global and China V2X (Vehicle to Everything) and CVIS (Cooperative Vehicle Infrastructure System) Industry Report 2021", *Business Wire*, 29 June 2021, <<https://www.businesswire.com/news/home/20210629005648/en/Global-and-China-V2X-Vehicle-to-Everything-and-CVIS-Cooperative-Vehicle-Infrastructure-System-Industry-Report-2021---ResearchAndMarkets.com>>.

¹⁷⁸ Research and Marketing (note 177).



and regulators in Europe, Japan and the US.

China has more test fields with more cross-industry companies participating in deployment of C-V2X than either the United States, Europe or Japan.¹⁷⁹ The Shanghai pilot zone was the first and is the most advanced intelligent and connected vehicle (ICV) test zone in China. It has 15 kms of closed roads, 73 kms of open test roads and an urban roads demonstration zone of 100 km². The closed test zone can conduct testing of up to 200 vehicles. The urban roads demonstration zone can provide more than 200 test scenarios, including autonomous driving, efficiency and C-V2X tests.

In April 2021, the Chinese government announced the first six pilot cities for intelligent and connected vehicles: Beijing, Shanghai, Guangzhou, Wuhan, Changsha and Wuxi. The pilot cities were asked to build intelligent infrastructure, enhance

Case study: Huawei

The movement towards connectivity in driving brings together the automotive industry and the mobile telecommunications industry. On the Chinese technology side, a company that covers almost all the aspects required for the digital transformation of vehicles is Huawei, a global leader in

network connectivity and explore the functionality of the Chinese “vehicle-road-cloud” platform. In December 2021, a further 10 cities were selected by the Chinese government as the second set of pilot cities for ICV (Chongqing, Shenzhen, Xiamen, Nanjing, Jinan, Hefei, Chengdu, Cangzhou, Wuhu and Zibo). Specific goals were set for each city. For example, the target for Chongqing is to implement ICV technologies in public transport for the benefit of the tourist industry; the target for Nanjing is to explore the functions of ICV for the customer; and the target for Jinan is to combine ICV technologies with the agricultural logistics industry.



















Given the dynamic unfolding of China’s approach, Figure 6.1 summarizes the most relevant actors that European policymakers should monitor in order to understand the most important technological and policy developments in the PRC.

telecommunications technology. It provides technology aimed at automotive perception and decision making, network communications, electric drive, batteries, electronic control, cloud-road networks outside vehicles, R&D and marketing.¹⁸⁰ In 2017, Huawei, together with China Mobile

¹⁷⁹ Tao Cui et al., “C-V2X Vision in the Chinese Roadmap: Standardization, field tests, and industrialization”, in Abdelfatteh Haidine (eds), *Vehicular Networks: Principles, Enabling Technologies and Perspectives* [working title], 21 November 2022, accessed 13 December 2022 at <<https://www.intechopen.com/online-first/83991>>.

¹⁸⁰ Research and Markets, “Global and China Automotive LiDAR Industry Report 2021: Application fields, technology and trends, companies and products”, *Business Wire*, 23 June 2021, <<https://www.globenewswire.com/en/news-release/2021/06/23/2251484/28124/en/Global-and-China-Automotive-LiDAR-Industry-Report-2021-Application-Fields-Technology-and-Trends-Companies-and-Products.html>>.



ACTOR TYPE	NAME OF KEY ACTOR	DESCRIPTION	KEY TASK	PRIORITY
Corporation	 Qualcomm (移远通信)	Innovation (non-state actor)	Collaboration with Qualcomm Technologies to offer advanced and smart connections to vehicles, including 5G, LTE/LTE-A, C-V2X; In January 2020 Qualcomm's AG15 C-V2X module was announced as supporting Hongqi's E-HS9 vehicle and Buick's GL8 Avenir by providing intelligent connectivity, making them the world's first commercialized production vehicles to feature LTE-V2X technology	
Corporation	 Huawei (华为)	Innovation (non-state actor)	Cloud service, Edge intelligence, V2X, Awareness (LiDAR)	
Corporation	 Alibaba (阿里巴巴)	Innovation (non-state actor)	Edge intelligence, autonomous driving services	
Corporation	 Tencent (腾讯)	Innovation (non-state actor)	Autonomous driving services	
Corporation	 Baidu (百度)	Innovation (non-state actor)	Apollo Open Autonomous driving platform, an open platform designed to foster innovation and speed up the development and rollout of autonomous driving technology through collaboration with industry partners	
Corporation	 SIMCom (芯讯通)	Innovation (subsidiary of Sunsea AIoT Technology, a non-state actor)	SIMCom 5G modules in the SIM8200 series are powered by Qualcomm's latest 5G NR modem Snapdragon X55 platform	
Policy institution	 National Development and Reform Commission (NDRC) (国家发展和改革委员会)	Overall coordination of smart roads (state actor)	Policy coordination	
Policy institution	 Ministry of Industry and Information Technology (中华人民共和国工业和信息化部)	Smart roads and telecom (state actor)	Regulation	
Policy institution	 Ministry of Transport (中华人民共和国交通运输部)	Smart roads: physical (state actor)	Policymaking	



ACTOR TYPE	NAME OF KEY ACTOR	DESCRIPTION	KEY TASK	PRIORITY
Association	 China Industry Innovation Alliance for Intelligent and Connected Vehicles (CAICV) (中国智能网联汽车产业创新联盟)	Industry alliance affiliated with a state actor (Ministry of Industry and Information Technology)	Promote the development of ICV Industry in China	
Research institute	 China Intelligent and Connected Vehicles (Beijing) Research Institute Co., Ltd (CICV) (北汽(北京)智能网联汽车研究院有限公司)	Research institute created by two car industry associations (China SAE and CAAM) and CAICV (an industry alliance affiliated with a state actor)	Promote the development of ICV Industry in China and the global value chain	
Platform	 IMT-2020 (5G) Promotion Group (IMT-2020(5G)推进组)	5G cooperation and promotion platform established by state actors (Ministry of Industry and Information Technology, National Development and Reform Commission, Ministry of Science and Technology)	Promote the development of 5G technologies in China and facilitate cooperation with foreign companies and organizations	

Figure 6.1 – Major technological and policy actors in China

and the Shanghai Automotive Industry Corporation (SAIC), demonstrated the world’s first 5G-based remote driving on a commercially available vehicle. For the demonstration, Huawei provided the 5G wireless solution, SAIC provided the smart concept car and China Mobile provided the 5G connectivity. Two years later, Huawei launched the world’s first 5G car module at the Shanghai Auto Show: the MH5000 module, based on its Balong 5000 5G chip.

Huawei has been explicit about its ambitions in the car industry. According to its rotating chair, Xu Zhijun (Eric Xu), the auto-

otive sector is increasingly becoming an ICT sector,¹⁸¹ which “doesn’t need the Huawei brand, but instead, needs our ICT expertise to help build future-oriented vehicles”.¹⁸² Huawei set up an “Internet of Vehicles Division” in 2013, starting with the automotive communication module ME909T. The company started developing an autonomous driving communication architecture in 2015, and has rolled out the autonomous driving AI chip “Ascend”, the Ascend-based intelligent driving computing platform MDC, the intelligent driving cloud service “Octopus” and the intelligent driving operating system

¹⁸¹ Juan Pedro Tomás, “Huawei launches 5G powered hardware for self-driving cars”, *RCR Wireless News*, 23 April 2019, <<https://www.rcrwireless.com/20190423/5g/huawei-launches-5g-powered-hardware-self-driving-cars>>.

¹⁸² Sidra Butt, “Huawei’s desire to Be the Bosch of China”, *Economy.pk*, 20 April 2021, <<https://www.economy.pk/huaweis-desire-to-be-the-bosch-of-china/>>.



AOS, as well as VOS, LiDAR and 4D imaging radar, among other things.

A combination of the difficulties the company ran into, the economic impacts of Covid-19 and the Russian war in Ukraine have largely pushed Huawei out of public view in Europe. Recent, potentially high impact, developments relating to the company have gone almost unnoticed. In January 2020, for example, the Dutch navigation and digital mapping company TomTom announced it had signed a deal with Huawei for the use of its maps and services in smartphone apps.¹⁸³ Another little-noticed development in June 2021 saw Huawei launch HarmonyOS 2, a new version of its internally developed operating system now available not only for smartphones, but possibly also for use in cars.

Several European carmakers have commercial partnerships with Huawei. European brands such as Audi and Volkswagen (both part of the Volkswagen Group) set up software subsidiaries in China to meet the demands of Chinese customers in order to be part of a dynamic and promising automotive market and make use of the pool of software engineers. In January 2022, Stephan Wöllenstein, CEO of Volkswagen Group China, announced that

his firm and Huawei were engaged in negotiations. It seems likely that Huawei is one of the three unspecified joint venture partners of CARIAD China, a software company and subsidiary of the Volkswagen Group.¹⁸⁴ On 13 October 2022, CARIAD signed a deal with Horizon Robotics, one of the leading providers of computing solutions for smart vehicles in China, as part of efforts to speed up the regional development of Advanced Driver Assistance Systems and autonomous driving systems for the Chinese market.¹⁸⁵ CARIAD has integrated 15 software companies and has more than 5000 employees in more than 70 countries. The company is developing the VW.OS operating system for all of the Volkswagen Group's brands, including Audi, Seat and Skoda. By 2030, there should be 40 million cars operating on VW.OS. In markets outside of China, VW.OS is likely to run on the real-time operating system QNX developed by BlackBerry.¹⁸⁶

Within China, Huawei and Audi demonstrated their plans for cooperation in the field of intelligent connected vehicles featuring Huawei's Mobile Data Centre (MDC) integrated into the Audi Q7 during Huawei Connect 2018.¹⁸⁷ Further areas of

¹⁸³ "TomTom Closes Deal with Huawei for Use of Maps and Services: Spokesman", *Reuters*, 17 January 2020, <<https://www.reuters.com/article/us-tomtom-huawei-tech-idUSKBN1ZG1SW>>.

¹⁸⁴ "CARIAD Reinforces Regional Software Development with China Subsidiary", Volkswagen AG, 28 April 2022, accessed 13 December 2022 at <<https://www.volkswagenag.com/en/news/2022/04/cariad-reinforces-regional-software-development-with-china-subsidiary.html>>.

¹⁸⁵ "VW's Software Subsidiary CARIAD, Horizon Robotics to Build Joint Venture for ADAS, AD Solutions",

Gasgoo, 13 October 2022, <<https://autonews.gasgoo.com/icv/70021493.html>>.

