JANUARY 2020

The U.S.-China Race and the Fate of Transatlantic Relations

Part 1: Tech, Values, and Competition

Andrés Ortega

Executive Summary

Technological dominance is a key dimension of the competition between the United States and China, one that is further stressing transatlantic relations. This paper analyzes the narrative and reality around the nexus between new technologies, defense of shared values, and regulation. Values are a rising element in the transatlantic debate over technology, particularly with the proliferation of artificial intelligence (AI) surveillance systems and other aspects of exportable techno-authoritarianism. Both the United States and Europe must update their human rights approaches for the digital era, and clear values around new technologies must be defined.

The new European Commission in Brussels, as well as some EU member states, see the need to deal with great power competition as a strategic priority and as a way to achieve "technological sovereignty." They have identified the nexus between the industrial and digital agendas and regulation as key. From this, three areas of competition and cooperation between the United States and Europe emerge, all of which relate to China's capabilities: fifth-generation wireless technology (5G), AI, and web-based services. Differences in regulation will be a sticking point in transatlantic relations, but there need not be perfect alignment between the United States and the European Union. Nonetheless, both sides have to push for global regulations in fields such as AI ethics, cybersecurity, and internet governance to avoid China or others filling the void. The article offers some ideas for a transatlantic agenda on technology as it relates to China. A second, forthcoming part of this paper will discuss other geopolitical issues, beyond technology, related to the impact of U.S.-China competition on transatlantic relations and on European unity.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Introduction

The competition between the United States and China will not only determine in great part the structure of global geopolitics and economics in the years to come but also impact transatlantic relations and even European unity. The emergence—or re-emergence—of China and other powers coincides with an era of intense changes in technology and its social and global effects, particularly in geopolitics. The course of U.S.-Chinese relations, especially in technological terms, could undermine or reinforce transatlantic ties, European cohesion, and the global order. Despite a certain rapprochement in the technological field between European and U.S. attitudes toward China (including through shared values), some deep differences persist. These must be managed and, whenever possible, bridged with a new agenda. This should be a priority for policymakers in EU member states and institutions, though it will not be easy.

The current U.S. administration and some U.S. companies are in the process of designing a new strategy toward China. Some important elements of that strategy, based on trade and deterrence, are already in place. As the European Union is also engaged in such an exercise, common ground could be found. The European Union, however, is not engaged in superpower rivalry and will not have the same relationship with China as the United States; instead, it seeks a "new approach."[1]

The U.S. "competition" or "disengagement" with China—rather than "conflict" or "confrontation," as some U.S. officials put it—will be a lasting element of U.S. strategy, leading to divergence between the United States and China, at least in the near term.[2] This strategy, as it regards the technological dimension, has wide bipartisan support and buy-in from the tech, national security, and human rights communities but less support in the business arena.

This paper approaches the issue of U.S.-Chinese relations and their impact on Europe in two separate parts. This piece focuses on technological issues given their prominence in the bilateral relationship. It examines the nexus between technology, data protection and values, and regulatory differences and competition. A blunt consideration underpins this analysis: even with its major companies and global power, the United States is too small to deal with the challenges ahead (not limited to China) and will need partners and allies, principally Europe, which also needs the United States. Yet in discussions about China, the critical role of allies is often absent from the U.S. official discourse, even at the highest levels.[3]

The change in approach toward China from the United States and the European Union, and even NATO, has been relatively sudden. Long focused on other issues, they are now starting to grapple with technology and, increasingly, values that relate to it (e.g., democracy, open societies), a shift partly necessitated by China's own focus on technological advancement. In a 2019 defense white paper, *China's National Defense in the New Era*, China recognizes that "international strategic competition is on the rise;"[4] this competition is highly complex and set in a framework of mutual, if asymmetrical, interdependence. China's main, publicly stated objective is to fulfill the "China dream" of becoming a "moderately well-off society" by

[1] Julie Smith and Torrey Taussig, "The Old World and the Middle Kingdom," *Foreign Affairs* 98, no. 5 (August 2019), https://www.foreignaffairs.com/articles/china/2019-08-12/old-world-and-middle-kingdom.

[2] Randall Schriver, "Global China: Assessing China's Growing Role in the World and Implications for U.S.-China Strategic Competition," (conference remarks, Brookings Institution, October 1, 2019), https://www.brookings.edu/events/global-china-assessing-chinas-growing-role-in-the-world-and-implications-for-u-s-china-strategic-competition/.

[3] Mike Pence, "Vice President Pence Delivers Inaugural Frederic V. Malek Public Service Leadership Lecture," (conference remarks, Wilson Center, October 24, 2019), https://www.wilsoncenter.org/event/live-webcast-vice-president-pence-delivers-inaugural-frederic-v-malek-public-service.

[4] Anthony H. Cordesman, *China and the United States: Cooperation, Competition, and/or Conflict* (Washington, DC: CSIS, October 2019), https://www.csis.org/analysis/china-and-united-states-cooperation-competition-andor-conflict.

2021, a fully developed country by 2049 (the 100th anniversary of the founding of the People's Republic of China), and a major technological power, as stated in its Made in China 2025 strategy (MIC2025).[5,6]

The United States sees China as the only geopolitical, economic, and eventually military power that could rival or challenge U.S. power in the twenty-first century. And while Russia is still seen as an existential threat due to its nuclear capacity and its military renewal, it is no longer perceived as a superpower. In the U.S. vision for the century, technological dominance plays a central role. U.S. strategy thus primarily aims to prevent China from becoming overall more powerful than the United States.[7] Though there is no unanimity on this aspect, the strategy also aims to slow Chinese progress, especially in the technological field, by decoupling as much as possible from the Chinese ecosystem. This is not meant to produce a new Cold War setting but a situation of competition and interdependence.[8] Competition outside of a Cold War logic does not imply a zero-sum game, however; the United States will continue to trade with China in many areas.

Values in Tech

The United States, Europe, and China have realized technology is neither culturally neutral nor devoid of values; it showcases deep cultural differences between systems. Thus, technology ushers in a clash of cultures to which insufficient attention has been paid. For the transatlantic community, policy toward China in the technological field can be a way to inoculate free and open societies against negative Chinese influence.

