Chapter III: Areas of Lesser Initial Convergence

By Franklin D. Kramer and Sarah Kirchberger

Areas of lesser transatlantic convergence include China's trade and investment practices and its efforts to dominate new technologies and set international technology standards. Divergence among transatlantic partners here was due initially to the fact that many nations had registered immediate benefits from their economic and technological ties with China while ignoring the longer-term and less obvious risks. Divergence has appeared in the handling of the Huawei Technologies Co., Ltd. 5G issue and is also demonstrated by the fact that both the United States and the European Union (EU) have negotiated separately with China on trade and investment pacts. Nonetheless, China has overplayed its hand in enough instances since the onset of the COVID-19 pandemic that transatlantic partners are increasingly finding common ground on these areas of lesser convergence. A place to start is by countering Chinese subsidies, leverage-seeking investments, supply dependencies, and similar predatory practices that give China dangerous economic, political, and technical leverage over democratic nations.

Section A: Economic Challenges

1. The Challenges

China presents significant economic challenges to transatlantic nations that can usefully be divided in a first, and necessarily oversimplified, approximation into challenges arising within markets in the transatlantic nations, markets within China, and markets in the rest of the world. The most consequential challenges include those arising in the transatlantic markets—unfair competitive practice, resilience issues, cyber espionage, investments in sensitive industries—and in China, particularly issues of technology transfer and access to markets.

A related, but different, challenge is the ability of the United States and Europe, including especially the EU, to undertake complementary approaches in dealing with the economic issues raised by China.

a) Challenges within transatlantic markets

China presents five key challenges in transatlantic markets.

First is the issue of the impact on market competition from unfair practices undertaken by China's state-driven economic model.[322] For example, in a paper on "leveling the playing field as regards foreign subsidies," the European Commission highlighted the problem of China's use of "heavy subsidies to both state-owned and private sector companies."[323] Reports by the United States Trade Representative (USTR) to Congress have thoroughly described Chinese unfair market practices,[324] which can be summarized accordingly: "In an attempt to dominate critical global markets and manufacturing industries, China leverages policy tools such as low interest loans; subsidized utility rates; lax environmental, health, and safety standards; and dumping to boost its industry. China also uses counterfeiting and piracy, illegal export subsidies, and overcapacity to depress world prices and push rivals out of the global market. It has implemented these tactics to capture much of the world's solar and steel industries and intends to extend its dominance to other industries such as automobiles and robotics."[325]

Second, China presents a series of resilience challenges for the transatlantic nations.[326] Chinese companies are

322 This section draws directly in places from the chapter author's prior reports, Franklin D. Kramer, *Effective Resilience and National Strategy: Lessons from the Pandemic and Requirements for Key Critical Infrastructures*, Atlantic Council, October 9, 2020, 13, https://www.atlanticcouncil.org/wp-content/uploads/2020/10/Effective-Resilience-Latest.pdf, and Franklin D. Kramer, *Managed Competition: Meeting China's challenge in a multi-vector world,* Atlantic Council, December 12, 2019, 15, https://www.atlanticcouncil.org/in-depth-research-reports/report/managed-competition-meeting-chinas-challenge-in-a-multi-vector-world/.

323 European Commission and HR/VP contribution to the European Council, *EU-China – A strategic outlook*, March 12, 2019, 5, https://ec.europa.eu/commission/sites/beta-political/files/communication-eu-china-a-strategic-outlook.pdf.

324 United States Trade Representative, *2018 Report to Congress on China's WTO Compliance*, February 2019, https://ustr.gov/sites/default/files/2018-USTR-Report-to-Congress-on-China%27s-WTO-Compliance.pdf.

325 Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806, *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States,* September 2018, 36, https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF.

326 Kramer, *Effective Resilience*, 12.

pervasively present in supply chains.[327] As one analysis described: "In addition to China dominating many material sectors at the upstream source of supply (e.g., mining), it is increasingly dominating downstream value-added materials processing and associated manufacturing supply chains, both in China and increasingly in other countries. Areas of concern … include a growing number of widely used and specialized metals, alloys, and other materials, including rare earths and permanent magnets."[328] Moreover, "that pervasiveness raises the issue of whether China will remain a reliable supplier, particularly when there are political or other pressures such as can occur during a pandemic. Historically, in order to achieve its geopolitical goals, China has utilized economic pressure including restricting supply chains."[329]

One highly important resilience issue arises from China's involvement in the information technology and communications supply chains. Those considerations are specifically presented by China's role in 5G technology, in particular through Huawei, and raise the issues of system and component vulnerabilities, including the potential for the introduction of malware.[330] Moreover, the recent, very significant SolarWinds intrusions into US government and private sector networks that were accomplished through compromised software supply chains[331] underscore the degree of vulnerability that Chinese engagement in supply chains presents.[332]

Third, China has used cyber espionage against the transatlantic nations for economic (and national security) advantage. A recent example has been Chinese espionage against companies working on the development of vaccines for the coronavirus. The seriousness of the problem was highlighted by the Department of Homeland Security and the Federal Bureau of Investigation (FBI) issuing a joint alert "warning … of … targeting and attempted network compromise by the People's Republic of China … [of] [h]ealthcare, pharmaceutical, and research sectors working on the COVID-19 response."[333] This action by China is, of course, in complete disregard of its promise to the United States to halt commercial cyber espionage.[334] China's coronavirus espionage highlights the dangers faced on both sides of the Atlantic by firms seeking to develop and market emerging and advanced technologies. Companies, and especially small and medium-sized companies, cannot be expected to undertake effective cyber protection against the very significant cyber capabilities of China.