¹⁸⁶ "Volkswagen Group Software Powerhouse CARIAD Selects BlackBerry QNX for Its Software Platform", *BlackBerry*, 6 July 2022, <<https://www.blackberry.com/us/en/company/newsroom/press-releases/2022/volkswagen-group-software-powerhouse-cariad-selects-blackberry-qnx-for-its-software-platform>>.

¹⁸⁷ "Huawei and Audi announce Joint Innovation in L4 Automatic Driving", *Huawei*, 11 October 2018, accessed 13 December 2022 at <<https://www.huawei.com>>.



cooperation between Huawei and Audi are the joint training of experts in the field of intelligent connected vehicles, and planning for an ICV training academy.¹⁸⁸ Huawei is also partnered with Volvo and Mercedes-

Benz on providing car owners with the HMS for Car smart vehicle solution, using Huawei's smart voice assistant and based on the application of Huawei's terminal cloud services.

Relevance to EU Strategic Autonomy

China's strong role in V2X technology has implications for Europe's strategic technology autonomy. This section assesses the impact on four dimensions: supply chain resilience, national security, values protection and technological competitiveness.

Resilience of supply chains

Chinese firms do not currently appear to be supplying core V2X technology to European car makers in the EU. All the European car brands that cooperate with Huawei on developing software for the Chinese market have alternative systems for their cars on the European market. Nonetheless, German carmakers are increasingly investing in R&D in China, thereby establishing linkages with Chinese technology companies and with the Chinese automotive ecosystem.¹⁸⁹ A relevant question for European strategic autonomy is whether in future European companies working in China with Chinese technology will have the resources to develop a second, separate

system based on non-Chinese technology in other markets.

A challenge for the resilience of supply chains that became evident during the Covid-19 pandemic is that most chips for the automotive sector are produced in China. While China is dependent on Europe and the US for the design of chips for the automotive industry, the final production stage of many chips takes place in China. This interdependency makes it less likely that the Chinese government will weaponize chips in their struggle for tech-leadership with Europe and the US. However, given the current tensions, both China, on one side, and the US and Europe, on the other, will put a lot of money and effort into becoming less dependent on each other.

To avoid future disruption of the supply chain, carmakers are increasingly engaging in long-term commitments with major chip manufacturers in relation to future autonomous vehicles.¹⁹⁰ The US companies Intel, Qualcomm and Nvidia seem to be leading this process. The race for long-

com/en/news/2018/10/huawei-audi-l4-automatic-driving>.

¹⁸⁸ It is not clear whether this has been realized yet. Saad Metz, "Audi and Huawei explore new driving experience", *IoT Automotive*, no date, accessed 13 December 2022 at <<https://iot-automotive.news/huawei-and-audi-explore-new-driving-experience/>>.

¹⁸⁹ Gregor Sebastian (note 165).

¹⁹⁰ Agam Shah, "Car Makers Lock in Long-Term Deals for Chip Giants for Future Autonomous Vehicles", *The Register*, 6 January 2022, <https://www.theregister.com/2022/01/06/self_driving_car_makers_chips/>.



term contracts is getting more intense now that these companies offer a platform solution that can combine many different functions that used to run on different chips. All European car brands have long-term contracts with these US tech companies.

Given the size of the Chinese market for electric vehicles, it can be expected that Chinese makers of electric vehicles will become increasingly active and competitive internationally – including with Chinese brands – and that Chinese V2X technology will follow in their footsteps. European carmakers that are already embedded in a Chinese V2X ecosystem might decide to participate in such development in order to remain competitive vis-à-vis their Chinese counterparts. They could potentially decide to expand partnerships with Chinese technology suppliers to third markets or to the EU itself. Even if they do not, Chinese technology companies could still become successful exporters of V2X technology. A situation where Chinese suppliers of key V2X equipment and software become internationally dominant would be unfavourable for European strategic autonomy as it would make the EU more dependent on China. At the same time, from a resilience point of view, the European car industry should not be strategically dependent for such technology on any non-European country, including the US. Cooperation with Chinese actors could reduce the EU's dependence on US technology firms.¹⁹¹

¹⁹¹ Gregor Sebastian (note 165).

¹⁹² Go Matthew Holroyd, "Gridlock as Hackers Order Hundreds of Taxis to Same Place in Moscow", *Euronews*, 7 September 2022, <<https://www.euronews.com/my-europe/2022/09/02/gridlock-as-hackers-order-hundreds-of-taxis-to-same-place-in-moscow>>.

National Security

One concern in the security sphere is the possible future use of Chinese V2X technology in cars on the European market to collect data that could harm national security. Camera-equipped cars could be used for surveillance of strategically sensitive objects or persons, and the Chinese government might be able to retrieve the resulting data. Important factors in this regard are where the data collected is stored and which actors have access to the relevant data centres. Another longer-term risk is that vehicles could be controlled remotely by criminal or hostile actors, and then used to disrupt traffic flows or cause other forms of damage. A recent preview of this potential future risk can be found in the actions of a group of hackers which ordered hundreds of taxis to the same place in Moscow, causing huge traffic jams.¹⁹² Since Chinese V2X technology is not yet used in cars on the European market, there is still time to develop technical and regulatory solutions to mitigate such security risks. To an important extent, such an approach will be necessary even if Chinese technology does not enter the EU car market, as V2X systems based on non-Chinese technology could still potentially be hacked by Chinese or other actors.

Values and sustainability

The privacy of user data in in-car communications systems could potentially be compromised. The EU has several GDPR-related



instruments that are relevant in this regard. In January 2017, the EU Agency for Network and Information Security (ENISA) published a study on cybersecurity and the resilience of smart cars, which listed sensitive assets and the corresponding threats and risks, as well as mitigation factors and possible security measures to be implemented. In September 2017, the International Conference of Data Protection and Privacy Commissioners (ICDPPC) adopted a resolution on connected vehicles. Finally, in April 2018, the International Working Group on Data Protection in Telecommunications (IWGDPT), published a working paper on connected vehicles.

In terms of sustainability, the transition to electric driving is an important element of the transition away from fossil fuels. The EU could potentially face a dilemma if it had to make a trade-off between becoming strategically dependent on Chinese

V2X technology and speeding up the process of energy transition in road vehicles.

Technological competitiveness

A combination of Chinese dominance in battery technologies for electric vehicles (where Chinese companies already play a leading role) and in V2X technology would make it hard for the European car industry to remain competitive. Even in a scenario where Chinese suppliers of V2X technology were banned from EU and US markets, they might still be able to build up a strong position not only in China, but also in many third markets. Highly relevant in this regard is that the EU appears to be lagging behind with the introduction of 5G networks. This could have serious consequences once C-V2X technologies are connected to 5G networks and display much better performance than the older ITC-G5.

Conclusions and recommendations

The EU car manufacturing industry does not currently appear to be dependent on Chinese suppliers of V2X technology, which involves both AI and the IoT. Given the scale and pace of application of V2X in China, however, there is a possibility that Chinese companies could eventually become highly competitive internationally. This could lead to various risks to EU strategic autonomy, in particular with regard to supply chain resilience and technological competitiveness. National security and values-related risks also require serious attention. That said, the evolution of Chinese V2X

technology could also provide opportunities for the EU to strengthen its strategic autonomy. Provided that Chinese suppliers do not become dominant, that Chinese standards are open and developed jointly with non-Chinese actors, and that EU car user data is protected from access by the Chinese government, the EU could benefit from European-Chinese cooperation to accelerate the transition to electronic driving and smart mobility, maintain an innovative and competitive car industry, and mitigate strategic dependence on US technology firms.






DIMENSION OF STRATEGIC AUTONOMY	SHORT DESCRIPTION OF CHALLENGE IN KEYWORDS	RELATIVE IMPORTANCE OF CHALLENGE ON A SCALE OF 1 TO 4	POLICY INSTRUMENTS FOR TACKLING CHALLENGE IN KEYWORDS
 Resilience of supply chains	<ul style="list-style-type: none"> Mitigating risks of supply interruptions for the car industry associated with increasing dependence on Chinese AI and IoT technology 	4	<ul style="list-style-type: none"> Maintain Chinese strategic dependencies on the EU such as on access to automotive chips; Ensure that cooperation between Chinese and EU companies on V2X technology results in open standards
 National security	<ul style="list-style-type: none"> Mitigating potential use of in-car cameras for data collection that harms national security; Preventing loss of vehicle control to hostile actors 	3	<ul style="list-style-type: none"> Store car data in the EU; limit access to data centres from outside the EU; Develop technical solutions
 Values and sustainability	<ul style="list-style-type: none"> Ensuring that the transition to electric vehicles does not create one-sided dependence on Chinese technology suppliers; Protecting the privacy of car user data 	3	<ul style="list-style-type: none"> Maintain two-way dependence; avoid Chinese market dominance in key technologies; Store car data in the EU; limit access to data centres from outside the EU
 Technological competitiveness	<ul style="list-style-type: none"> Maintaining the competitiveness of the European car industry 	4	<ul style="list-style-type: none"> Adopt open standards across Europe and avoid adopting closed standards developed in China or the US; Create a dual system for both DSRC and C-V2X that provides the EU with the option to switch to C-V2X once 5G is widely available

Figure 6.2 – Main Chinese AI/IoT technology-related risks in the European automotive sector

Recommendations for EU and EU member state policymakers

Supply chain resilience

- European policymakers can limit the threats from and maximize the potential benefits of V2X cooperation between Chinese and European actors in the automotive sector by adopting open standards across Europe. This would limit the power of individual actors, and encourage and support

European alternatives to the currently dominant US operating systems, as well as IT technology for use by carmakers as a basis for their own operating systems. Europe should avoid automatic adoption of de facto but closed standards developed in other large markets, such as the Chinese or even the US market. To some extent, this is already happening in the car infotainment sector, but it should be avoided for ADAS,



V2X and other strategically important automotive systems.

- Mitigate the risk of strategic dependence on China by maintaining Chinese dependencies on the EU in terms of access to technology and cooperation with European counterparts.
- Aim for joint development of V2X technologies and standards, involving European, Chinese, US and other actors. EU carmakers and technology companies should play a central role in such an approach.

National security

- Store car user data in the EU and limit access to data centres from outside the EU in order to prevent the Chinese government from using cars with built-in cameras to collect strategically sensitive information. Currently, the discrepancy between the European GDPR and the US Cloud Act shows that European data is not fully protected by the GDPR if collected on European soil by a foreign company.

Values and sustainability

- Maintain two-way dependence and avoid Chinese market dominance in key technologies in order to allow Chinese technology to contribute to the transition to electric driving without becoming strategically dependent on China.
- To protect user privacy, store car user data in the EU and limit access to data centres from outside the EU. Sensitive data should only be stored in European-owned data centres. Assess whether additional regulation is required to achieve this aim.