Values are a central part of the competition for soft power between the United States and China (and Europe). According to the University of St. Gallen's Tomas Casas i Klett, it is a "competition for global affection and cognitive bandwidth that is tied to [the two major powers] individually" and constitutes the "contest for the 21st century's grand narrative."[9] Values, which grow in a sociopolitical context, are also embedded in tech, which in turn fuels soft power as well as hard, military power.

The United States places more emphasis than Europe on China exporting its authoritarian model, though for China it is also a matter of creating situations of influence, according to some experts.[10] Apart from direct political influence, China uses its surveillance technology to export techno- or digital authoritarianism, defined as "the use of digital information technology by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations," a process that is "reshaping the power balance between democracies and autocracies."[11,12] There are currently 64 states in the world that use Chinese AI surveillance systems, which are sometimes developed with the help of Western tech companies. The West is not exempt from this issue, as shown by the 2013 leaks by Edward Snowden and the surveillance scandals of such U.S. firms as Facebook and Apple. However, the major difference is that U.S. and European companies are not forced to give that information to the government, while companies operating in China

[5] Robert Lawrence Kuhn, "Xi's Chinese Dream," *New York Times*, June 4, 2013, https://www.nytimes.com/2013/06/05/opinion/global/xi-jinpings-chinese-dream.html.

[6] U.S. Chamber of Commerce, *Made in China 2025: Global Ambitions Built on Local Protections* (Washington, DC: 2017), https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf.

[7] President of the United States, *National Security Strategy of the United States of America* (Washington, DC: 2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[8] Andrés Ortega, "The US Versus China: The Names of Things," Real Instituto Elcano, March 9, 2019, https://blog.realinstitutoelcano.org/en/the-us-versus-china-the-names-of-things/.

[9] Tomas Casas i Klett, "Beyond Sino-American Rivalry: Whose Global Narrative?" *Globalist*, October 6, 2019, https://www.theglobalist.com/united-states-china-robert-schiller-the-west/.

[10] Conversation with Dan Hamilton.

[11] International Republican Institute, *Chinese Malign Influence and the Corrosion of Democracy* (Washington, DC: 2019), https://www.iri.org/sites/default/files/chinese_malign_influence_report.pdf.

[12] Alina Polyakova and Chris Meserole, *Exporting Digital Authoritarianism: The Russian and Chinese models* (Washington, DC: Brookings Institution, August 2019), https://www.brookings.edu/research/exporting-digital-authoritarianism/.

(be they Chinese or foreign) may be requested (and forcibly compelled) to do so. Furthermore, China uses this information for political control, while the West sees mostly commercial or informational purposes.

According to a recent report, of 176 countries surveyed, at least 75 are actively using AI technologies for surveillance purposes.[13] Indeed, there are almost as many surveillance cameras in London as in Beijing (and actually more, if measured per capita).[14] But the use and goals of AI differ across the world. China and other techno-authoritarian regimes have leveraged AI to become surveillance states; in the West, AI has underpinned a form of consumer surveillance in the service of capitalism (though some elements are used for security purposes as well).[15]

The United States' 2017 National Security Strategy, drafted under the current administration, addressed the issue of political and social values ("We will never lose sight of our values and their capacity to inspire, uplift, and renew"[16]), but the administration has only recently begun using values as a tool of policy in its relations to China. In October 2019, violation of human rights of Uighur Muslims in the province of Xinjiang prompted the Department of Commerce to blacklist eight advanced Chinese AI and facial recognition firms (among a total of 28 entities) that were used to put hundreds of thousands of people in detention camps.[17] It marked the first time the Trump administration based this kind of action on human rights (as tied to values and technology), and the United States was the first country to do so. It is an open question whether the Department of Commerce has taken this step to defend human rights or to slow down AI advances in China, as the eight blacklisted firms are some of China's most advanced. It is clear, however, that the U.S. focus on values in regard to China is growing. Recent speeches by Vice President Mike Pence and Secretary of State Michael Pompeo have pointed in that direction.[18,19] The U.S. government is also demanding more of civil society and of companies that cooperate with China.[20] This has created an unresolved dilemma between business interests and principles.

To adapt to the digital era and China's approach, both the United States and Europe must update their human rights approach. The United States should be conscious that a measure of its soft power is also in its software. Human rights must be embedded in the digital and AI culture in ways that ensure their protection in times of increased surveillance and repression capabilities. As this paper discusses, there are differences between the United States and Europe on issues such as privacy, but these should not prevent the renewal of policies on human rights and the defense of shared values.

The Race for Technology Dominance

Europe and the United States have had, until recently, an almost exclusively economic approach to China, focused on mutual trade and investments. And though both are increasingly aligned in their approach to China, Europeans still see a major role for China in a global economy that should ideally be kept open to all. This is visible in the European Union's stated goal to achieve a Comprehensive Investment Agreement with Beijing at the next EU-China summit in 2020. This should include, among other items, the acceptance

[13] Steven Feldstein, "The Global Expansion of AI Surveillance," Carnegie Endowment For International Peace, Working Paper, September 17, 2019, https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

[14] Madhumita Murgia, "How London Became a Test Case for Using Facial Recognition in Democracies," *Financial Times*, August 1, 2019, https://www.ft.com/content/f4779de6-b1e0-11e9-bec9-fdcab53d6959.

[15] Shoshana Zuboff, *The Age of Surveillance Capitalism* (New York: Public Affairs, January 2019).

[16] President of the United States, *National Security Strategy of the United States of America*.

[17] Ibid.

[18] Pence, "Frederic V. Malek Public Service Leadership Lecture."

[19] Michael R. Pompeo, "The China Challenge," (speech, Hudson Institute, October 30, 2019), https://www.state.gov/the-china-challenge/.

[20] Pence, "Frederic V. Malek Public Service Leadership Lecture."

of a WTO Government Procurement Agreement, improved market access, and a prohibition of forced transfer of technology for foreign companies that operate in China. That summit will be held under the German presidency of the European Union; Chancellor Angela Merkel has said relations with China will be a priority during her country's rotating EU presidency.[21]

Yet despite this seemingly welcoming tone, some European countries and the European Commission have started to change their position on Chinese investments in high-tech firms and in critical infrastructure. The alarm bell, or the *Sputnik moment*, came in 2016 when the Chinese Midea Group acquired German robot maker Kuka. Afterward, one study found that between 2014 and 2017, 64 percent of Chinese corporate investments above a 10 percent stake in German companies were in sectors prioritized by MIC2025.[22] Furthermore, in 2018 the majority of Chinese foreign investment in the IT industry and technology was in Europe, potentially due to restricted access to the U.S. market.