Fourth is the key issue of Chinese foreign direct investment (FDI) focused on Western companies with sensitive and/or security-related technologies.[335] In Europe, China's acquisition of the German robotics firm Kuka led to a heightened degree of focus on Chinese acquisitions throughout Europe. As a consequence, in 2019, the EU enacted a regulation "establishing a framework for the screening of foreign direct investments into the Union."[336] In the United States, analyses have comparably concluded, for example, that "High-tech industries such as artificial intelligence (AI), biotechnology, and virtual reality have been the primary targets of Chinese VC [venture capital] activity … [One] study found that Chinese investors targeted sensitive technologies in 78 percent of all U.S. VC funding rounds involving a Chinese investor between 2000 and May 2018 … These investments are not just lucrative business opportunities, they also enable Chinese firms to acquire valuable U.S. technology and IP."[337]

Fifth, China is directing substantial resources into innovation and advanced technologies.[338] The Made in China 2025 program identifies ten areas in which China plans to be a world leader.[339] More recently, Chinese President Xi Jinping has focused on AI, quantum computing, and other comparable arenas as exemplified by the "New Generation

327 Ibid.

328 Report to President Donald J. Trump, *Assessing*, 36-37.

329 Kramer, *Effective Resilience*, 12.

330 Ibid.

331 Cybersecurity & Infrastructure Security Agency, "Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director Of National Intelligence (ODNI), and the National Security Agency (NSA)," January 5, 2021, https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure.

332 While the SolarWinds intrusions have been ascribed to Russia, China is an equally capable cyber adversary.

333 Cybersecurity & Infrastructure Security Agency, *Chinese Malicious Cyber Activity*, accessed May 13, 2020, https://www.us-cert.gov/china.

334 David E. Sanger and Steven Lee Myers, "After a Hiatus, China Accelerates Cyberspying Efforts to Obtain U.S. Technology," *New York Times*, November 29, 2018, https://www.nytimes.com/2018/11/29/us/politics/china-trump-cyberespionage.html?auth=login-email&login=email.

335 Kramer, *Managed Competition*, 15.

336 *Official Journal of the European Union*, "Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union," March 21, 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0452&from=EN.

337 U.S.-China Economic and Security Commission, Report to 115th Congress, Second session, November 2018, 39, https://www.uscc.gov/sites/default/files/annual_reports/2018%20Annual%20Report%20to%20Congress.pdf.

338 Kramer, *Managed Competition*.

339 U.S. Chamber of Commerce, *Made in China 2025: Global Ambitions Built on Local Protections*, 2017, 10, https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf.

Artificial Intelligence Development Plan."[340] These significant efforts have potential consequences for economic markets[341] (and for national security) as advanced and emerging technologies will be the leading drivers of the global economy.[342] The competition in innovation is entangled with the ability to have fair and efficient markets for transatlantic advanced and emerging technology companies in the face of China's unfair market practices.[343]

b) Challenges in markets within China

For markets within China, transatlantic companies face numerous nontariff barriers that restrict their ability to compete and must also contend with the forcible transfer of their technology to Chinese firms. Additionally, recently promulgated rules, approved by China's State Council, could have a potentially significant impact on firms that are subject to US or European constraints on dealing with China, though the practical application of these rules is yet to be determined.[344]

One analysis by the USTR enumerated multiple Chinese actions affecting transatlantic firms: "WTO-inconsistent activities pursued by China [include]: (1) local content requirements in the automobile sector; (2) discriminatory taxes in the integrated circuit sector; (3) hundreds of prohibited subsidies in a wide range of manufacturing sectors; (4) inadequate intellectual property rights (IPR) enforcement in the copyright area; (5) significant market access barriers in copyright-intensive industries; (6) severe restrictions on foreign suppliers of financial information services; (7) export restraints on numerous raw materials; (8) a denial of market access for foreign suppliers of electronic payment services; (9) repeated abusive use of trade remedies; (10) excessive domestic support for key agricultural commodities; (11) the opaque and protectionist administration of tariff-rate quotas for key agricultural commodities; and (12) discriminatory regulations on technology licensing."[345]

Second, China uses several approaches that lead to the "forcible transfer of technology," including, as described by USTR: "(1) pressuring the transfer of technology through the abuse of administrative processes and other means; (2) using discriminatory regulations to force non-market licensing outcomes for U.S. businesses; (3) leveraging state capital to acquire U.S. high-technology assets for transfer to Chinese companies in accordance with China's industrial policy objectives; and (4) obtaining U.S. intellectual property and sensitive business information through cyber theft for the commercial benefit of Chinese industry."[346]

Third, China has determined to rely heavily on domestic capabilities, as exemplified in its "dual-circulation" policy.[347] The recently concluded Fifth Plenum of the Central Committee of the Chinese Communist Party (CCP) reiterated the policy of dual circulation,[348] with the communiqués stating that China would "accelerate the construction of a new development pattern with the domestic cycle as the main body and the domestic and international dual cycles mutually promoting each other."[349] While the precise impact is yet to be determined, China, for example, "ordered all government offices and public institutions to remove foreign computer equipment and software within three years."[350]

Fourth, as noted above, China has issued rules that "allow government officials to issue orders saying that companies do not have to comply with certain foreign restrictions. Chinese companies that incur losses because of another party's compliance with those laws can sue for damages in Chinese courts, according to the Commerce Ministry's notice."[351] The impact of the rules is yet to be determined: "It is unclear whether global companies would end up

340 Gregory C. Allen, *Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security*, Center for a New American Security, February 2019, https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Understanding-Chinas-AI-Strategy-Gregory-C.-Allen-FINAL-2.15.19.pdf?mtime=20190215104041.