Technological competitiveness

- Adopt open standards across Europe and avoid adopting closed standards developed in either China or the US.
- Prepare roadside units and on-board units for dual-use by both DSRC and C-V2X so that European researchers, companies and drivers can gain experience with DSRC and then make a relatively easy switch to C-V2X once 5G networks are widely available.

Authors:

Raúl Rojas is Professor of Artificial Intelligence at the Freie Universität Berlin. Contact: rojas@inf.fu-berlin.de

Sanne van der Lugt is a researcher and policy adviser on China in Africa, Chinese technological developments and the consequences for European strategic autonomy. She is based in the Netherlands. Contact: sannevdlugt@fastmail.com

Frans-Paul van der Putten is an independent researcher on China and geopolitics. He is based in the Netherlands. Contact: fputten@chinageopolitics.nl





AI for Urban Public Security: Threats to European Security and Values

Gregory Walton, Valentin Weber

Abstract

This chapter argues that the emergence of networks of interdependent smart cities, particularly where this involves AI-driven surveillance for public security as part of China's "safe cities" programmes, presents challenges for European strategists developing the concept of Open Strategic Autonomy (OSA). There is comparatively limited foresight research into the normative and geopolitical challenges that these cyber-physical-social systems-of-systems (CPSSoS) will present to the European Union's OSA strategy. We consider the implications of China's Urban AI in relation to the four dimensions of European Strategic Autonomy: supply chain resilience, national security, ethical values and technological competitiveness, while focusing on the potential for China's "safe cities export strategy" to negatively affect security and universal ethical values. We make recommendations on how European instruments might surmount these challenges, including the role of European smart cities in enhancing the "Brussels effect". Finally, we issue a call for branding strategists to rethink what a uniquely European design and engineering philosophy might bring to smart cities, in order to chart a future course away from both digital authoritarianism and surveillance capitalism.

Cities will define the future because they are where the vast majority of people will live. By 2050, more than two-thirds of humanity will live in urban areas.¹⁹³ Cities are undergoing a rapid process of digital transformation, much of it involving new systems that fuse biometric surveillance with

AI. Roughly half of the 1000 smart city initiatives under way globally are in China.¹⁹⁴ In US foreign policy circles, Chinese cities are becoming synonymous with unprecedented levels of surveillance and increasing "digital authoritarianism".¹⁹⁵ China is also exporting these technologies. AI-

¹⁹³ United Nations, Department of Economic and Social Affairs, "68% of the world population projected to live in urban areas by 2050, says UN", New York, 16 May 2018, <<https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html>>.

¹⁹⁴ Katherine Atha et al., "China's Smart Cities Development", *Research Report Prepared on Behalf of the*

US-China Economic and Security Review Commission, Reston, SOS International (SOSi), 2020.

¹⁹⁵ Dorota Głowacka et. al., "Digital technologies as a means of repression and social control", European Parliament, Policy Department for External Relations, Brussels, 2021.



enabled “safe city platforms” are being sold as turn-key solutions to over 75 countries globally. Chinese companies either owned by or closely aligned with the party-state, including Huawei¹⁹⁶ and CETC’s Hikvision,¹⁹⁷ supply AI surveillance technology to over 63 countries, 36 of which have signed up to China’s Belt and Road Initiative.¹⁹⁸ In recent years, the vast smart city market in China has produced a complex supply chain for smart cities. This ecosystem is built around a few flagship companies, such as Huawei and ZTE, that sell their smart or safe cities as turnkey solutions. These two players also integrate other services into their services, such as Alibaba,¹⁹⁹ to provide cloud infrastructure for data surveillance,²⁰⁰ which in turn provides the business layer software for the police command management system, or Sensetime,²⁰¹ for facial recognition capabilities.

The European smart city ecosystem is markedly different. Major companies, such as Nokia and Siemens, do not work autonomously as systems integrators or market smart city solutions as turnkey solutions,

but instead focus on their core technologies and work with other corporate and government actors to integrate their products into existing projects. Nokia’s solutions, for instance, are much more limited in scale, focused on providing urban 5G connectivity in France,²⁰² or deploying drones in a Japanese city to help with tsunami preparedness.²⁰³ Similarly, while Siemens has tested the concept of a digital twin in a Berlin district (Siemensstadt), Chinese companies’ digital twins of cities are already operational in China at the city-wide level.²⁰⁴ Even the aerospace giant, Airbus, is largely focused on discrete segments of the smart city vertical, for example, with its Urban Air Mobility.²⁰⁵ Thales, which markets complete urban management systems as smart and safe cities under its Protection Systems Portfolio, is an exception to this piecemeal approach.²⁰⁶

China has made the smart city a core part of its national development strategy. Xi Jinping has endorsed the concept and it featured in the 13th Five-Year Plan (2016–2020), adopted in March 2016. The 14th

¹⁹⁶ Cao Zhihui, “Nowhere to hide: Building Safe Cities with Technology Enablers and AI”, *Huawei*, July 2016, <<https://www.huawei.com/us/technology-insights/publications/winwin/ai/nowhere-to-hide>>.

¹⁹⁷ Hikvision, “Advanced Security, Safer Society”, accessed 2 December 2022, at <https://www.hikvision.com/en/solutions/solutions-by-industry/safe-city/>.

¹⁹⁸ Steven Feldstein, “The Global Expansion of AI Surveillance”, *Working Paper*, Carnegie Endowment for International Peace, Washington, DC, 2019.

¹⁹⁹ Laura Dobberstein, “Alibaba execs hauled in to discuss Shanghai Police data leak”, *The Register*, 18 July 2022, <https://www.theregister.com/2022/07/18/apac_tech_news_roundup/>.

²⁰⁰ Valentin Weber and Vasilis Ververis, “China’s Surveillance State: A Global Project”, *Top10VPN*, 2021.

²⁰¹ Zhang Xia, “SenseTime Collaborates with Huawei to Introduce Ultra High-Precision Facial Recognition

Solution”, *Yicai Global*, accessed 2 December 2022, at <<https://www.yicaiglobal.com/news/sensetime-collaborates-with-huawei-to-introduce-ultra-high-precision-facial-recognition-solution>>.

²⁰² Nokia, “Sendai City improves tsunami preparedness with connected drones”, accessed 2 December 2022, at <<https://www.nokia.com/networks/case-studies/sendai-city/>>.

²⁰³ Nokia (note 202).

²⁰⁴ Albert Wong, “Digital twins in smart city”, PWC, 2020.

²⁰⁵ Airbus, “Urban Air Mobility”, accessed 2 December 2022 at, <<https://www.airbus.com/en/innovation/zero-emission-journey/urban-air-mobility>>.

²⁰⁶ Thales, “Smart City”, accessed 2 December 2022 at, <<https://www.thalesgroup.com/en/activities/security/city/smart-city>>.



Five-year Plan for National Informatization reinforces the importance of smart cities to core national development objectives and directs that smart cities “should advance in a graded, categorized, and orderly manner”.²⁰⁷ The 14th plan also links rural digitalization to smart cities. In surveillance terms, this means the Sharp Eyes programme in both rural and urban areas. Beyond the national hi-tech corporate champions, the government is investing heavily in smart city R&D. State Key Laboratories (SKL), for example, conduct basic and applied research in science and technology. The Center for Security and Emerging Technologies, a US think tank, has mapped over 500 SKLs,²⁰⁸ among them laboratories that contribute directly to party state-driven smart city research and development, such as the State Key Laboratory of the Internet of Things for the Smart City at the University of Macau.²⁰⁹ Other SKLs that contribute to fundamental research related to smart cities include the Key Laboratory of Internet of Things Intelligent Technology at Harbin Institute of Technology and the State

Key Laboratory for Management and Control of Complex Systems (SKL-MCCS),²¹⁰ hosted by the Institute of Automation, Chinese Academy of Science (CASIA). Another significant state-backed laboratory in this R&D ecosystem is the Pengcheng Lab,²¹¹ led by the “father of the Great Firewall”, Fang Binxing.

There has been comparatively little foresight research into the normative and geopolitical challenges that these cyber-physical,²¹² cyber-social,²¹³ systems-of-systems²¹⁴ are likely to present to the EU’s strategy on Open Strategic Autonomy in the coming decades. However, the European Parliamentary Research Service Scientific Foresight Unit (STOA) and other consultants based in the European Parliament have produced some interesting work in this regard,²¹⁵ which informed our thinking in this chapter. We recommend this to readers who want to go deeper into thinking through the ethical and societal challenges from a distinctly European perspective.²¹⁶

²⁰⁷ Translation: 14th Five-Year Plan for National Informatization, DigiChina, December 2021, <<https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/>>.

²⁰⁸ Emily Weinstein et al., “China’s State Key Laboratory System”, *Data Brief*, Center for Security and Emerging Technology (CEST), June 2022.

²⁰⁹ State Key Laboratory of Internet of Things for Smart City, “Lab Introduction”, *University of Macau*, accessed 2 December 2022 at, <<https://skliotsc.um.edu.mo/about/lab-introduction/>>.

²¹⁰ The State Key Laboratory for Management and Control of Complex Systems (SKL-MCCS), “About Us”, accessed 2 December 2022 at, <<http://www.compsys.ia.ac.cn/EN/index.html>>.

²¹¹ Openi, “no title”, accessed 2 December 2022 at, <https://openi.pcl.ac.cn/Smart_City_Model_Zoo>.

²¹² Google Scholar, “‘Cyber-physical system’ AND ‘smart city’”, accessed 2 December 2022.

²¹³ Google Scholar, “Cyber-physical-social systems AND smart city”, accessed 2 December 2022.

²¹⁴ Google, “‘site:europa.eu’ ‘system of systems’ AND ‘smart city’”, accessed 2 December 2022.

²¹⁵ European Parliament, ‘Ethical and societal challenges of the approaching technological storm’, European Parliamentary Research Service (EPRSP) Scientific Foresight Unit (STOA), PE 729.543, July 2022, <[https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729543/EPRS_STU\(2022\)729543_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729543/EPRS_STU(2022)729543_EN.pdf)>.

²¹⁶ European Parliament, Artificial Intelligence in smart cities and urban mobility, Briefing, 23 July 2021, <[https://www.europarl.europa.eu/thinktank/en/document/IPOL_BRI\(2021\)662937](https://www.europarl.europa.eu/thinktank/en/document/IPOL_BRI(2021)662937)>.