This changing tone is also reflected in the leadership transition in Brussels with the arrival of a new European Commission that prioritizes great power competition, and which has identified the nexus between industrial policy, digital agendas, and global governance as a key element of this competition. Recent EU decisions have highlighted a more cautious approach toward Chinese investments as well. In spite of some internal opposition, EU leaders finally approved the Investment Screening Regulation in April 2019 (coming into force in October 2020), a mechanism to oversee non-EU capital investments in strategic companies.[23] This screening should help prevent unwanted Chinese (and other) takeovers, though the final decision ultimately rests with member states. National screening processes have also been reinforced in some countries, such as Germany and Spain. In addition, the commission is designing a plan for a €100 billion (approximately $111 billion) European sovereign fund that could invest in strategic sectors where the European Union lags behind global rivals and that could intervene to protect strategic sectors, buying relevant companies when there is no European capital available (though it is unclear whether the new commissioners will push this plan forward).[24] Germany has designed such a fund at the national level to foil unwanted takeovers by non-European companies.[25] These efforts at the EU level still do not establish protective tools like the U.S. Foreign Investment Risk Review Modernization Act (FIRRMA) and the Committee on Foreign Investment in the United States (CFIUS), nor does the commission have executive powers in these areas—but it is a start.

It has become clear that technological dominance is an essential prerequisite of power in our world, including in the military realm. The arrival of China in the upper echelons of fields such as AI and biotechnology, for so long dominated by the United States, has provoked a certain alarm in the West. This alarm is also caused by China's at times dubious acquisition of Western technology—even as China moves to protect its own intellectual property, it is widely understood to be stealing it from abroad.[26] For

[21] Michelle Martin, "Germany Will Make ties with China a Priority During EU Presidency: Merkel," Reuters, October 17, 2019, https://www.reuters.com/article/us-germany-eu-china-idUSKBN1WW0WX.

[22] Cora Jungbluth, *Kauft China systematisch Schlüsseltechnologien auf? Chinesische Firmenbeteiligungen in Deutschland im Kontext von „Made in China 2025"* (Gütersloh, Germany: GED Studie, Bertelsmann Stiftung, 2019), https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/MT_Made_in_China_2025.pdf.

[23] "EU Foreign Investment Screening Enters Into Force," European Commission, April 10, 2019, http://trade.ec.europa.eu/doclib/press/index.cfm?id=2008

[24] Mehreen Khan, "EU Floats Plan for €100bn Sovereign Wealth Fund," *Financial Times*, August 23, 2019, https://www.ft.com/content/033057a2-c504-11e9-a8e9-296ca66511c9.

[25] Michael Nienaber, "Exclusive: Germany to Create Fund to Foil Foreign Takeovers After China Moves," Reuters, March 20, 2019, https://www.reuters.com/article/us-germany-industry-exclusive/exclusive-germany-to-create-fund-to-foil-foreign-takeovers-after-china-moves-idUSKCN1R10IR.

[26] W. C. Hannas, and Huey-meei Chang, *China's Access to Foreign AI Technology* (Washington, DC: Center for Security and Emerging Technology, September 2019), https://cset.georgetown.edu/wp-content/uploads/CSET-Chinas-Access-to-Foreign-AI-Technology-2.pdf.

these reasons, current U.S. policy seemingly aims to slow down China's technological progress through various methods (e.g., export interdictions for technologies and essential advanced components, such as the latest generation of semiconductors) and even to decouple as much as possible from the Chinese tech ecosystem (i.e., reducing mutual interdependence). At the very least, the policy aims to use U.S. leverage to renegotiate the terms of this interdependence, as the United States understands China's dependence on advanced U.S. technologies and research (especially in IT, biotechnology, and aerospace—excluding missiles). Indeed, Chinese attempts to match U.S. dominance in some fields, such as super-advanced semiconductors, have so far failed, but decoupling could potentially bring about the objectives it is trying to stop, that is, an increased national technological push by China.

Faced with U.S. and Chinese technological advances, Europe has lost the race for the first wave of AI and other technological fields. Nonetheless, European industry is highly diversified and more open to Chinese competition. Europe's weakness lies in a digital single market that is still not fully implemented, in an overabundance of companies in some fields (e.g., telecommunications), and in a lack of investment, private and public, in high-tech areas. And though World Bank data show the European Union has a high-tech export capacity, it could waste it if it does not update its technological field to remain competitive.[27]

The European Union and its member states are now launching a series of programs to overcome this gap, but it may be too little, too late unless it targets next generation technology. French President Emmanuel Macron talks about European "digital sovereignty,"[28] but what does "European" mean? France and Germany are giving primacy to a Franco-German cooperation, in particular in AI, as reflected in a bilateral cooperation treaty agreement signed in January 2019 that creates a joint virtual research and innovation center for AI and a digital platform for audiovisual and informational content.[29] While such cooperation is welcomed, it is neither comprehensive nor does it speak for all of Europe."

The issue of European digital sovereignty arises from the worry of European tech companies that they are in a technological "neocolonial" situation (or "techno-oligopolist dependency") with regard to some U.S. companies and even Chinese ones. This partly self-inflicted trap could force Europeans to choose between American and Chinese options, sometimes inadvertently (e.g., some applications' origins are unclear to most users).[30] And though Germany's Chancellor Merkel also supports this idea of digital sovereignty, and competition with Silicon Valley, for example, when urging Europe to seize control of its data from U.S. tech giants, it is unclear how likely this is in the near future.[31] The information economy and tech competition are clearly becoming central to the EU-U.S. relationship.

In recent years, three main ways of approaching data control and management have emerged in the United States, Europe, and China. In the United States, major companies such as Facebook, Apple, Netflix, Google, and Amazon have access to large amounts of consumer data, and these companies have successfully monetized this data. In the European Union, citizen and consumer rights are a priority, potentially at the expense of the competitiveness of companies, countries, or particular sectors (e.g., the EU General Data Protection Regulation (GDPR), which allows individuals to control their personal data but has placed the

[27] "High-Tech Exports," World Bank, https://data.worldbank.org.