341 Kramer, *Managed Competition*.

342 Kramer, *Effective Resilience*, 13.

343 Ibid., 12.

344 Amy Qin, "China's New Rules Could Hit U.S. Firms and Send a Message to Biden," *New York Times*, January 9, 2021, *https://www.nytimes.com/2021/01/09/business/china-rules-trump-biden-sanctions.html?referringSource=articleShare*.

345 United States Trade Representative, *2018 Report*.

346 Ibid., 6.

347 Fengyang, "China's 'dual-circulation' strategy means relying less on foreigners," *Economist*, November 7, 2020, https://www.economist.com/china/2020/11/07/chinas-dual-circulation-strategy-means-relying-less-on-foreigners.

348 Reuters staff, "Factbox: Key details from fifth plenum of China's Communist Party," Reuters, October 29, 2020, https://www.reuters.com/article/us-china-politics-plenum-factbox/factbox-key-details-from-fifth-plenum-of-chinas-communist-party-idUSKBN27E1XY.

349 Xinhuanet, Communiqué of the Fifth Plenary Session of the 19th Central Committee of the Communist Party of China, https://translate.google.com/translate?hl=en&sl=zh-CN&u=http://www.xinhuanet.com/2020-10/29/c_1126674147.htm&prev=search&pto=aue.

350 Yuan Yang and Nian Liu, "Beijing orders state offices to replace foreign PCs and software," *Financial Times,* December 8, 2019, https://www.ft.com/content/b55fc6ee-1787-11ea-8d73-6303645ac406.

351 Qin, "China's New Rules.

being punished in China for complying with U.S. sanctions. Under the rules … companies could seek a waiver from the Commerce Ministry in order to comply with American restrictions."[352]

c) Challenges in markets worldwide

China utilizes both economic pressure and investments to achieve its goals in worldwide markets.

Economic coercion is regularly practiced by China, including by "[p]unish[ing] countries that undermine its territorial claims and foreign policy goals with measures such as restricting trade, encouraging popular boycotts, and cutting off tourism."[353] One listing of particular examples of economic coercion included: "(1) Chinese restrictions on rare earths exports and other measures directed at Japan after a collision between a Chinese fishing boat and a Japanese coast guard ship near the disputed Senkaku/Diaoyu islands in 2010; (2) Chinese restrictions on imports of Norwegian salmon after Liu [Xiaobo] won the Nobel Peace Prize in 2010; (3) Chinese reductions of imports of bananas and other agricultural goods from the Philippines as well as cuts in tourism from China after a dispute over the South China Sea from 2012 to 2016; (4) Chinese reductions in tourism and other measures against Taiwan in response to the election of Tsai [Ing-wen] in 2016; (5) Chinese tourism reductions and restrictions on certain trade with South Korea after Seoul agreed to deploy a US THAAD missile defense system in 2016; and (6) temporary Chinese restrictions on cross-border trade with Mongolia after it allowed the Dalai Lama's visit in 2016."[354]

China's international economic investments are generally undertaken through its Belt and Road Initiative (BRI). The BRI has come to be more of a general approach than a highly specific initiative. The investment amounts are substantial though precise data are not easily available, distinctions are often not made between actual and planned investment, and the impact of the COVID-19 pandemic is also unclear. The World Bank had reported that, as of May 2018, "projects in all sectors that are already executed, in implementation or planned are estimated to amount to US$575 billion."[355] More recently, however:

> "New data released by the American Enterprise Institute show that most countries of the Belt and Road Initiative (BRI) have experienced a decline in Chinese investments in the first half of 2020. Overall investments in the BRI were USD 23.4 billion in the first six months of 2020, dropping by about 50% from USD 46 billion invested during the first six months of 2019 (and dropping by 60% compared to the first six months of 2018). 2020 BRI investments were the slowest of any 6 months period since the BRI had been announced in 2013."[356]

Another recent analysis, with a still different investment number, underscored the foreign policy and influence aims of the BRI:

> "Five years down the road, China has invested more than 90 billion USD into BRI-related infrastructure projects, not counting projects still under construction or in the planning phase, which involve much larger investment volumes. It is clear by now that BRI is about much more than securing China's trade routes and energy supplies as well as exporting its industrial over-capacities to far-away construction projects. The initiative is a key part of Xi Jinping's grand foreign policy design to increase China's influence in its regional neighborhood and beyond."[357]

2. Transatlantic Convergence and Divergence

The transatlantic countries have generally similar analyses of the economic challenges presented by China. The more open issues arise as to what should be the actual responses, which are also affected by transatlantic differences in other areas such as antitrust, data, taxation, and transatlantic trade.

The discussion above set forth significant US concerns regarding the challenges presented by Chinese distortive market behaviors, including issues surrounding subsidies, supply chain dependencies and vulnerabilities, and investments into sensitive industries. Europe, including at both the EU and national levels, has reached broadly similar conclusions.

The European Commission's trade policy of "open strategic autonomy" recognizes that this "commitment must go

352 Ibid.

353 Peter Harrell, Elizabeth Rosenberg, and Edoardo Saravalle, *China's Use of Coercive Economic Measures*, Center for a New American Security, June 2018, 2, https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/China_Use_FINAL-1.pdf?mtime=20180604161240&focal=none.