ACTOR TYPE	NAME OF KEY ACTOR	DESCRIPTION	KEY TASK	PRIORITY
Research institution (State Key Laboratory, SKL)	 State Key Laboratory of Internet of Things for Smart City, University of Macau (智慧城市物聯網國家重點實驗室 (澳門大學))		Urban IoT R&D	
Research institution (SKL)	 Key Laboratory for Internet of Things and Intelligent Technology, Harbin Institute of Technology (物联网智能技术重点实验室 (哈尔滨工业大学))		Urban IoT R&D	
Research institution (SKL)	 The State Key Laboratory for Management and Control of Complex Systems (SKL-MCCS), hosted by the Institute of Automation, Chinese Academy of Science (CASIA) (复杂系统管理与控制国家重点实验室)		Complex Systems engineering	
Research institution	 Pengcheng Lab (鹏城实验室)	Led by the "Father of the Great Firewall", Fang Binxing.	Blue sky urban AI R&D, Southeast Asia	
Corporation/Policy	 Huawei (华为)	AI surveillance	Integrator of smart city solutions	
Corporation/Policy	 CETC/Hikvision (中国电子科技集团) / (海康威视)	PLA-aligned/owned Safe City exports; XUAR.	Integrator of smart city solutions	
Corporation	 ZTE (中兴通讯)	AI surveillance	Integrator of smart city solutions	
Corporation	 Alibaba (阿里巴巴集团)	Citybrain, cloud storage for many safe city deployments	Provides cloud technology for smart cities	
Corporation	 SenseTime (商汤科技)	AI surveillance	Provides AI algorithms for urban surveillance	
Policy	 Cyberspace Administration of China (中央网络安全和信息化委员会办公室)	Launched the Inter-Ministerial Coordination Working Group on New Smart Cities under the SAC	Establishes priorities for China's smart cities efforts by measuring progress against eight key indicators	

Figure 7.1 – Actors to watch



The Four Dimensions of European Strategic Autonomy

Supply Chain Resilience

Smart cities are an assemblage of foundational technologies: a complex system of systems. At present, most European suppliers of smart city technologies offer fragmented solutions; that is, sub-systems of complete digital urban governance packages. What arguably makes a city smart is the extent to which a manufacturer can successfully integrate disparate sub-systems into a unified urban management platform. The supply chains that support this assemblage are more complex even than any of the individual ecosystems that support it. The recent literature that models interdependent supply chains as Complex Adaptive Systems (CAS) is relevant here.²¹⁷

The core technology common to all these technologies is the microprocessor, so the resilience of semiconductor supply chains globally is a key factor in understanding how to mitigate the risk of shortages underlying the emerging smart city supply ecosystem. The significant impact of the global semiconductor shortage on critical European industries, such as car making, has demonstrated that adequate redundancy and resilience in supply chains will be crucial to Europe's technological sovereignty and competitiveness in the coming decades. One of the five strategic objectives of the European Chips Act is to develop an "in-depth understanding of global semiconductor supply chains".²¹⁸

This objective could be achieved by accelerating development of Artificial Intelligence of Things (AIoT)-driven supply chain optimization methods to support predictive demand forecasting throughout the industry, thereby optimizing inventory levels and leading to a reduction in hazardous waste and the industry's outsized carbon footprint, and supporting not only increased supply chain resilience, but also greater sustainability.

National Security

In a similar vein, any assessment of the national security implications of European dependence on the components for smart cities would also have to incorporate assessments of dependence on imported urban sensors, the networks that connect them and the underlying data processing capacity for: (a) facial recognition cameras; (b) fifth- (5G) and sixth-generation (6G) wireless communications networks; (c) the vast array of urban sensors and other devices that fall under the category of the Internet of Things; (d) technology to support big data processing using Artificial Intelligence (AI), including existing cloud computing services, and the transition to edge computing; (e) technologies to support extended reality (VR, AR, MR); (f) Geographic Information System mapping and urban planning software, including recursive urban-scale simulation; and (g) semi-autonomous or autonomous vehicles.

²¹⁷ Google Scholar, "complex adaptive systems" AND "supply chain resilience", accessed 2 December 2022.

²¹⁸ European Commission, "European Chips Act", accessed 2 December 2022 at, <<https://digital-strategy.ec.europa.eu/en/policies/european-chips-act>>.



One of the most visible components of Chinese safe cities are biometric surveillance cameras. A 2020 study found that only two of the top 10 companies in this industry are European: Axis, a Swedish company, and TKH Group, a Dutch company.²¹⁹ More than two-thirds of all sales in this industry are to Chinese companies. These cameras are widely used at European airports and in other critical infrastructure. In emerging markets, where deployment of surveillance cameras is growing rapidly, PRC market share is perhaps even greater.

A recent IoT scan case study focused on scanning the IoT ecosystem in EU candidate states in south-eastern Europe, for example, found that that over 90% of the cameras in some urban areas, including Skopje, Podgorica and Tirana, had been manufactured by CETC's HikVision.²²⁰ Significantly, we also found that while US manufactured, and the few EU manufactured devices we could enumerate, were on the whole adequately secure and exhibited few known vulnerabilities or excessive attack surfaces, Chinese manufactured devices in the ecosystem (almost entirely internet-connected cameras) exhibited systemic insecurity at scale, including Remote Management protocol issues, known vulnerabilities in IP camera firmware and excessive attack surfaces. So alarming were the systemic vulnerabilities observed in these small IoT ecosystems in these cities

that we made the case that there was scope to assess whether there were serious grounds for suspecting that use of the devices at scale would endanger national security or national defence in the region.

These case studies informed our thinking on how these complex interdependencies might translate into national security challenges for member states. Several potential national security challenges could arise from technological dependencies. The key challenges are cybersecurity vulnerabilities; vulnerability to supply chain disruption, particularly in moments of crisis; data privacy and "data traps",²²¹ and infrastructure vulnerabilities. As with any networked system, smart cities are vulnerable to cyberattacks that could compromise the security and privacy of their citizens. Throughout the Digital Silk Road, there are concerns about the role of Chinese tech companies in building and operating smart city infrastructure, and the potential for them to access or misuse the data collected from citizens. For example, in Lahore, Wi-Fi modules linked to the video surveillance system were removed due to the potential for misuse.²²² Business Efficiency Solutions LLC is suing Huawei in the California federal court for allegedly creating a "backdoor". Huawei has countered that the alleged backdoor is in reality a digital twin or a back-up mirror hosted at a Chinese data centre. Nonetheless, it is reported to

²¹⁹ William Pao, "2021 Security 50: the top companies in surveillance and access control", *asmag.com*, 18 November 2021, <<https://www.asmag.com/show-post/32612.aspx>>.

²²⁰ Unpublished research by Greg Walton.

²²¹ Mary Hui, "The UK spy chief's warning about China's 'data traps' highlights digital supply-chain risks", Quartz,

2 December 2021, <<https://qz.com/2097355/why-the-uk-spy-chief-is-warning-about-chinas-data-traps>>.

²²² Leo Kelion and Sajid Iqbal, "Huawei wi-fi modules were pulled from Pakistan CCTV system", BBC, 8 April, 2019, <<https://www.bbc.co.uk/news/technology-47856098>>.



have afforded Huawei access to sensitive data “important to Pakistan’s national security” in the safe city project in Lahore.²²³

Complex digital systems such as smart cities almost inevitably rely on imported technology and software, which creates dependencies on foreign suppliers. This could leave a country vulnerable to potential disruptions or supply chain vulnerabilities. In the case of China, there have been serious concerns about the country’s reliance on foreign technology, including from the United States, particularly post-Snowden; while in the US parallel fears have been growing about dependencies in critical infrastructure, particularly on Huawei in 5G core networks. Europe’s openness to trade in this sector while also guarding its autonomy is likely to be one of the defining geopolitical challenges in the coming decades. Similarly, the sheer scale of the collection and use of personal data in smart cities through ubiquitous AIoT networks raises concerns about the privacy of citizens and the potential for abuse of data by governmental authorities, as well as questions about just how closely aligned China’s tech giants are with the very core of the party state. Networks of and between smart cities will become so fundamental to global trade and so critical to everyday life that these technological interdepend-

encies will become one of the most serious non-traditional national security challenges that a state will face.

Technological Competitiveness

US corporations have first mover advantage in the smart city export space. IBM coined this term when it launched its Smarter Cities campaign in 2009. One significant consequence of the US pioneering the smart city concept is that US government agencies are active in promoting smart city partnerships as part of their diplomacy and aid programmes, which often twin the urban digital transition with sustainability goals. For example, the US-ASEAN Smart Cities Partnership (USASCP),²²⁴ led by the US State Department, coordinates an inter-agency package focused on improving urban quality of life in this strategically important region. Similarly, USAID’s programme on supporting climate-smart cities twins the urban digital transition and resilient digital ecosystems with environmental goals.²²⁵

China has second mover advantage and Beijing’s approach to transnational data governance is to supply infrastructure – both digital and material – more cheaply than western corporations. This component of the “Beijing Effect”,²²⁶ as Erie and Streinz style it, is an important dimension of the challenge that China presents not

²²³ Blake Brittain, “Huawei accused of stealing trade secrets, spying in Pakistan”, Reuters, 12 August 2021, <<https://www.reuters.com/legal/transactional/huawei-accused-stealing-trade-secrets-spying-pakistan-2021-08-12/>>.

²²⁴ US Department of State, US-ASEAN Smart Cities Partnership (USASCP), 22 August 2022, <<https://www.state.gov/u-s-asean-smart-cities-partnership-usascp-sharing-expertise-between-cities-to-benefit-the-people-of-asean/>>.

²²⁵ USAID, USAID’s Program Supporting Climate-Smart Cities, accessed 6 January 2022 at, <<https://www.climatelinks.org/sites/default/files/asset/document/USAID%20Urban%20CCA%20Programs.pdf>>.

²²⁶ Matthew S. Erie and Thomas Streinz, “The Beijing effect: China’s Digital Silk Road as Transnational Data Governance”, *NYU Journal of International Law & Politics*, vol. 54, no. 2 (Fall 2021), p. 2.



only to competitiveness, but also to normative or ethical values in the urban AI space.

Ethical Values

Chinese cities are becoming synonymous with unprecedented surveillance and increasing digital authoritarianism.²²⁷ Some have gone so far as to claim that Beijing is creating a novel digital surveillance model of urban governance,²²⁸ and that this grand normative challenge to European values will shape future geopolitical contests, leading inexorably to the proliferation of two (or more) wholly incompatible urban-led governance models globally.²²⁹

Erie and Streinz analyse the phenomenon of China shaping transnational data governance by exporting its digital infrastructure and values to other countries, which is increasingly being referred to as digital authoritarianism.²³⁰ The authors problematize this explanatory framework, suggesting that both push and pull factors contribute to China's growing influence in data governance beyond its borders, the latter including the demand for Chinese-built digital infrastructure in emerging economies and emulation of China's approach to data governance in pursuit of data sovereignty and digital development.