[28] Emmanuel Macron, "France's New National Strategy for Artificial Intelligence," Elyseé, March 29, 2018, https://www.elysee.fr/emmanuel-macron/2018/03/29/discours-du-president-de-la-republique-sur-lintelligence-artificielle.

[29] "Traité franco-allemand d'Aix-la-Chapelle," Elyseé, https://www.elysee.fr/emmanuel-macron/traite-franco-allemand-aix-la-chapelle.

[30] For instance, this has happened with the app TikTok: "What's going on with TikTok, China, and the US government?", Vox, December 16, 2019. https://www.vox.com/open-sourced/2019/12/16/21013048/tiktok-china-national-security-investigation.

[31] Guy Chazan, "Angela Merkel Urges EU to Seize Control of Data From US Tech Titans," *Financial Times*, November 12, 2019, https://www.ft.com/content/956ccaa6-0537-11ea-9afa-d9e2401fa7ca.

burden on companies to comply). The third, most different model is China's: technology is sponsored by the state and the government has all the power to acquire citizens' data. The choice between these three models, and decisions about whether private companies, the state, or users themselves have ownership of people's data, will have tremendous implications for the future of the global economy and for geopolitics.[32]

Competition between these models to achieve technological dominance will be fierce, and economic reality will weigh on this choice. It may be that the veil of European naivete toward China has fallen,[33] but the reality of the interdependence is still abundantly clear. Europe must learn how to better manage it, especially through cooperation with allies like the United States, Japan, and others.

Three Areas of Competition

There are three key areas of U.S.-Chinese technological competition that put Europeans in a difficult position: 5G, AI and semiconductors, and web-based services.[34] All three impinge on trade and on deeper security issues, the latter of which incentivizes cooperation between the United States and Europe, as there is transatlantic agreement over the threat posed by Chinese cyber capabilities, including intellectual property theft, cyberattack capabilities, and information warfare.[35] The United States has pushed for cooperation on the issue, as has NATO, with an initiative gathering some 30 countries (not all European) on "Advancing Responsible State Behavior in Cyberspace." This effort aims to create real consequences for harmful behavior in cyberspace (without mentioning China or Russia by name) and aims to develop a common culture.[36] It a foundation from which U.S. and European cooperation can grow.

5G TECHNOLOGY

The first great technological battle with China revolves around 5G (Fifth Generation) cellular network technology. Such technology is crucial because it underpins a series of other industries and will process huge amounts of information (e.g., advanced web services and the Internet of Things (IoT)—including autonomous driving, autonomous weapons, and other strategic assets). China has leaped ahead in 5G, and European operators have invested significantly in Chinese equipment made by Huawei, ZTE, and other Chinese companies with which they have existing relationships from the development of the 4G network. Europeans operators also count on companies such as Nokia and Ericsson to prove that Europe can be a technological leader, but the EU 5G market cannot currently rival China's domestic market, resulting in significantly smaller orders for the two European competitors. The United States lags behind in some 5G infrastructure and lacks firms with the capability to build that kind of hardware, though it is well advanced in other aspects of 5G, notably the IoT and services side.

The current U.S. administration was first to ring the alarm over the possibility that China might use 5G equipment to control and eventually disrupt what goes through those networks.[37] It has since pressured its allies not to use Huawei and other Chinese equipment and has even banned Huawei from U.S. projects through a combination of rhetoric and voluntary measures with federal procurement rules that incentivize

[32] Dhruva Jaishankar, "From the iPhone to Huawei: The New Geopolitics of Technology," Brookings, July 31, 2019, https://www.brookings.edu/blog/order-from-chaos/2019/07/31/from-the-iphone-to-huawei-the-new-geopolitics-of-technology/.

[33] Andrés Ortega, "Europe Lifts its Chinese Veil," Real Institute Elcano, February 4, 2019, https://blog.realinstitutoelcano.org/en/europe-lifts-its-chinese-veil/.

[34] Conversation with Will Carter, CSIS.

[35] Mario Esteban, "Spain-China Relations," Real Institute Elcano, November 2018, http://www.realinstitutoelcano.org/wps/portal/rielcano_es/publicacion?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/publicaciones/informe-elcano-24-relaciones-espana-china.

[36] "Joint Statement on Advancing Responsible State Behavior in Cyberspace," U.S. Department of State, press release, September 23, 2019, https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/.

[37] Emily Stewart, "The US government's battle with Chinese Telecom Giant Huawei, Explained," Vox, August 19, 2019, https://www.vox.com/technology/2018/12/11/18134440/huawei-executive-order-entity-list-china-trump.

operators not to buy Chinese equipment. It has taken other general measures, such as restricting the sale of advanced semiconductors or software to Huawei and other companies, though some of these measures have yet to enter into force. This may not be in the United States' immediate industrial interest, as it currently lacks companies that can compete with Huawei in this sphere (Europe, at least, has Nokia and Ericsson).

Many Europeans operators are already dependent on Huawei equipment for the development of the 5G network (the deployment of which they do not want to postpone) either in their own countries or in other areas where they operate, for example, Spain's Telefonica and its operations in Latin America or in Germany. EU and Latin American telecom markets are much more competitive than the protected U.S. market, resulting in lower margins for operators and cost pressures on investments. Yet some European countries, such as Denmark, Sweden, and the Netherlands, are on the verge of limiting Huawei equipment and phasing out the company's products within their mobile networks. The German government has decided not to formally exclude any single company, preferring to focus instead on security standards, though there is an internal debate over the safety of using Chinese equipment.[38] The United Kingdom, for its part, will be a decisive case (even if it leaves the European Union), as the U.S. administration has threatened to cut information sharing with the so-called "Five Eyes" anglophone countries if they use Huawei equipment.[39] Britain does not yet share U.S. worries, and its certification technicians have not found any proof of a Chinese "backdoor" in that equipment.