354 Ibid., 7-8.

355 World Bank, "Belt and Road Initiative," March 28, 2018, https://www.worldbank.org/en/topic/regional-integration/brief/belt-and-road-initiative.

356 Christoph Nedopil Wang, "Brief: Investments in the Chinese Belt and Road Initiative (BRI) in 2020 during the Covid-19 pandemic," Green Belt and Road Initiative Center, July 31, 2020, https://green-bri.org/investment-report-belt-and-road-initiative-bri-2020-covid19.

357 MERICS, *MERICS Belt and Road Tracker*, accessed November 10, 2020, https://merics.org/en/bri-tracker.

hand in hand with efforts to ensure that our openness is not abused by unfair, hostile or uncompetitive trade practices."[358] Relatedly, the commission recently presented an "Action Plan on Critical Raw Materials" which, recognizing the issue of overdependency on single sources, includes a focus on China which "provides 98% of the EU's supply of rare earth elements."[359] Further, as noted above, the European Commission highlighted the problem of China's use of "heavy subsidies to both state-owned and private sector companies."[360] That concern, as well as the broader challenges of a state-driven economy, have been raised by the European private sector, including Germany's Federation of German Industries (BDI).[361]

Responding to such issues, the EU enacted a regulation "establishing a framework for the screening of foreign direct investments into the Union."[362] A number of European nations, including France, Germany, Italy, the Netherlands, and Spain, have enacted legislation consistent with the regulation, and the United Kingdom has also increased its FDI reviews.[363] Those actions are broadly similar to the expansion in the United States of the jurisdiction of the Committee on Foreign Investment in the United States (CFIUS).[364]

In March 2019, the "EU Heads of State or Governments called for a concerted approach to the security of 5G networks," which led to the establishment in January 2020 of the "EU toolbox of risk mitigating measures" whose progress the European Commission continues to monitor.[365] The "tool kit," if adhered to, essentially limits the use of Huawei 5G capabilities, and an expanding number of nations, including the Czech Republic, Denmark, Estonia, France,[366] Latvia, Poland, Romania, Slovenia, Sweden, and the UK have effectively determined not to utilize Huawei in their 5G networks.[367] The United States has effectively restricted the use of Huawei in the United States (and elsewhere by others) through a variety of mechanisms, including inclusion on the Commerce Department's entity list and limits on the use of US semiconductors in projects in which Huawei components are to be utilized.[368]

The EU and the United States, along with Japan, have also had ongoing talks regarding reform of the World Trade Organization (WTO) in response to issues stemming from China's actions.

Despite this general convergence, however, there is no coordinated transatlantic policy regarding how to address economic challenges posed by China, whether for transatlantic markets, for markets in China, or worldwide. The United States and the EU have engaged in separate trade negotiations with China. The United States struck a so-called Phase One deal that focused on reducing the US trade deficit with China, though currently available statistics indicate that its terms have not been met by China in 2020, for among other reasons, the issues raised by the pandemic.[369]

The EU and China in December of 2020 agreed in principle to a Comprehensive Agreement on Investment (CAI), though the precise terms have yet to be established and

358 European Commission, "A renewed trade policy for a stronger Europe," Consultation Note, June 16, 2020, 8, https://trade.ec.europa.eu/doclib/docs/2020/june/tradoc_158779.pdf.

359 European Commission, "Communication From The Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Critical Raw Materials Resilience: Charting a Path Towards Greater Security and Sustainability," September 3, 2020, 3, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0474&from=EN.

360 European Commission and HR/VP contribution to the European Council, 5.

361 Federation of German Industries (BDI), "Partner and Systemic Competitor: How Do We Deal With China's State-Controlled Economy?" policy paper, January 10, 2019, https://english.bdi.eu/publication/news/china-partner-and-systemic-competitor/.

362 *Official Journal of the European Union*, "Regulation (EU) 2019/452."

363 Henry Smith and Alexandra Kellert, "The rise of investment screening in Western Europe," Lexology, August 4, 2020, https://www.lexology.com/library/detail.aspx?g=380ff627-4579-4973-969c-312635ddfee2.

364 US Department of the Treasury, "Summary of the Foreign Investment Risk Review Modernization Act of 2018," https://www.treasury.gov/resource-center/international/Documents/Summary-of-FIRRMA.pdf; U.S. Department of the Treasury, "Title XVII—Review of Foreign Investment and Export Controls," https://home.treasury.gov/sites/default/files/2018-08/The-Foreign-Investment-Risk-Review-Modernization-Act-of-2018-FIRRMA_0.pdf.

365 European Commission, *Report on Member States' progress in implementing the EU Toolbox on 5G Cybersecurity*, July 24, 2020, https://ec.europa.eu/digital-single-market/en/news/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity.