By contrast, Europe is pursuing a markedly different approach to smart cities and data sovereignty, and thus to Open Strategic Autonomy. European Union member states have put strong emphasis on data protection and privacy, and have implemented policies and regulations such as the General Data Protection Regulation (GDPR) to ensure that individuals' personal data are handled responsibly and securely. While the EU has, to a limited extent to date, focused on the integration of systems and technologies to improve the efficiency and sustainability of cities, it emphasizes the primacy of respecting its citizens' rights and freedoms, as evidenced, for example, by the privacy debates around the passage of the AI Act.²³¹

The approaches to smart cities and data governance of Europe and China differ in terms of their priorities and normative values. While China has focused on exporting its digital infrastructure – and to a much lesser extent its normative values – to other countries, Europe has placed a greater emphasis on protecting citizens' rights and freedoms. This emphasis on respecting digital rights in the urban AI export market could distinguish EU services and systems from China's in the developing world, with the consequence that soft

²²⁷ Dorota Głowacka et al., "Digital technologies as a means of repression and social control", European Parliament, Policy Department for External Relations, Brussels, 2021.

²²⁸ Bethany Allen-Ebrahimian, "Beijing is creating a digital surveillance-based governance model", *Axios*, accessed 2 December 2022 at <<https://www.axios.com/2022/09/06/beijing-digital-surveillance-governance-model>>.

²²⁹ Alice Ekman and Cristina de Esperanza Picardo, "Towards Urban Decoupling: China's Smart City Ambitions at the Time of Covid-19", *EUISS*, 14 May 2020,

<https://www.iss.europa.eu/content/towards-urban-decoupling-china%E2%80%99s-smart-city-ambitions-time-covid-19#_the_normative_challenge_china__s_smart_city_as_an_alternative_form_of_urban_governance__>.

²³⁰ Matthew S. Erie and Thomas Streinz (note 226).

²³¹ Jedidiad Bracy, "A look at European Parliament's AI Act negotiations", *The Privacy Advisor*, 29 Nov. 2022, accessed 3 December 2022 at <<https://iapp.org/news/a/a-look-at-european-parliaments-ai-act-negotiations/>>.



power and the attractiveness of the “Brussels effect” could offset the disadvantages that the EU faces from following the US

and China into the smart cities export market.





DIMENSION OF STRATEGIC AUTONOMY	SHORT DESCRIPTION OF CHALLENGE IN KEYWORDS	RELATIVE IMPORTANCE OF CHALLENGE ON A SCALE OF 1 TO 4	POLICY INSTRUMENTS FOR TACKLING CHALLENGE IN KEYWORDS
 Resilience of supply chains	<ul style="list-style-type: none"> • Complex adaptive system of systems; • Interdependence; • Semiconductor shortage 	4	<ul style="list-style-type: none"> • European Chips Act: in-depth understanding of global semiconductor supply chains; • Accelerating development of AIoT-driven supply chain optimization methods to support predictive demand forecasting; • Cooperation with Taiwan
 National security	<ul style="list-style-type: none"> • Biometric AI surveillance cameras; • Systemic digital insecurity at scale among PRC vendors 	4	<ul style="list-style-type: none"> • AI Act and regulation of biometric surveillance; • Privacy Enhancing Technologies (PETs)
 Values and sustainability	<ul style="list-style-type: none"> • Twin transitions to a green and digital future; • Enhancing the “Brussels Effect”, countering the “Beijing Effect” 	3	<ul style="list-style-type: none"> • Transatlantic Cooperation on Standards; • Privacy Enhancing Technologies (PETs); • FIWARE
 Technological competitiveness	<ul style="list-style-type: none"> • US: first mover advantage; • PRC: second mover advantage. 	2	<ul style="list-style-type: none"> • FIWARE • EU-scale consortia; • A European rebranding of smart cities

Figure 7.2 – Recommendations

European Instruments for Rising to the Challenge and Recommendations

Technological competitiveness: EU systems-of-systems privacy engineering consortia, powered by Open Source

The most promising developments in European companies’ systems-of-systems

engineering consortia are clustered around Airbus and Thales.²³² They have developed an Open Source codebase, the FIWARE platform,²³³ and baked privacy-by-design into domestic and export deployments.

²³² Google, “systems of systems”, “smart city”, “airbus”, accessed 2 December 2022; and Google, “systems of systems”, “smart city”, “thales”, accessed 2 December 2022.

²³³ FIWARE, “FIWARE Marketplace”, accessed 2 December 2022 at, <<https://www.fiware.org/>>.



It is questionable, however, whether large European defence companies can make a better public case for protecting privacy than their Chinese or US counterparts offering smart city solutions, such as Google. The California-based company's efforts to build a smart Toronto were met with suspicion. Google channelled the project through its urban planning subsidiary, Sidewalk Labs,²³⁴ which argued that the project failed to materialize because of the Covid-19 pandemic. Many others, however, mentioned that a failure to sufficiently protect the data of citizens was the deciding factor in the ending of the proposed project. The former Privacy Commissioner for Ontario, Ann Cavoukian,²³⁵ for instance, withdrew from the planning process because depersonalization of the gathered urban data was made only voluntary rather than a requirement. As shown above, Europe does not have first- or second-mover advantage, but its far-reaching privacy regulations might offer a privacy-based smart city package that can compete as an alternative to Chinese and US companies in the international market.

Supply Chain Resilience: Cooperate with Taiwan

Europe should further deepen its partnerships on technology development, deployment and exports with like-minded

leaders with regard to the ethical use of AI in urban environments and complementary smart city supply chains. One such partner is Taiwan,²³⁶ which is a leader not only in semiconductors but also in the use of AI in cities. The EU has added Taiwan to its Joint Communication on the Strategy for Cooperation in the Indo-Pacific, noting that closer technological cooperation with Taiwan could help the EU to move closer to its ambition of Open Strategic Autonomy.

Cooperation with Taiwan should aim to create a long-lasting partnership that builds on both the EU's and Taiwan's strengths. EU entities could contribute their traditional strengths in development and production, such as in the automotive industry or on 5G connectivity. Taiwan could add to the partnership in areas such as hardware/software integration models and the development of AI semiconductors. By building on their respective strengths, the EU and Taiwan could cover large segments or elements that are crucial to smart cities, urban mobility and connectivity, among other things.

The EU would have a partner in the deployment of smart cities in the growing Asian market that has exported its smart city solutions to Indonesia, Brunei, the Philippines and Malaysia.²³⁷ For its part,

²³⁴ Adam Carter and John Rieti, "Sidewalk Labs cancels plan to build high-tech neighbourhood in Toronto amid Covid-19", *CBC*, accessed 2 December 2022 at, <<https://www.cbc.ca/news/canada/toronto/sidewalk-labs-cancels-project-1.5559370>>.

²³⁵ CBC, "I resigned in protest from Sidewalk Labs' 'smart city' project over privacy concerns", Toronto, 7 May 2020, accessed 2 December 2022 at, <https://www.youtube.com/watch?v=1t12UqYI5SA&ab_channel=CBC>.

²³⁶ Caribbean News Global, "Smart City Taiwan: A hub for digital solutions to new heights, Part 1", CNG Media, 27 October 2021, accessed 2 December 2022 at, <<https://www.caribbeannewsglobal.com/smart-city-taiwan-a-hub-for-digital-solutions-to-new-heights-part-1/>>.

²³⁷ The Smart City Taiwan Project, 2018–2020, accessed 19 December 2022 at, <<https://www.twsmartcity.org.tw/en/project>>.



Taiwan would find it easier to export its smart city solutions to the world's largest trading bloc. EU member states' governmental agencies should take on the role of facilitator in bringing European and Taiwanese companies together and allowing synergies to emerge.

Ethical Values: Towards a Green and Digital Future and Transatlantic Cooperation on Standards

The EU should accelerate its values-based digital transition by "twinning" it with its green transition.²³⁸ The governance of smart cities is the logical policy nexus for shaping these parallel transitions, which could be mutually reinforcing trends but are not automatically aligned. As with supply chains, the goal is urban resilience amid growing uncertainty and complexity, and accelerating the development of AIoT-driven supply chain optimization methods to support predictive demand forecasting throughout the urban AI industry. As noted above, this optimizes inventory levels, leading to a reduction in hazardous waste and the industry's outsized carbon footprint, thereby supporting not only increased supply chain resilience, but also greater sustainability.

²³⁸ Stefan Muench et al., "Towards a green & digital future", Joint Research Centre (JRC) Publications Repository, Brussels, 2022, doi:10.2760/54, JRC no. 12 9319.

²³⁹ European Commission, "EU-US Trade and Technology Council", accessed 2 December 2022 at, <https://ec.europa.eu/info/strategy/priorities-2019-2024/stronger-europe-world/eu-us-trade-and-technology-council_en>.

²⁴⁰ European Union, EU-US Summit 2021: Statement, "Towards a Renewed Transatlantic partnership", accessed 2 December 2022 at, <<https://www.consilium.europa.eu/media/50758/eu-us-summit-joint-statement-15-june-final-final.pdf>>.

Excessive dependency on imports in this AI-urban transition will steadily increase vulnerabilities and attack surfaces, erode citizens' rights and introduce Internet of Things-related insecurity at scale, including through imports from China. The EU should work with like-minded countries, including the US, to shape global technology standards that put urban interoperability with privacy by design at the heart of the emerging digital-urban stack. For example, a Trade and Technology Council (TTC)²³⁹ was established at the EU-US summit in 2021 to support transatlantic coordination on standards and regulations on a digital transition underpinned by democratic values, including respect for human rights.²⁴⁰ It could become a key platform for countering the growing influence of Chinese technical standards-setting in the smart city export space.²⁴¹

National Security: The AI Act and Privacy Enhancing Technologies

The EU AI Act is a body of legislation²⁴² that seeks to take a risk-based approach to regulating the use of AI within the European Union but could have significant influence beyond the borders of the EU, not least in the smart cities export space.

²⁴¹ Ana Chubinidze, "EU-US Trade and Technology Council: Case on China, AI and Smart Cities", Medium, accessed 2 December 2022 at, <<https://medium.com/urban-ai/eu-us-trade-and-technology-council-case-on-china-ai-and-smart-cities-626039612922>>.

²⁴² Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM(2021) 206 Final, <<https://artificialintelligenceact.eu/the-act/>>.