After a period of tension, there is some transatlantic rapprochement on the issue. In October 2019, the European Commission and the European Union Agency for Cybersecurity (ENISA) Cooperation Group published a public report stating that "threats posed by states or state-backed actors are perceived to be of highest relevance" for the 5G system. It will "in turn, increase the number of attacks paths that could be exploited by threat actors . . . because of their capabilities (intent and resources) to perform attacks against EU Member States telecommunications networks, as well as the potential severity of the impact of such attacks."[40] The report did not single out any country; it aimed to serve as a basis for the preparation of a toolbox of risk mitigation measures. An unpublished version of the document reportedly identified specific techniques that could be used in attacks, including the possibility that a vendor could intentionally insert concealed hardware, malicious software, and software flaws into the 5G network.[41]

In parallel, Trump administration officials have suggested the United States could support Nokia and Ericsson in building enough equipment to replace Huawei's and to guarantee the long-term survival of the two European companies through strategic investment and rapid scaling up in production in 5G infrastructure to cover potential new orders.[42] Even then, however, the costs for operators that have already bought Huawei gear would be high. Nevertheless, the U.S. administration's actions have undermined Huawei's viability as a company, and Europeans are beginning to see that.

AI AND SEMICONDUCTORS

AI is a cross-cutting technology that serves all sorts of advances. It is already a main driver of growth, competitiveness, and job creation (and job destruction) and will have an even greater effect in the

[38] "Germany Rules Leave 5G Network Door Open for Huawei," *Deutsche Welle*, https://www.dw.com/en/germany-rules-leave-5g-network-door-open-for-huawei/a-50847915.

[39] Five Eyes is an intelligence alliance involving Australia, Canada, New Zealand, the United Kingdom, and the United States.

[40] NIS Cooperation Group, *EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks* (October 2019), https://euractiv.us15.list-manage.com/track/click?u=ec8c3035cd2e0ab2e3760549e&id=f2b467c372&e=f73a626f6a.

[41] Anna Isaac and Parmy Olson, "EU Warns of 5G Risks Amid Scrutiny of Huawei," *Wall Street Journal*, October 11, 2019, https://www.wsj.com/articles/eu-warns-of-5g-risks-amid-scrutiny-of-huawei-11570814799?mod=djemalertNEWS.

[42] Kiran Stacey, "US Pushes to Fund Western Rivals to Huawei," *Financial Times*, October 7, 2019, https://www.ft.com/content/94795848-e6e3-11e9-b112-9624ec9edc59.

future. It will flourish with the advent of technologies such as deep learning, neural networks, and 5G communications. It also impacts surveillance capacities, be they from firms or states. And, as Anthony Mullen, an expert with the IT firm Gartner, has stated, "right now, AI is a two-horse race between China and the US."[43] Europe is the battleground.

Indeed, China and the United States are well ahead of Europe in this field. According to the 2018 EU Digital Transformation Monitor, in 2016 the United States was investing $15-23 billon in AI, Asia (specifically China, South Korea, and Japan) was investing $8-12 billion, and Europe (including the United Kingdom) was investing just $3-4 billion.[44] EU member states and the European Union are now investing more actively in AI. The European Union accounted for 8 percent of global AI equity investment in 2017, an important increase from just 1 percent in 2013. However, this investment is relatively small compared to the U.S. market, which went from just 3 percent of AI start-up equity investments worldwide in 2015 to two-thirds of the total value of investment today. Chinese companies attracted 36 percent of global AI private equity investment in 2017, according to OECD figures.[45] The OECD forecasts that by 2030, China's AI industry will exceed RMB 1 trillion ($143 billion) with AI-related fields totaling RMB 10 trillion ($1.4 trillion) China is also competing for the commercial use of AI in several developing countries that are of interest to the European Union.

According to a report by the Center for Data Innovation which examines six categories of metrics—talent, research, development, adoption, data, and hardware—the United States "still leads in absolute terms."[46] China comes in second, and the European Union further behind. The report warns that this could change in coming years, as China appears to be making more rapid progress than either the United States or Europe. Although the European Union (the United Kingdom included) has the talent and research to compete with the United States and China, there is still a gap between its commercial AI adoption and funding and that of China or the United States. Due to its demographic size and its intrusive regime (once again an issue of different values in tech), China has more access to data, which is crucial for AI systems as they require large datasets to train their models.

In this landscape, Europe could become dependent on AI models that it does not control. Partly in response, the European Commission is designing a European AI strategy that builds on some member state strategies (e.g., France, Germany, and the United Kingdom). But there is a general view that Europe is too far behind for the first and even second generation of AI, and it should concentrate on the next generations. Brexit could also impact the weight, research, and innovation capacity of the European Union, as the United Kingdom is one of the most advanced EU countries in this field of research and development. Furthermore, the European Union has failed to fully grasp how AI impacts issues of work and rising inequality, at least during the transition phase.

The issue of semiconductors is inseparable from AI, as the latter relies on the former. Importantly, China is dependent on advanced U.S. semiconductors that are critical for some industries, as became clear when the Trump administration had to partially lift the ban on ZTE so as not to asphyxiate the company, an outcome Xi Jinping was keen to avoid. These imports from the United States could only be replaced by Taiwanese, South

[43] James Vincent, "China and the US Are Battling to Become the World's First AI Superpower," The Verge, August 3, 2017, https://www.theverge.com/2017/8/3/16007736/china-us-ai-artificial-intelligence.

[44] Digital Transformation Monitor, "USA-China-EU Plans for AI: Where Do We Stand?" European Commission, January 2018, https://ec.europa.eu/growth/tools-databases/dem/monitor/content/usa-china-eu-plans-ai-where-do-we-stand.

[45] "Private Equity Investment in Artificial Intelligence," OECD, December 2018, https://www.oecd.org/going-digital/ai/private-equity-investment-in-artificial-intelligence.pdf.

[46] Daniel Castro, Michael McLaughlin, and Eline Chivot, *Who Is Winning the AI Race: China, the EU or the United States?* (Brussels: Center for Data Innovation, August 2019), https://www.datainnovation.org/2019/08/who-is-winning-the-ai-race-china-the-eu-or-the-united-states/.