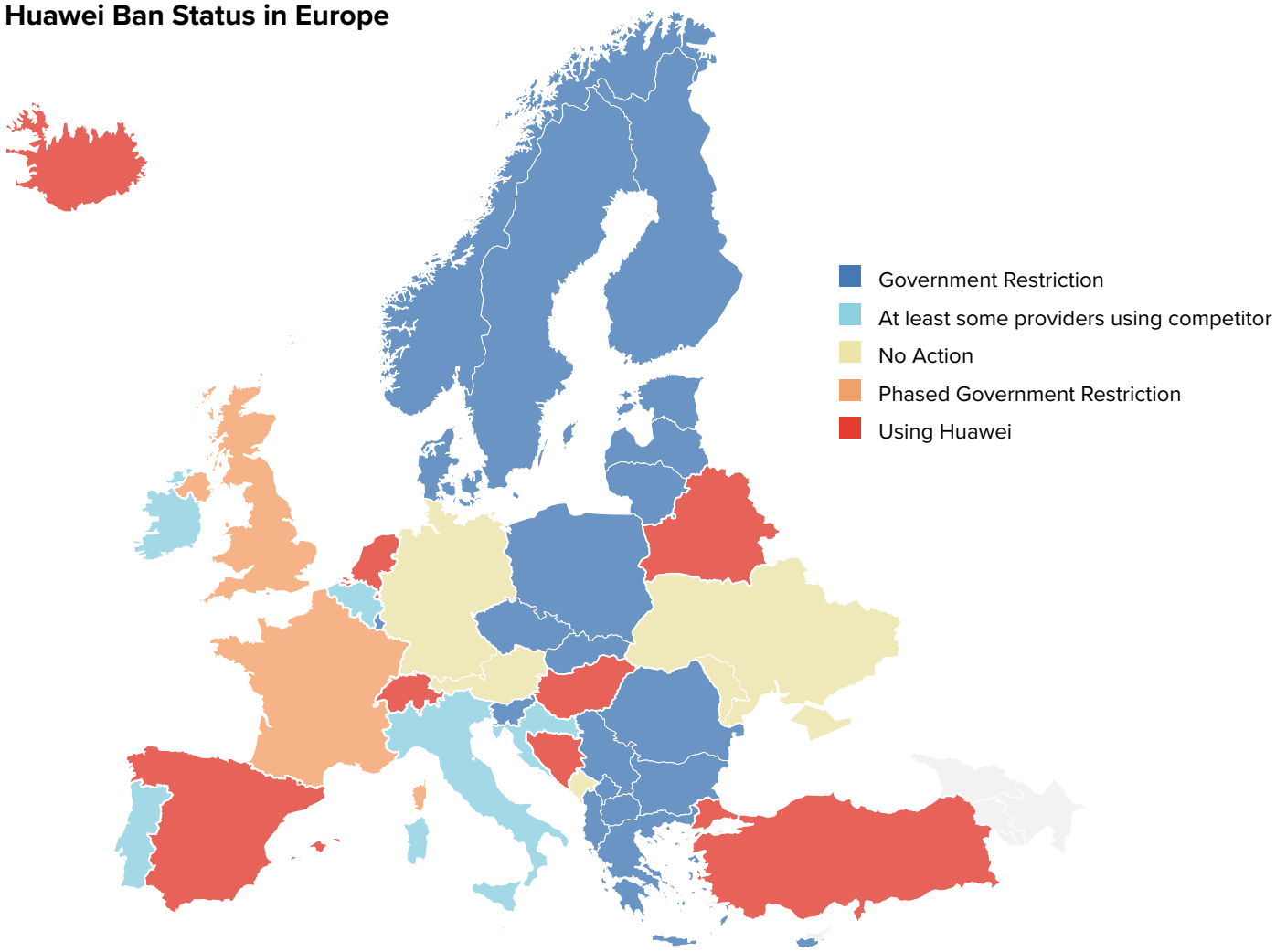
366 Reuters, "France's limits on Huawei 5G equipment amount to de facto ban by 2028," *South China Morning Post,* July 23, 2020, https://www.scmp.com/news/world/europe/article/3094312/frances-limits-huawei-5g-equipment-amount-de-facto-ban-2028.

367 See, e.g., Robbie Gramer, "Trump Turning More Countries in Europe Against Huawei," *Foreign Policy,* October 27, 2020, https://foreignpolicy.com/2020/10/27/trump-europe-huawei-china-us-competition-geopolitics-5g-slovakia/; Laurens Cerulus, "Huawei challenges legality of 5G bans in Poland, Romania," *Politico*, November 2, 2020, https://www.politico.eu/article/huawei-hints-at-legal-action-against-5g-bans-in-poland-romania/; US Secretary of State Michael R. Pompeo, Welcoming the United Kingdom Decision To Prohibit Huawei From 5G Networks, press statement, US Embassy in Mauritania, July 14, 2020, https://mr.usembassy.gov/welcoming-the-united-kingdom-decision-to-prohibit-huawei-from-5g-networks/.

368 US Department of Commerce, Commerce Department Further Restricts Huawei Access to U.S. Technology and Adds Another 38 Affiliates to the Entity List, press release, August 17, 2020, https://www.commerce.gov/news/press-releases/2020/08/commerce-department-further-restricts-huawei-access-us-technology-and.

369 Chad P. Bown, "US-China phase one tracker: China's purchases of US goods (As of November 2020)," Peterson Institute for International Economic, January 8, 2021, https://www.piie.com/research/piie-charts/us-china-phase-one-tracker-chinas-purchases-us-goods.

Huawei Ban Status in Europe



the agreement will have to be ratified by the EU.[370] The agreement in principle was concluded despite a statement by Jake Sullivan, at the time the Biden administration's national security advisor-designate, encouraging US-EU consultations about China's economic practices.[371]

The timing of the CAI as well as some of its terms raise the question of whether the United States and the EU will have a cooperative approach to countering China's malign economic actions, including distortive trade behavior and commercial espionage. Neither the Phase One agreement nor the CAI appear to answer this question. Among other points, it is worth first noting that neither is an initiating agreement—that is, there has been a great deal of both US and EU trade and investment with China in the absence of such agreements, so each agreement is intended to be more of a regulating arrangement than a new undertaking—though, of course, there are new terms. Second, there are provisions in each agreement, including terms seeking to limit forced technology transfers and provide greater market access, that demonstrate a commonality of objectives between the United States and the EU. On the other hand, the CAI calls on China to take certain steps—for example, with respect to labor standards—that many observers consider very unlikely, thus raising the prospect that the EU will accept promises rather than actions.