The legislation sets out a number of principles and requirements on the development and use of AI, such as the need for AI systems to be transparent, fair and trustworthy. The AI Act therefore has significant implications for the development of smart cities globally. At the time of writing, however, the extent to which the AI Act will regulate AI-driven biometric surveillance remains to be seen. According to privacy-focused NGOs and Members of the European Parliament, an outright ban on predictive policing and real-time facial recognition technologies is still on the table.²⁴³ Should exceptions for law enforcement and counterterrorism not be made in the final version of the legislation, European manufacturers would be unable to develop sub-systems to compete in the PRC-led safe city vertical that is growing rapidly in the developing world. If broad exceptions *are* made in order to permit the deployment of biometric AI surveillance to combat urban crime, however, the EU risks undermining its commitment to human rights. Both outcomes highlight the quandary that smart cities pose to the concept of European Open Strategic Autonomy, particularly in terms of the age-old tension between ethical values and national security in the urban space. One field of research that could help to address this paradox is that of Privacy Enhancing Technologies (PETs), specifically in the field of biometrics (so-called B-PETs) for face recognition.²⁴⁴ If robust privacy preserving technologies can be built into urban AI surveillance systems,

the EU could build systems that quantifiably preserve individual privacy while providing law enforcement agencies with the tools they need to combat crime and other threats to national security.

Enhancing the Brussels Effect

The Brussels Effect could become one of the EU's most effective instruments for developing Europe's Open Strategic Autonomy. The Brussels Effect refers to the ability of the European Union (EU) to shape global regulations and standards through its policymaking processes. As the GDPR and similar legal instruments, potentially including the AI Act, set the agenda for access to the single market, the EU is demonstrating leadership in the development of an internal regulatory environment with an impact that extends well beyond Europe's borders. This process is deepening both internal and external digital sovereignty. In a 2021 article,²⁴⁵ Erie and Stranz contrast the Beijing Effect with the Brussels Effect, whereby companies' global operations gravitate towards the EU's regulations. The EU way also deviates from US efforts to shape global data governance through instruments of international economic law. Enhancing the Brussels Effect in the Urban AI space means getting smart about the EU's growing international role as a normative power ensuring that the twin transitions accelerate Europe's capacity to export norms of good governance, notably representative democracy and human rights, through PETs-focused Urban AI engineering.

²⁴³ Jedidiad Bracy (note 231).

²⁴⁴ Blaž Meden et al., "Privacy-enhancing Face Biometrics: A Comprehensive Survey", IEEE, 12 July

2021, accessed 4 December 2022 at, <<https://ieeexplore.ieee.org/document/9481149>>.

²⁴⁵ Matthew S. Erie and Thomas Streinz (note 226).



A European Rebranding of Smart Cities

'Smart' is increasingly understood to be a euphemism for surveillance.²⁴⁶ In the United Kingdom, both the Department for Digital, Culture, Media and Sport and the National Cyber Security Centre are now talking about "connected places".²⁴⁷ Outputs from the Royal Society funded project, "Beyond Smart Cities: A comparative analysis of China and UK", posit Urban AI as the 'post-smart city'.²⁴⁸ In the Chinese literature, (in translation) digital city was supplanted by 'smart city' following a 2009 IBM campaign. 智慧城市 is only translated as "wisdom city" in the declining number of papers in this field that explicitly cite Qian Xuesen's later work. "Safe

city" dominates the export market literature, and in Chinese is a concept distinct from the smart city in policy and procurement documents. The implications of the safe dimension of smart cities, the rollout of AI-driven biometric surveillance networks operated by or on behalf of the public security and state security authorities, is the focus of this chapter. A distinctly European model of Urban AI that incorporates its core values and offers the possibility of an alternative to both digital authoritarianism and surveillance capitalism also calls for its own unique terminology.

Authors:

Greg Walton is Senior Research Associate for Cyber Security, Smart Cities, & Data Analytics at the SecDev Group, based in the United Kingdom. Contact: g.walton@secdev.com.

Valentin Weber is a research fellow with the German Council on Foreign Relations, based in Berlin. Contact: weber@dgap.org.

²⁴⁶ Robert Muggah and Greg Walton, "'Smart' Cities are Surveilled Cities", *Foreign Policy*, 17 April 2021, accessed 2 December 2022 at, <<https://foreignpolicy.com/2021/04/17/smart-cities-surveillance-privacy-digital-threats-internet-of-things-5g/>>.

²⁴⁷ UK National Cyber Security Center, "Connected Places Cyber Security Principles", 7 May 2021,

accessed 2 December 2022 at, <<https://www.ncsc.gov.uk/collection/connected-places-security-principles>>.

²⁴⁸ Simon Marvin et al., "Urban AI in China: Social Control or Hyper-capitalist Development in the Post-smart City?," *Frontiers in Sustainable Cities*, 11 October 2022, <<https://www.frontiersin.org/articles/10.3389/frsc.2022.1030318/full>>.





The ethics of Artificial Intelligence in the European Union and China

Kristin Shi-Kupfer, Luca Turchet

Abstract

The Chinese party-state has become increasingly active in shaping and setting standards for the ethics of Artificial Intelligence (AI) not only at home, but also in international institutions. The core goals and concepts of the Chinese Communist Party in its implementation of AI ethics differ significantly from those of the European Union. This paper provides an analytical overview of the key Chinese actors involved in setting China's AI ethics policy, develops a checklist for assessing the specific features and related risks of AI-based applications and services supplied by Chinese companies, and makes recommendations on how to deal with the challenges presented by China's AI ethics leadership ambitions. Of key importance will be to prioritize work on regulatory frameworks on the ethics of AI and to mitigate the use of Chinese AI-based applications in research and education.

Human-centredness and a strong focus on the protection of individual rights have been the core goals of European Union (EU) digitalization efforts in general, and the development and deployment of Artificial intelligence (AI) in particular. The General Data Protection Regulation (GDPR) demonstrates the EU's global leadership and leaves it well-placed to achieve something similar in the field of AI ethics.

The Chinese leadership under Xi Jinping has become increasingly active in shaping

and setting standards for AI ethics not only at home, but also in international institutions. Any interest in or concern about human life and dignity in Beijing in connection with the potential misuse of AI is to be welcomed. However, it is important to be aware that the Chinese leadership has repeatedly emphasized "national security" and "cyber sovereignty" as all-pervading governance principles, solely defined by and to serve the Chinese Communist Party (CCP).²⁴⁹ In addition, Beijing is increasingly

²⁴⁹ Katja Drinhausen and Helena Lagarda, *Comprehensive National Security: How Xi's Approach Shapes China's Policies at Home and Abroad*, Mercator Institute

for China Studies (MERICS) China Monitor, 15 September 2022,



using international institutions to counter what it regards as a “Western-dominated” global order, and using the same justification to redefine “legal systems” and “social stability” in its own authoritarian/totalitarian context.

Therefore, statements by the Chinese party-state on AI ethics, such as that “governments should, in light of their own stage

of AI development as well as social and cultural characteristics, and in accordance with the new features of scientific and technological innovation, gradually establish AI ethical systems suited to their national conditions”,²⁵⁰ must be contextualized with Chinese domestic law and practice, and the EU’s interests and vulnerabilities.

State of play of AI ethics in China and the EU

An analysis of the differences between the overarching goals, regulatory frameworks and practices for interacting with commercial and societal actors is key to understanding the incentives and disincentives of

the actors involved in shaping, developing and using AI. Figure 8.1 provides an overview of the key dimensions of AI ethics in the EU and China.

The actors shaping AI ethics in China

According to the *New-Generation AI Development Plan* issued by the State Council, the Leading Small Group on the Construction of Reform and Innovation Systems in Science and Technology has been assigned to coordinate and deliberate on the key tasks, policies and work priorities linked to the overall development of AI. The current head of the Leading Small Group, Liu He, is due to step down from all his posts in March 2023. His potential successor as Vice-Premier in charge of economics and finance is He Lifang, currently head of the National Reform and Development Commission (NDRC), in charge of traditional

industry-/sector-specific policy. It will be interesting to see to what extent the NDRC and/or people linked to He will be involved in implementing tasks on – and thus also gaining access to the budget for – AI policy. The *Ministry of Science and Technology (MOST)* has been tasked with shaping the governance of AI ethics. Interestingly, MOST is currently also managing the New-Gen AI Development Plan Promotion Office, which is supposed to drive implementation of key science and technology projects related to AI, and has a coordinating function regarding other tasks/sub-plans, putting the Office (and MOST) in

<https://merics.org/sites/default/files/2022-09/Merics%20China%20Monitor%2075%20National%20Security_final.pdf>.

²⁵⁰ Ministry of Foreign Affairs of the People’s Republic of China, “Position Paper of the People’s Republic of China on Strengthening Ethical Governance of

Artificial Intelligence (AI)”, Xinhua, Updated 17 November 2022, accessed 1 December 2022 at <http://english.scio.gov.cn/international/exchanges/2022-11/17/content_78524156.htm>.



DIMENSION	EU	CHINA
Overall strategic goal	<ul style="list-style-type: none"> • Enable the development and uptake of AI in the EU; • make the EU the place where AI thrives from the lab to the market; build strategic leadership in high-impact sectors 	<ul style="list-style-type: none"> • Become the global AI leader by 2030; AI to “enhance national competitiveness and protect national security”; • establish an ethical framework with “Chinese characteristics” for strengthening a “centralized and united” CCP leadership
Role of humans/ human factor	<ul style="list-style-type: none"> • Ensure that AI works for people and is a force for good in society; • creation of design guidelines for ethics-compliant AI systems 	<ul style="list-style-type: none"> • A focus on “the well-being of humankind” (in English, often misleadingly translated as “human wellbeing”); • a more collective, state-centred view; • and “respecting [but not complying with] the demand for human rights [not human rights per se]”
Legal framework	Provisions on the creation of a legal framework, which is expected to be operational in 2024	<ul style="list-style-type: none"> • Three stages of implementation: • implementation of “some parts” in 2020, completion of “initial stage” by 2025, finalization by 2030; • linked to overall development timetable; • ethics one item at the bottom of the list
Standardization efforts	The EU has specific provisions on the creation of AI standards in its general 2022 Rolling Plan for ICT standardization	<ul style="list-style-type: none"> • Ethics is mentioned as a focus research area to be completed by 2021; • linked with security in the goal to complete; • standards on key AI applications/ sectors by 2023 but low priority (52nd of 53 standards)
Role of industry	The EU has put in place instruments to support research at the academic and industrial levels that target the use of AI. One notable example is the call for funding by the European Innovation Council under EIC Pathfinder	<ul style="list-style-type: none"> • Companies (and researchers) are part of an AI governance committee in the Ministry of Science and Technology; • companies have published two sets of (non-binding) principles on governance and self discipline; • strong call for companies to self-regulate but party-state entities are never mentioned
Role of civil society	On 30 November 2021, European Digital Rights (EDRI) and 119 civil society organizations launched a collective statement calling for an Artificial Intelligence Act that foregrounds fundamental rights	<ul style="list-style-type: none"> • Officially very limited and guided participation through quasi-parliamentary sessions of the National Political Consultative Conference; nominal possibility of providing feedback during the process of soliciting opinions on draft regulations; • strong emphasis on paternalistic “guiding” of the public on “ethical awareness”

Figure 8.1 – Key dimensions of AI ethics in the European Union and China



the operational lead of the overall AI strategy. Coordinated by the Office, 15 other ministries or institutions with a ministerial-like ranking – including three linked to the military, among others the powerful Office of the Commission for Civil-Military Integration – are mentioned as being involved.²⁵¹

The Office was set up in 2017 following “notification of the new generation ai development plan” by the State Council. The current party secretary and minister for MOST, Wang Zhidong, also heads the Office. However, Wang was not re-selected as a member of the CCP Central Committee and will therefore also be stepping down in March 2023.