Korean, or, to a lesser degree, European ones. Today, only 16 percent of semiconductors used in China are produced there, and only half of those are made by Chinese firms. To lead in AI, China needs those complex chips, which it has tried to build for years unsuccessfully. The United States is two to three generations ahead in semiconductor production, creating a gap that would take at least ten years to close, according to some experts.[47] And unfortunately for China, reverse engineering does not always work without the human know-how. Not everything can be copied. Faced with a U.S. ban, China could try to fill the gap in some years and become technologically more autonomous or self-sufficient, but success is not guaranteed.[48,49]

WEB-BASED SERVICES

Web-based services could be the next battleground, not only between the United States and China, but also between Europe and the United States. The United States dominates the field (which includes cloud services) through a few tech giants, such as Amazon, Google, Microsoft, and Apple. So far, U.S.-Chinese competition in this field has been limited; neither has made serious attempts to enter the other's market in these areas, with the exception of Apple, but it could happen soon. China is investing in Indian and Southeast Asian start-ups through Baidu (dominating Chinese-language recognition algorithms), Alibaba (e-commerce), and Tencent (managing the world's largest e-payment system in collaboration with Alibaba). These companies are increasingly present in Europe as well, and even in the United States.

In web-based services, as in 5G and AI, Europe is lagging and dependent on U.S. and Chinese systems. With some small exceptions, it lacks the ability to scale and create large enough companies in this field. To make up for this, France and Germany's industrial strategy will be crucial, as will the new European Commission's strategy. Cooperation between European and U.S. companies remains inevitable and essential if Europeans want to stay relevant for the next tech generation, including 6G. And if Europe wants to control the data it produces, European cloud services will play an important role.

If they cannot catch up, EU member states and companies could end up having to choose between U.S. and Chinese web-based services. Though there is a choice to be made on economic grounds, no such choice exists on the political level since China's tech-related values and behavior differ so much from the Western values. Still, Europe does not want to see a U.S. tech regime that is largely decoupled from China; some selective decoupling now seems inevitable for Europe, but Europe desires much less decoupling than what the United States is calling for.

Could competition in these three areas lead to a U.S.-European (and others), anti-China tech alliance?[50] It should, but it cannot come at the price of Europe's own technological development. AI governance and regulation, as the next section explores, could be a more appropriate field for such an alliance.

Regulation: Power, Dispute, and Interoperability

Regulation is power and standard setting is becoming a new geopolitical battleground.[51] Both are essential in this competition with China and for transatlantic relations. A new wave of regulation is in the making

[47] William A. Carter and William Crumpler, "Understanding the Entities Listing in the Context of U.S.-China AI Competition," CSIS, *Critical Questions*, October 15, 2019, https://www.csis.org/analysis/understanding-entities-listing-context-us-china-ai-competition.

[48] Puja Tayal, "China Accelerates Its Semiconductor Self-Sufficiency Efforts," Market Realist, June 6, 2019, https://marketrealist.com/2019/06/china-accelerates-its-semiconductor-self-sufficiency-efforts/

[49] James Andrew Lewis, *China's Pursuit of Semiconductor Independence* (Washington, DC: CSIS, February 2019), https://www.csis.org/analysis/chinas-pursuit-semiconductor-independence.

[50] Andrew Grotto and Martin Schallbruch, "The Great Anti-China Tech Alliance," *Foreign Policy*, September 16, 2016, https://foreignpolicy.com/2019/09/16/the-west-will-regret-letting-china-win-the-tech-race/.

[51] Lorenzo Mariani and Micol Bertolini, "The US–China 5G Contest: Options for Europe," IAI, *IAI Papers* 19, no. 16 (September 2019), https://www.iai.it/en/pubblicazioni/us-china-5g-contest-options-europe.

for the digital economy, from content to taxes and data. A dispute or a rift in regulation between the United States and Europe could benefit China. As a recent report states, "China has not only managed a technological leap forward by implementing new national/indigenous technology standards, but also effectively internationalized some of those standards as viable alternatives."[52]

Indeed, on these issues the distance in values is much greater between Europeans and China than with the United States. But there are some transatlantic value differences in regulation, in particular on the protection of privacy (including divergence not only on the concept itself but also in terms of the mechanisms to deliver that privacy), the protection of users (especially young people), the right to be forgotten (Latin America is also generally against this), and on competition policy (though there is a movement in the United States to reduce the size and influence of some tech companies). China has understood the power of regulation and has become much more active regarding the issue; it is also counting on Russia for help, particularly on regulation of the internet and on cybercrime.[53]

The European Union sees itself as a regulatory player with global influence—as shown by the GDPR—that concentrates on privacy of data, which in some ways clashes with the U.S. Constitution's protections for freedom of speech. And though the European Union cannot strive to be a regulatory superpower—a position it cannot achieve without being a true digital power—the new European Commission has made clear its intention to establish rules and standards concerning technologies of the future, such as artificial intelligence or 5G, and competition in the tech space. In his November hearing before the European Parliament, Thierry Breton, then Commissioner-Designate for Internal Market, stressed the need to regulate tech and cyber space, as well as to ensure that single market rules are properly implemented: "[w]e have to work on our technological sovereignty," he told members of the European Parliament.[54] Margrethe Vestager, who will oversee EU digital policy in the new commission, has promised to reinforce competition policy with potential measures against U.S. chipmaker Broadcom.[55]

Transatlantic tensions in the regulatory space are not uncommon and are bound to continue. Commissioner for Justice Didier Reynders has taken aim at the U.S. Cloud Act, which gives U.S. law enforcement agencies the right to force the release of customer data outside the United States with "extraterritorial" effect.[56] And though in the United States standards for regulating technology and the digital economy are more private-sector driven than in Europe, the country has not avoided regulation with global impact (e.g., a presidential executive order limiting some types of cooperation with Huawei for U.S. companies, to global effect).[57] The current administration has also used trade deals to shield its tech giants from foreign regulators, for example, in the new U.S.-Mexico-Canada Agreement and with Japan.[58]

[52] Marianne Schneider-Petsinger et al., *US–China Strategic Competition. The Quest for Global Technological Leadership* (London: Chatham House, 2019), https://www.chathamhouse.org/sites/default/files/publications/research/CHHJ7480-US-China-Competition-RP-WEB.pdf.

[53] Allison Peters, "Russia and China Are Trying to Set the U.N.'s Rules on Cybercrime," *Foreign Policy*, September 16, 2019, https://foreignpolicy.com/2019/09/16/russia-and-china-are-trying-to-set-the-u-n-s-rules-on-cybercrime/.