370 European Commission, EU and China reach agreement in principle on investment, press release, December 30, 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2541.

371 Jake Sullivan (@jakesullivan), "The Biden-Harris administration would welcome early consultations with our European partners on our common concerns about China's economic practices," Twitter, December 21, 2020, 7:33 p.m., https://twitter.com/jakejsullivan/status/1341180109118726144.

A bigger question is whether having signed the agreement the EU will continue to view China as a "systemic rival" and whether it maintains the view that stringent constraints on distortive Chinese economic behavior will still be needed particularly for the protection of transatlantic markets. China certainly intends that the answer be no. In a statement issued following a meeting between the Chinese foreign minister and his Cypriot counterpart shortly after the agreement in principle on the CAI, China's Ministry of Foreign Affairs wrote, "Consensus between China and the EU outweigh differences, as the two sides are cooperative partners, rather than systemic rivals."[372] That would, of course, be a major policy shift after two years of the EU and its member states having adopted increasingly tougher positions vis-à-vis China, including on issues ranging from 5G technology to direct investment by China.

Despite increasingly common positions, the Trump administration utilized more aggressive rhetoric and took more restrictive actions with respect to China than has Europe. In addition to the limits on Huawei, the CFIUS process has been utilized to bar Chinese acquisitions of US firms.[373] Additionally, the Trump administration issued two significant executive orders[374]—one for the information and communications technology sector and the other for the bulk-power system—"establishing a framework to prohibit transactions in each of these arenas with a foreign adversary that poses significant risk."[375] China is the obvious target although the implementing regulations have yet to be established. Additionally, there have been US sanctions against Chinese companies over human rights violations, especially regarding the Uyghur minority; the New York Stock Exchange is faced with the issue of delisting Chinese state-run companies three major Chinese state-run companies; and there are limits on the use of US software and machines to make chips for Huawei.[376] There are, by contrast, no comparable European actions. Moreover, a number of European countries appear to be more focused on the benefits of Chinese investment rather than the dangers, as illustrated to some extent by the fact that eighteen EU member states have engaged with the BRI,[377] and there is further engagement in the "17+1" initiative between China and seventeen EU and non-EU nations, even as some of these participants have begun to grow wary of China's intentions.[378]

There have been calls on both sides of the Atlantic for greater commonality of action with respect to China. The advent of a new US administration significantly increases the prospect of common transatlantic approaches to China, though it is far from clear precisely what the Biden administration will decide regarding the already significant actions that the United States has taken vis-à-vis China. Additionally, the differences over antitrust, data, taxation, and transatlantic trade that exist between the United States and the EU—while not directly China-related—may add to the difficulty of achieving common China policies. As the foregoing analysis suggests, consultations are clearly necessary and agreement on a coordinated approach to China's most harmful actions would appear of high importance. The discussion in the next section proposes key elements of a coordinated transatlantic economic policy toward China.

3. Possible Transatlantic Responses

An effective transatlantic strategy to respond to China's economic challenges would include common US and European approaches to protecting their own markets from Chinese depredation, coordinated efforts for access to markets in China, and common approaches with respect to economic policies worldwide. Generally, it will be most useful to seek an approach of strategic compatibility and coordination rather than a more formal approach that collective action would require, especially given calls for European "autonomy" and "sovereignty" as well as the multiplicity of bureaucratic structures that Europe presents. As has been described: "Europe now has the size, capabilities, inclinations, and bureaucratic structures that generate decision-making in many areas without requiring engagement with the United States. … Even when the broad strategy is in accord, such differences can require a degree of flexibility of approach in support of common objectives. The European Union is, of course, a main player. But, not

372 Ministry of Foreign Affairs of the People's Republic of China, "Wang Yi Meets with Cypriot Foreign Minister Nicos Christodoulides," January 5, 2021, https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1844488.shtml.

373 David McLaughlin, Saleha Mohsin, and Jacob Rund, "All About Cfius, Trump's Watchdog on China Dealmaking," *Washington Post*, September 15, 2020, https://www.washingtonpost.com/business/energy/all-about-cfius-trumps-watchdog-on-china-dealmaking/2020/09/15/1fdb46fa-f762-11ea-85f7-5941188a98cd_story.html.

374 The White House, "Executive Order on Securing the United States Bulk-Power System," May 1, 2020, https://www.whitehouse.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/; the White House, "Executive Order on Securing the Information and Communications Technology and Services Supply Chain," May 15, 2019, https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

375 Kramer, *Effective Resilience*, 21.

376 Qin, "China's New Rules."

377 Green Belt and Road Initiative Center, *Countries of the Belt and Road Initiative (BRI)*, https://green-bri.org/countries-of-the-belt-and-road-initiative-bri#:~:text=34%20BRI%20countries%20are%20in,are%20part%20of%20the%20BRI.