In 2019, MOST set up a *National New-Gen Artificial Intelligence Governance Specialist Committee*, which comprises at least seven scholars and is currently led by Xue Lan, an internationally renowned Professor of Public Policy and Management at Tsinghua (Qinghua) University, where he is also Director of the Institute for AI International Governance. The Specialist Committee has thus far issued two sets of AI ethics specifications, in 2019 and 2012, confirming China’s overall party-state-centric orientation

and a more collective “humankind” direction for AI ethics priorities.

The *Standardization Administration of China* (SAC) is responsible for setting up an overarching system for national AI standards, as well as other systems for other industrial and technology standards, and introducing these national standards into international standard setting bodies. “Ethics” is defined as one of 53 stand-alone standard families on AI. Although placed in the same box as “security”, the description is the shortest of all the standard categories and notes that the task is “to standardize demands arising from a conflict between AI services with traditional moral and legal procedures”. No further explanation is offered of what is meant by traditional morals or legal procedures. Health, traffic and emergency response are named as foci for research.²⁵² It is notable that China has already begun shaping international AI standards. In August 2022, SAC successfully pitched its own standards for AI medical devices to the International Institute of Electrical and Electronics Engineers.²⁵³

The *China Cybersecurity Administration* (CAC) oversees all AI cyberspace applications. In 2019, the CAC started to regulate the use of AI-based facial recognition software, which included a crackdown on

²⁵¹ International Research Collaboration Platform, “科技部召开新一代人工智能发展规划暨重大科技项目启动会” [The Ministry of Science and Technology held a new generation of artificial intelligence development plan and a major science and technology project launch meeting], 12 November 2017, accessed 1 December 2022 at <<http://www.ircip.cn/web/1044764-1044764.html?id=26645&newsid=1118169>>.

²⁵² Standardization Administration of China (SAC), “国家新一代人工智能标准体系建设指南” [Guidelines

for the Construction of the National New Generation Artificial Intelligence Standard System], 9 August 2020, accessed 1 December 2022 at <<http://www.sac.gov.cn/sxxgk/zcwj/202101/P020210122407767317794.pdf>>.

²⁵³ Zhongguoyiliaobao (China Medical News), “我国主导的IEEE人工智能医疗器械全球标准发布” [China-led IEEE global standards for artificial intelligence medical devices released], 24 August 2022, accessed 1 December 2022 at <http://k.sina.com.cn/article_7517400647_1c0126e4705903r9hz.html#>.



deepfakes, and issued regulations to protect personal biometric information. The most recent proposal in January 2022 specifies that deepfakes (deep synthesis services, 深度合成服务 in Chinese) must “... respect social public morals and ethics, and uphold the correct political line, direction of discourse and tendency of values” (坚持正确政治方向、舆论导向、价值取向). Seemingly non-political categories that revolve around ethics are given a clear political framing.²⁵⁴ The CAC has also issued joint rules with the Ministry of Industry and Information Technology (MIIT), the Ministry of Public Security and the State Administration for Market Regulation to platform companies that use algorithmic recommendations, requesting them to share information about their algorithm and holding them accountable for algorithmic discrimination or misuse of personal data. However, the “promotion of core socialist values and the protection of national security and social public interest(s)” is also mentioned at the very beginning, and should be interpreted as setting the guiding principles for the more rules-based, specific paragraphs.²⁵⁵

A first batch of companies has already disclosed their algorithms to the CAC. This has raised questions such as why some companies, including Bytedance, have

registered different numbers of algorithms under different categories for different apps; and why other companies, many with allegedly close ties to the party-state, such as Huawei (Smart TV) or Megavii (facial recognition), have not yet publicly disclosed their algorithms.²⁵⁶

Both company representatives and university scholars have participated in state agencies’ expert consultation groups and influenced the evolving regulations. Under the leadership of a state-led think tank, the China Academy of Information and Communications Technology (CAICT) in the MIIT, academics and entrepreneurs have devised several sets of AI self-regulatory/self-governing ethical standards, such as the Pledge on AI Industry Self-Discipline or the Beijing AI principles. CEOs, including Robin Li from Baidu and Pony Ma from Tencent, have not just contributed to state-led initiatives and regulations, but proposed AI ethics principles to the National Political Consultative Conference, set up as a sounding board for the quasi-parliament, the National People’s Congress.²⁵⁷ The general public or informed public stakeholders such as IT engineers or students have not been given an opportunity or a channel to affect developments in the field of AI ethics, but their contribution by posing questions

²⁵⁴ China Cyberspace Administration, “国家互联网信息办公室关于《互联网信息服务深度合成管理规定（征求意见稿）》公开征求意见的通知”, 28 January 2022, accessed 2 December 2022 at <http://www.cac.gov.cn/2022-01/28/c_1644970458520968.htm>.

²⁵⁵ CAC, “互联网信息服务算法推荐管理规定”, 4 January 2022, accessed 2 December 2022 at <http://www.cac.gov.cn/2022-01/04/c_1642894606364259.htm>.

²⁵⁶ Kevin Xu, “So Which Algorithms Do the Chinese Regulators Have?”, *Interconnected*, 21 August 2022, accessed 2 December 2022 at <https://interconnected.blog/so-which-algorithms-do-the-chinese-regulators-have/>

²⁵⁷ Rebecca Arcesati, “Lofty principles, conflicting incentives: AI ethics and governance in China”, *MERICs China Monitor*, 24 June 2021, accessed 2 December 2022 at <https://meric.org/en/report/lofty-principles-conflicting-incentives-ai-ethics-and-governance-china>



and discussing them publicly online has pressured both party-state and commercial actors to understand that users increasingly

care about issues such as privacy and transparency.²⁵⁸








ACTOR TYPE	NAME OF KEY ACTOR	DESCRIPTION	KEY TASK	PRIORITY
Policy institution	 Leading Small Group on Construction of the Reform and Innovation System for Science and Technology 国家科技体制改革和创新体系建设领导小组	Under the State Council	Coordinates and deliberates on key tasks, policies and work priorities regarding the overall development of AI, based on the New-Generation AI Development Plan issued by the State Council	●
Policy institution	 New-Gen AI Development Plan Promotion Office 新一代人工智能发展规划推进办公室	Managed by the Ministry of Science and Technology (MOST), Operational lead on the overall AI strategy	Drives implementation of key science and technology projects related to AI; coordinating role in other tasks/subplans	◐
Individual researcher	 Xue Lan 薛澜	Director of the Institute for AI International Governance, Qinghua University, Beijing	Heads the National New-Gen. Artificial Intelligence Governance Specialist Committee, which comprises at least seven scholars	◐
Policy institution	 Standardization Administration of China (SAC) 中国国家标准化管理委员会	Standards	Responsible for setting up the overall AI standard system; "Ethics" is defined as one of 53 stand-alone standards	◐
Research institution	 China Academy of Information and Communications Technology (CAICT) 中国信息通信研究院	Think Tank of the Ministry of Industry and Information Technology (MIIT)	Provides advice to industry on critical issues such as standards, technical trials and emerging technology sectors such as AI	◐
Company	 ByteDance 北京字节跳动科技有限公司	Chinese internet technology company headquartered in Beijing but incorporated in the Cayman Islands	Has invented and owns TikTok, the most popular video platform among young people in Europe	◐
Company	 Megvii 旷视科技	Based in Beijing; technology company that designs image recognition and deep-learning software	Develops AI technology for business and the public sector; Face++ often used by researchers; known entanglement in Xinjiang	◐

Figure 8.2 – Actors to watch

²⁵⁸ Yishu Mao and Kristin Shi-Kupfer, "Online public discourse on artificial intelligence and ethics in China: Context, content, and implications", AI

Society, 16 November 2022, accessed 3 December 2022 at <https://link.springer.com/article/10.1007/s00146-021-01309-7>



Criteria for assessing Chinese AI-based consumer applications for use within the EU

The criteria listed below are intended to be useful for assessing the ethical dimensions of and potential risks related to the use of Chinese AI-based consumer applications and services by European users.²⁵⁹ The ordering of the criteria is not informed by a weighted hierarchy of likelihood of impact, but provides a systematic and comprehensive framework that can be refined in follow-up studies.

At the macro level of the regulatory and political environment in China, such criteria, among others, are:

- There is potential for legal requests for data to be made by the Chinese authorities to Chinese companies, linked to the National Security Law. This might include the user data of high-level managers/politicians on TikTok and/or WeChat for blackmail purposes, data on a cross-national video samples and/or data on members of the Chinese diaspora using Face++.
- *The potential for the Chinese government to gain access to algorithms:* Bytedance has registered the algorithm of its app Douyin under the category “Personalization and Content Pushing”. Publicly available information on the

extent to which the algorithms of Douyin and TikTok are similar does not allow a clear judgment. The possibility that the Chinese government has detailed knowledge of how TikTok works cannot therefore be completely ruled out.²⁶⁰

- *Evidence of use of some Chinese AI-based apps as part of repressive surveillance systems in Xinjiang and other parts of China:* Megvii’s foreign users of Face++ might help to improve its product or help it to gain market share or increase exports.
- *The likelihood of apps being banned by allied/partner countries:* There are calls in the US to ban TikTok and/or other AI-based tools for communication and research (Face++). These may not affect collaboration and trust among the actors involved, but could affect joint research projects as the US might ask European researchers not to use AI-based services provided by Chinese companies.