[54] "Hearing of Commissioner-Designate Thierry Breton," European Commission, press release, November 14, 2019, https://www.europarl.europa.eu/news/en/press-room/20191112IPR66319/hearing-of-commissioner-designate-thierry-breton.

[55] Adam Satariano, "Europe's Margrethe Vestager Takes a Rare Step Toward Big Tech," *New York Times*, October 16, 2019, https://www.nytimes.com/2019/10/16/business/-big-tech-europe-antitrust.html.

[56] Samuel Stolton, "Digital Brief: Commissioners On Trial," Euractiv, October 3, 2019, https://www.euractiv.com/section/digital/news/digital-brief-commissioners-on-trial/.

[57] Donald J. Trump, "Executive Order on Securing the Information and Communications Technology and Services Supply Chain," White House, May 15, 2019, https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

[58] David McCabe and Ana Swanson, "U.S. Using Trade Deals to Shield Tech Giants From Foreign Regulators," *New York Times*, October 7, 2019, https://www.nytimes.com/2019/10/07/business/tech-shield-trade-deals.html.

Despite U.S. pushback, the GDPR model and content has been followed by an increasing number of countries, states (e.g., California), and U.S. companies so they can keep operating in the European market. The GDPR is, however, incompatible with Chinese laws: if the Chinese government requests data transmitted over 5G networks, any Chinese or foreign company operating in China would have to comply, even if dealing with European data. China does have a privacy standard—the Personal Information Security Specification—that gives Chinese citizens some control over their data, but it is governed by the principle of "data sovereignty," which implies that all information related to citizens must be stored in-country and be made accessible on-demand to the Chinese government.[59] Despite these incompatibilities, it is clear the European Union has regulatory influence in the world, as shown by the success of the GDPR (though, as said, it may need to become a real digital power to buttress its credibility as a regulatory power). To find transatlantic common ground, the European Union should try to convince rather than impose rules, while the United States should offer more ideas in the regulatory space. Together, allied on a common model for data management and privacy, they could pressure the Chinese model to get closer to theirs.

Unlike data, the field of AI ethics provides more ground for cooperation between the United States, Europe, and China. Both EU and U.S. policymakers have offered proposals. The European Commission is already making proposals for the development stage and testing of AI, and it is poised to advocate for an "ethics-by-design" approach, whereby products and services using AI take into account ethical guidelines at the earliest possible stage in their development. European Commission President Ursula von der Leyen has promised to deliver a strategy on AI and ethics in the first 100 days of the new commission. China has presented its own proposals, including 15 points drawn up by the Beijing Academy of Artificial Intelligence (BAAI), supported by the Ministry of Science and Technology and other local governments, academia, and companies (e.g., Peking University, Baidu, Alibaba, and Tencent).[60] The OECD has also offered a plan, which has received the support of the G20.[61],[62] But the United States and Europe would be well advised to be more active, as Asia (not just China) could end up leading AI ethics and governance in a global way.[63]

There is a general agreement on some of these AI ethics principles, which are general, well intentioned, and cover issues from human-centered AI to transparency and privacy. That China has supported the OECD plan shows the issue is not the principles themselves; the real problems and differences will arise when those principles are translated into algorithms and embedded in the machines. Potential for U.S.-EU cooperation is highest in that implementation phase, focused on an "ethics-by-design" approach, as laid out by Didier Reynders. Most of the background work on design and future implementation has been done in the European Union.

Importantly, "common" does not mean that in AI as in other fields the United States and Europe need to follow exactly the same digital policies or regulations. What they need are some common fundamentals to tackle the problems of the digital age, particularly interoperable public policies in those fields that surpass the Chinese competition. They can then design alternative forms of regulation that are more adapted to their own situations. Innovation in regulation and technology can move in tandem. A good example of transatlantic regulatory cooperation is the EU-U.S. Privacy Shield Framework, which provides companies

[59] Bradley Honigberg, "The Growing Need for U.S. Leadership on Technology Regulation," CSIS, *New Perspectives in Foreign Policy* 19 (October 2019), https://www.csis.org/growing-need-us-leadership-technology-regulation.

[60] "Beijing AI Principles," BAAI, https://www.baai.ac.cn/blog/beijing-ai-principles.

[61] "Forty-two countries adopt new OECD Principles on Artificial Intelligence," OECD, https://legalinstruments.oecd.org/api/print?ids=648&lang=en; https://www.oecd.org/science/forty-two-countries-adopt-new-oecd-principles-on-artificial-intelligence.htm.

[62] "G20 Ministerial Statement on Trade and Digital Economy," Ministry of Foreign Affairs of Japan, https://www.mofa.go.jp/files/000486596.pdf

[63] MIT Technology Review Insights, "Asia's AI Agenda: The Ethics of AI," *MIT Technology Review*, July 11, 2019, https://www.technologyreview.com/s/613935/asias-ai-agenda-the-ethics-of-ai/.

on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union (and Switzerland) to the United States in support of transatlantic commerce.[64] The framework underwent its third review in the fall of 2019: with more than 5,000 participating companies, it has moved from the inception phase to a more operational phase, covering both commercial aspects and issues relating to government access to personal data.[65]

The United States and Europe should also cooperate to preserve the open governance system of the internet. China has become much more active in this space, with clear purposes. Xi Jinping has proposed addressing the issue through "Four Principles of global Internet governance system transformation" and "Five Propositions of building a cyberspace community of shared destiny."[66] The four principles are: (1) respect for cyber sovereignty; (2) safeguarding peace and security; (3) fostering open cooperation; and (4) building a satisfactory order. Behind these lies the desire for control, both domestically and beyond China's borders. China has been active on issues of regulation of the digital economy at the United Nations, and its technology companies are reportedly shaping new facial recognition and surveillance standards.[67] To shape these standards in developing countries in Africa, the Middle East, and Asia, China has leveraged its Belt and Road Initiative to secure favorable policies. A transatlantic common stance (which should also include Japan, Australia, and other like-minded countries) should consider promoting alternative standards.