378 Emilian Kavalski, "How China lost central and eastern Europe," *Conversation*, July 20, 2020, updated July 30, 2020, https://theconversation.com/how-china-lost-central-and-eastern-europe-142416.

only is it not the simplest structural entity (for example, three EU presidents combined to give a press conference after a meeting with China), it is not the only European Indo-Pacific actor. Relevant competencies are also found at national levels …"[379]

Effective transatlantic coordination will, therefore, require multiple channels. As part of such efforts, dialogue between the United States and EU will be important, but a broader and more effective approach would be generated by the establishment of a "Transatlantic Coordinating Council on China" that would include Canada, Iceland, Norway, and the UK, important nations for trading and security issues that are not encompassed within the EU.[380] The proposed council would provide a central forum for discussion and coordination among relevant players on the multiple issues that China presents. Such a forum would include the member nations of both the EU and NATO as well as the EU and NATO as entities. Establishment of a "Transatlantic Coordinating Council on China" would allow decision making that takes account of the full scope of the issues that China presents, including when decisions in one arena have ramifications for another. An expanded exchange of intelligence and diplomatic information, as well as including engagements with the private sector, would also be helpful in establishing a common perspective on which to base policy.

a) Policy for transatlantic markets

A commonly agreed approach to trade with China in transatlantic markets that includes a focus on resilience of supply chains could provide a basis for compatible transatlantic policies. Key elements would include limitations in transatlantic markets as a consequence of strategic or important equitable market competition considerations,[381] enhancement of resilience for key critical infrastructures, and tying Chinese access to transatlantic markets to reciprocal access to Chinese markets. The United States and Europe could agree on the following:

Trade. For strategic sectors vital to national security or other critical national objectives, Chinese products, components, and services should be excluded from the supply chain unless their use is specifically approved by the government in question.[382] Comparable limitations should be placed on Chinese investments in strategic sectors whether through financial, licensing, or other transactions. Those limitations would necessarily include the defense and intelligence sectors, and perhaps others, such as advanced and emerging technologies.

For sectors not designated strategic for national security reasons, the question of China's exclusion from the supply chains or investments in transatlantic markets should nonetheless be evaluated at a more granular level,[383] and a particular attention should be given to key critical infrastructures. Those key critical infrastructures would include energy (electric grid and pipelines), food, finance, health, information and communications technology, transportation, and water.[384]

Supply chain issues will be of greatest concern in the context of software. Software frequently includes flaws, creating vulnerabilities that can be exploited, and supply chains are mechanisms for inserting maliciously intended flaws.[385] The United States and Europe should prohibit the use of Chinese software in elements of the supply chain for key critical infrastructures that could lead to exploitation posing significant risks.[386]

For non-strategic sectors unfairly affected by China's state-directed economic practices—particularly for emerging technologies like those identified in China's Made in China 2025 initiative—the United States and Europe should develop frameworks that will have selective, but effective, offsetting impact, including import restraints and/or selective focused tariffs so as to ensure a level playing field for US and European firms.[387]

For other sectors, the United States and Europe should seek to establish generally open trade for commercial products and services to commercial users, but subject to the caveat that access to the US and European markets should depend on generally comparable access to China's domestic market.[388] However, it will also be important for the United States and Europe to have common approaches to new Chinese rules regarding responses to limits on

379 Franklin D. Kramer, *Priorities for a Transatlantic China Strategy,* Atlantic Council, November 2020, 6, https://www.atlanticcouncil.org/wp-content/uploads/2020/11/PRIORITIES-FOR-A-TRANSATLANTIC-CHINA-STRATEGY-IB.pdf.

380 Ibid.

381 Kramer, *Managed Competition*, 3.

382 Kramer, *Effective Resilience*, 2.

383 Ibid.

384 Ibid., 19.

385 Ibid., 2.

386 Ibid.

387 Kramer, *Managed Competition*, 2.

388 Ibid.

trade with China, as described above. Those Chinese rules are so new as of this writing that the most that can be said of them is that their potential impact should be a key element of transatlantic consultation.

Enhancing Resilience. Effective resilience will best be achieved by the transatlantic nations working together. First, it should be made clear that North America and Europe will be considered reliable elements in the supply chains for one another.

Second, investments will be required to obviate reliance on certain Chinese capabilities, for example, both the rare earth sector and 5G technologies. A coordinated transatlantic approach could support both innovation and investment efficiency in such cases.

Third, the United States and Europe should additionally agree that key critical infrastructures should have a resilience plan that would avoid overdependency on China for their supply chains. A resilience plan mandate should require key critical infrastructure companies to have at a minimum non-Chinese companies in their supply chains—a "China-plus one" approach—to a sufficient extent so that China does not have an exclusive or predominant position affecting such critical infrastructures. Moreover, the creation of new suppliers will be more economically efficient if markets exist on both sides of the Atlantic. Providing economic incentives for the establishment of such new capabilities could be important, and transatlantic cooperation on common incentives would be valuable. Finally, as noted above, both sides of the Atlantic should agree that China should be excluded from the strategic supply chains of defense and intelligence activities, areas where the transatlantic nations work extremely closely together in the context of NATO and otherwise.

Fourth, as discussed above, Chinese capabilities should not be included in information technology and communications networks. Since transatlantic companies are targets of Chinese cyber espionage, a coordinated transatlantic approach to establishing resilient cybersecurity architectures to be utilized by businesses, but run on their behalf by expert cybersecurity providers, could be a key element in providing protection and an important component of an effective transatlantic China strategy.[389] Additionally, an "International Cyber Stability Board," comprised of like-minded nations, could undertake campaigns designed to protect against Chinese cyber espionage and other disruptive cyber actions.[390]

Fifth, the United States and Europe should each enact policies to enhance innovation, including the provision of significant resources for research and development and the use of governmental programs and policies to support key initiatives—with particular attention to small and medium-sized enterprises.[391] With substantial governmental funds available to businesses as a result of COVID-19, utilizing some of these resources to spur innovation would be desirable.

b) Policy for markets in China

The key issues related to Chinese markets are protection against forced technology transfers and equitable market access.