At the micro-level, referring to app/in-app features, among other things:

- *The quality and detail of the overall information provided in English.* Compared to Chinese language versions,

²⁵⁹ To complement the other chapters in this volume, this paper focuses on AI-based applications and services for consumers. The authors have taken the video app TikTok and the chat and news app WeChat as well as the facial recognition app Face++ as their references as these are widely used in Europe. Fully fledged case studies proved to be beyond the scope and purpose of this policy paper. The authors are working on

more detailed case studies and would be glad to provide a more detailed analysis of the apps mentioned on another occasion.

²⁶⁰ Zeyi Yang, “TikTok’s secret sauce”, Protocol, [n.d.], accessed 4 December 2022 at <<https://www.protocol.com/newsletters/sourcecode/two-sides-same-code?rebellitem=1>>.



there is highly ambivalent information on Megvii's Face++²⁶¹ regarding storage of data in China or Canada. There are also clearly stated content limitations and legal liabilities for international developers based on Chinese regulations, among other things on "Provoking resentment, discrimination and unity among the nationalities". A European researcher using Face++ for research related to Xinjiang or Tibet could face penalties.

- *The features of the algorithm:* One of the major factors responsible for the success of Tik Tok is its recommendations system, which provides the content for the "For You" page. Such systems seek to predict which videos will pique a viewer's interest. According to the official Tik Tok website,²⁶² the recommendations are based on a number of factors:
 - *User interactions:* these include the videos a user likes or shares, the accounts s/he follows, comments s/he posts and content s/he creates, as well as information on whether a user watches a longer video from beginning to end;
 - *Video information:* this might include details on captions, sounds and hashtags, or whether the video's

viewer and creator are both in the same country;

- *Device and account settings:* this includes the user's language preference, country setting and device type.

Each of these factors receives a different weight. For example, device and account settings receive a lower weight as they are less related to a user's preferences. Videos are then ranked to determine the likelihood of a user's interest in a given piece of content, and then finally provided in the "For You" feed. Neither follower count nor whether the account has had previous high-performing videos are direct factors in the recommendation system.

Notably, the recommendations are typically not good or appropriate for new users. This is related to a common issue in recommender systems known as the "cold start problem", as the system cannot draw any inferences for users or items about which it has not yet gathered sufficient information. In an informal test conducted by *The Guardian* with three users,²⁶³ however, it emerged that new users typically receive viral or humorous videos, but within a few days the algorithm can profile the user well enough to provide generally appropriate content in the feeds.

²⁶¹ Service Agreement for Developer on the Face++ Artificial Intelligence Open Platform, accessed 4 December 2022 at <<https://www.faceplusplus.com/terms-of-service/>>.

²⁶² TikTok, How TikTok recommends videos #For You", 18 June 2020, accessed 4 December 2022 at <https://newsroom.tiktok.com/en-us/how-tiktok-recommends-videos-for-you>

²⁶³ Kari Paul, Johana Bhuiyan and Charlotte Simmonds, "How does TikTok's uncanny algorithm decide what you see? We tested it on three people", *The Guardian*, 6 November 2022, <<https://www.theguardian.com/technology/2022/nov/06/tiktok-algorithm-experiment-new-accounts>>.



However, it is likely that the recommendation system also uses several other inputs, as indicated in the Privacy Policy document published by the company.²⁶⁴ It states that a number of other sources of information about the user are collected beyond the simple profile information and the content mentioned above.

- *The scope and transparency of the data collected:* Of the information directly provided by users, Tik Tok collects users' direct messages, contacts and purchase information (e.g., payment card, PayPal), as well as its responses to surveys, research and promotions, and the information provided when users contact the company. The information automatically collected comprises:
(a) technical information, such as device model, operating system, keystroke patterns or rhythms, IP address and system language; (b) location information (e.g. country, state or city); (c) usage information, such as the content a user views, duration and frequency of use and the user's engagement with other users; (d) content characteristics and features, such as identification of objects and scenery, the existence or location in an image of a face or other body parts and the text of words spoken; (e) inferred information (e.g. age-range and gender); and (f) Cookies,

to remember a user's language preferences. Furthermore, Tik Tok acquires information from external sources such as advertising, measurement and data partners, third party platforms and partners, as well as a less specific category of "others". Of the aspects listed above, the "content characteristics and features" require careful attention, as these may be related to the automatic collection of biometric data from users and the content they provide. In 2021, TikTok updated its privacy policy to allow the app to collect biometric data on US users, including faceprints and voiceprints.²⁶⁵ This led to questions being raised in the US Senate, but the company's answers on the topic have been vague and inconclusive.²⁶⁶

- *Scope of data transfer:* TikTok has recently clearly stated that data from European users can be accessed and thus utilized by its staff in China, as well as in other countries such as Israel, Brazil and the US.²⁶⁷ However, clear information on data transfers to third parties in other countries cannot be found in their user regulations.²⁶⁸ WeChat provides information on data transfer, stating that: "Our servers are located in Singapore and Hong Kong SAR.... Our other support, engineering and other teams located around the world

²⁶⁴ TikTok, "Privacy Policy", Updated 2 November 2022, accessed 4 December 2022 at <<https://www.tiktok.com/legal/page/eea/new-privacy-policy/en>>.

²⁶⁵ Dan Milmo, "TikTok tells European users its staff in China get access to their data", *The Guardian*, 2 November 2022, <<https://www.theguardian.com/technology/2022/nov/02/tiktok-tells-european-users-its-staff-in-china-get-access-to-their-data>>.

²⁶⁶ Sarah Perez, "TikTok claims it's not collecting US users' biometric data, despite what privacy policy says", TechCrunch, 14 September 2022, accessed 4 December 2022 at <<https://techcrunch.com/2022/09/14/tiktok-claims-its-not-collecting-u-s-users-biometric-data-despite-what-privacy-policy-says/>>.

²⁶⁷ Dan Milmo (note 265).

²⁶⁸ TikTok Privacy Policy (note 264).



(including Singapore, Hong Kong SAR and the Netherlands) that deliver WeChat to Support you have access to your information. (...) We share your data with selected recipients who have the legal basis and authority to request such data. These categories of recipients include government agencies, public authorities, regulators, courts and law enforcement agencies".²⁶⁹

- *Overall transparency of user rights and protection:* Tik Tok has a Transparency Centre, which provides various reports,²⁷⁰ such as a Community Guidelines Enforcement Report, a Government Removal Requests Report and an Intellectual Property Removal Requests Report. Such reports claim that Tik Tok algorithms are devised in ways that take account of the safety and security of users, including from cyberattacks and fake news. However, none of these reports detail how users' data

are utilized. Moreover, the legal aspects related to government restrictions are not discussed in detail.

- *Non-transparent obstacles to cross-border usage/communication* also constitute criteria that are useful for assessing ethical risks related to an AI-based consumer app. For example, WeChat messages regarding "sensitive content" might appear in a chat history on a European interface, which the Chinese counterpart does not see in her/his chat history with a European counterpart. *Content censorship* has not thus far been clearly detected with regard to TikTok or WeChat Europe, but nor have *platform democratization opportunities* for users to provide feedback and shape development through participatory channels within the companies. Based on publicly available information, all three companies are yet to set up such structures.

Policy recommendations for the EU / EU member states in relation to the different dimensions of strategic autonomy

- *Prioritize work on regulatory frameworks on AI ethics.* To deter the Chinese government's efforts to position itself as a pioneer in enacting binding regulatory frameworks on AI ethics, the EU should finalize its own regulations on AI ethics as soon as possible. In addition, EU member states and relevant commercial as well as scholarly

actors should, ideally in a coordinated manner, actively contribute to AI standardization efforts within international standardization organizations.

- *Assess the use of Chinese AI-based applications and services in the fields of research and education, and the potential security risks.*

²⁶⁹ WeChat, "WeChat Privacy Policy", 9 September 2022, accessed 4 December 2022 at <https://www.wechat.com/en/privacy_policy.html>.

²⁷⁰ TikTok Transparency Center, "Our Commitment", accessed 4 December 2022 at <<https://www.tiktok.com/transparency/en-us>>.



Depending on the scope of usage, targeted information about potential risks and side-effects should be prepared and communicated, for example, through actor-specific hands-on workshops, or an actor-specific ban on apps such as WeChat and TikTok on mobile phones used for work purposes

- *Balance data privacy with the need to be competitive.* The EU needs to be aware of the fact that totalitarian regimes have total control over data regardless of user privacy. Since AI is a data-driven approach, the more data there is and the higher the quality of that data, the more efficient the algorithm will become. This might therefore give Chinese companies a competitive advantage over European companies.
- *Be aware that the ethics dimension adds to the pressure to create independent supply chains.* Different norms and values are at the core of the growing bifurcation of the global order. Companies therefore increasingly need to factor in whether a supplier is from a like-minded country to avoid fall-outs and pinch points in the supply chain. Cost-efficiency is no longer the core factor in building supply chains.
- *Carefully monitor continuity and potential changes in terms of institutional and personal responsibilities regarding the coordination and implementation of AI ethics-related policymaking.* As the Chinese party-state transitions towards a new state leadership in March, priorities and responsibilities might be subject to change not only due to conflicting policy goals, but also linked to jockeying for position and budgetary infighting.
- *Crosscheck the English version of relevant documents with original Chinese sources.* English versions provided by official Chinese institutions sometimes differ in important nuances from the original Chinese and this might lead to wrong assumptions. For example, “well-being of humankind” in the original Chinese clearly emphasizes the collective while “human well-being” in the official English version potentially refers to the individual and is more appealing to European/English-speaking readers.
- *Be aware that the Chinese government often uses references to “culture”, “the Chinese people” or “national conditions” to reject or circumvent global frameworks.* Beijing deliberately plays on a European reflex of self-criticism with regard to potential “Eurocentrism” and questions of “universal values”. In addition, Beijing is increasingly using international institutions to counter what it regards as a “Western-dominated” global order by using the same wording, such as “legal systems” or “social stability”, in their own authoritarian/totalitarian



contexts to reject global meanings/frameworks.

- *Increase media literacy on the strong dependency / disinformation potential of TikTok among young people and in schools, including by the political labelling*

of accounts and use of fact-checking options. TikTok has become a primary source of news and political/social information for teenagers. They therefore need to be equipped with easy, hands-on techniques for content questioning and fact-checking.

Authors:

Kristin Shi-Kupfer is a professor of Contemporary China Studies/ Focus on Digital media at the University of Trier. Contact: shikupfer@uni-trier.de.

Luca Turchet is an associate professor at the Department of Information Engineering and Computer Science, University of Trento. Contact: luca.turchet@unitn.it.



Digital Power China

A European research consortium