There is too much at stake when it comes to regulating tech for the transatlantic community to be drowned in its own disputes. The United States and Europe must cooperate on fundamental principles for AI, data, and internet governance rules to harness the power of the first-mover advantage and push back against China's advances in that space. The alternative is to risk giving up the game altogether.

Conclusion: A Transatlantic Tech Agenda in Light of China's Challenges

A common agenda in technology and related fields could be part of the "reset" of U.S.-Europe relations that some officials, like Josep Borrell and Secretary of State Michael Pompeo, have touted in recent months. This reset could reduce China's influence in this sphere, but it requires coalition-building and allies. As this paper has shown, failure to build such an agenda for China could undermine transatlantic relations that are already under strain and divide the European Union internally. This affects both EU governments and companies.

The United States and Europe could come to regret letting Beijing win the race to govern digital technology if they do not bridge their divide; together, the United States and Europe are a "formidable pair."[68] Changing China's behavior is only possible with alliances and a coordinated response from key partners and economies. As CSIS's James Andrew Lewis puts it, "[a]n alliance strategy is crucial for counterintelligence,

[64] International Trade Administration, "EU-U.S. & Swiss-U.S. Privacy Shield Framework," U.S. Department of Commerce, https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t0000000QJdg.

[65] "EU-US Data Transfers," European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en.

[66] The five propositions are: (1) speed up the construction of a global network infrastructure and foster interconnection and interactivity; (2) build shared platforms for online cultural interaction and stimulate exchange and mutual learning; (3) promote innovation and development in the online economy and stimulate common flourishing; (4) guarantee cybersecurity and stimulate orderly development; and (5) build the internet governance system and stimulate fairness and justice. Elsa Kania et al., "China's Strategic Thinking on Building Power in Cyberspace," New America Foundation, September 25, 2017, https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/.

[67] Anna Gross, Madhumita Murgia, and Yuan Yang, "Chiense Tech Groups Shaping UN Facial Recognition Standards," *Financial Times*, December 1, 2019, https://www.ft.com/content/c3555a3c-0d3e-11ea-b2d6-9bf4d1957a67.

[68] Andrew Grotto and Martin Schallbruch, "The Great Anti-China Tech Alliance," *Foreign Policy*, September 16, 2016, https://foreignpolicy.com/2019/09/16/the-west-will-regret-letting-china-win-the-tech-race/.

financial restrictions, and export controls. The United States will need a broad partnership to effectively use diplomatic and economic tools to compel change by China."[69]

In the search for a common agenda, the United States and Europe need not agree on everything, with regards to their relations with China. In this first part of the report, we have examined the dimensions related to technology, from the point of view that avoiding Chinese technological dominance is an essential part of present-day great power competition. Here are eight key recommendations relating to the tech dimension and China:

- Open a deep transatlantic discussion on the role of values and their embedment in new technologies, with a more stringent focus on how technological issues could affect human rights.
- Align U.S. and European tech-related regulation (particularly on AI currently in design) to prevent China from imposing its model and push it closer to Western regulatory standards. Target regulatory innovation that is rooted in common principles, with the aim of interoperability.
- Advance in a shared, transatlantic technical analysis of the perils of depending excessively on Chinese communications equipment.
- Build on the U.S. initiative for Advancing Responsible State Behavior in Cyberspace and look for global standards with the European Union in the security space.
- Nudge Chinese multinational tech companies to list on Western stock exchanges that require higher standards on transparency and reporting.
- Screen Chinese investments in strategic technological companies and infrastructure in the United States and Europe and share advanced intelligence on these investments.
- U.S. policymakers should manage European reticence toward decoupling and disengaging ecosystems from China.
- The European Union and its member states must invest much more in technology (public and private investments), particularly in next generations (5G and others), with the support of the U.S. government and companies. The large European public procurement market should adapt its rules to support tech innovation at early stages to prevent China from taking over too large a market share.

The United States and Europe must open a deep and sustained dialogue on these issues. The European Union must also make an effort to better explain its policies and attitudes in the United States, particularly in Washington.[70] This effort must focus not only on the administration but also on Congress, the U.S. business community, and the public. In turn, the United States should support tech growth in the European Union and reward the continent's changing approach to China. Both sides have much to gain if they succeed in this common approach—and much to lose if they fail.

***Andrés Ortega Klein** is a former visiting fellow with the Europe Program at the Center for Strategic and International Studies in Washington, D.C., and is a senior research fellow for global affairs and technology transformations at the Royal Elcano Institute in Spain.*

[69] James Andrew Lewis, *Emerging Technologies and Managing the Risk of Tech Transfer to China* (Washington, DC: CSIS, September 2019), https://www.csis.org/analysis/emerging-technologies-and-managing-risk-tech-transfer-china.
[70] Anabel González and Nicolas Veron. "EU Trade Policy Amid the China-US Clash: Caught in the Crossfire?" Bruegel, Working Paper, September 17, 2019, https://bruegel.org/2019/09/eu-trade-policy-amid-the-china-us-clash-caught-in-the-crossfire/.

The author would like to thank the Argyros Family Foundation for the financial support it has provided for his visiting fellowship at CSIS; Heather Conley for her support and guidance for this research; Rachel Ellehuus, Dejana Saric, Donatienne Ruy, and Phillip Meylan for all their help in the editing process; and the many people offered their insights, in events or in personal interviews, including: Erik Brattberg (CEIP), Frances Burwell (Atlantic Council), Will Carter (CSIS), Tarun Chhabra (CEST), Bonnie Glasser (CSIS), Dan Hamilton (SAIS), Jon Hillmam (CSIS), Tim Maurer (CEIP), James Andrew Lewis (CSIS), David O. Shullman (IRI), Chris Skaluba (Atlantic Council), Andrew Small (GMFUS), Jim Townsend (CNAS), Thomas Valasek (CEIP), and Thomas Wright (Brookings). Thanks also to Mario Esteban, Luis Simón, and Miguel Otero of the Elcano Royal Institute for their comments on drafts versions of this paper.

The author would also like to thank the various officials, who have preferred to remain anonymity for more candid conversations. This white paper also includes information gleaned from public and private meetings at CSIS, ECFR, CEIP, Atlantic Council, GMFUS, and the Heritage Foundation.

This report is made possible by general support to CSIS. No direct sponsorship contributed to this report.

This report is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).