Where US or European firms export to China or operate via subsidiaries, joint ventures, or other such arrangements in China, the United States and Europe should limit the transfer of technology, including emerging technologies and research into advanced technologies, unless approved by national governments. Each side of the Atlantic should adopt an enhanced review mechanism, which by requiring automatic review will provide support to companies as the government will be engaged in the decision making.[392]

The United States and Europe could agree on those categories of technology that would be generally limited and those generally authorized for transfer, thereby limiting restrictions to important arenas. At a minimum, this would require prohibition of support to Chinese military and security agencies. The United States and Europe would likewise need to come to agreement on rules for advanced and emerging technologies as well as to determine how to deal with China's military-civil fusion (MCF) policy.[393]

Otherwise, as noted above, the United States and Europe should seek generally open trade for commercial products and services to commercial end users, but subject to the very important caveat that Chinese access to US and European markets should depend on generally

389 Kramer, *Effective Resilience*, 28.

390 Frank Kramer, Bob Butler, and Catherine Lotrionte, "Raising the Drawbridge with an International Cyber Stability Board," *Cipher Brief*, March 4, 2019, https://www.thecipherbrief.com/raising-drawbridge-international-cyber-stability-board.

391 See, e.g., European Council and Council of Europe, *COVID-19: the EU's response to the economic fallout*, accessed January 10, 2021, https://www.consilium.europa.eu/en/policies/coronavirus/covid-19-economy/.

392 Kramer, *Managed Competition*, 2.

393 US Department of State, *The Chinese Communist Party's Military-Civil Fusion Policy*, accessed January 10, 2021, https://www.state.gov/military-civil-fusion/.

Charles Michel, president of the European Council, at the EU-China leaders meeting via video conference, December 30, 2020, Brussels. *Source:* European Union

comparable US/European access to China's domestic market.[394] Achieving actual reciprocity and obtaining such access to Chinese markets will, however, face significant difficulties, especially given China's focus on building up its domestic capabilities as its recently announced "dual-circulation" policy states. The United States and Europe have each taken steps through the Phase One agreement and the CAI, respectively. Despite these agreements, there is essentially no likelihood that there will be any fundamental change in China's approach to its own internal markets. That means that, despite language in the agreements, the United States and the EU should prepare for China to favor its own companies and not be transparent with respect to the support that the government provides to markets.

The United States and the EU, therefore, should plan to squarely face such obstacles and undertake to support the transatlantic private sector through a two-part US-European effort: first, establishing a common platform for reporting to and review by governments of requests for technology transfer with the intent of limiting pressure on companies to transfer technology in order to obtain market access,[395] and, second, as has been done with the Phase One and CAI agreements, utilizing direct government negotiations to ensure market access, including by establishing agreements—such as the use of targets—for sectors.[396] An approach that achieves effective access through direct actions, including bargaining on a continuing basis by governments, is necessary since it is unlikely that any

394 Kramer, *Managed Competition*, 2.

395 *Hearing on Risks, Rewards, and Results: US Companies in China and Chinese Companies in the United States*, US-China Economic and Security Review Commission, February 28, 2019, revised March 10, 2019, (statement of Mary E. Lovely, professor of economics and Melvin A. Eggers Faculty Scholar at Syracuse University's Maxwell School of Citizenship and Public Affairs and a nonresident senior fellow at the Peterson Institute for International Economics in Washington, DC), 8-9, https://www.piie.com/system/files/documents/lovely20190228.pdf.

396 Kramer, *Managed Competition*, 2.

rules-based mechanism in and of itself will be effective in removing the many non-tariff barriers in Chinese markets (many of which operate at the provincial and local levels) that effectively restrict reciprocal access.[397] The need for continuing bargaining and enforcement of the terms of the agreements by governments will be a critical factor to support transatlantic companies that operate in China's domestic markets. Those companies, no matter how large, do not have the capacity to withstand Chinese governmental pressures and it will be up to the transatlantic governments to support their companies. A common transatlantic approach in this regard will be far more effective than separate efforts by the United States and Europe.

c) Policies for markets worldwide

Significant issues for the transatlantic nations with respect to China and worldwide markets include the future of the WTO, establishing secure 5G networks utilizing open architectures as an alternative to Huawei, and coordination of international economic activities.

For the WTO, challenges include resolving issues surrounding the dispute settlement mechanism, which is not specifically China-related but a necessary predicate to a common transatlantic WTO approach, and determining how China's state-driven economy should fit into the framework of WTO rules. Each of these is worthy of, and has been the subject of, extensive discussion. A common transatlantic perspective, as may be more likely with the new US administration, will be essential for a resolution that meets the economic objectives of the transatlantic nations. However, it is not likely that China will acquiesce to change its state-driven economic system under its current leadership. Accordingly, transatlantic nations must determine how to work together, including how to recalibrate their approach to the WTO in light of this circumstance.

5G networks will be important components of future personal, business, and government activities. The transatlantic nations should work together to ensure that there are alternatives to China's Huawei by developing open-architecture 5G capabilities. Open architectures would allow multiple companies to provide capabilities and components to the networks and, thereby, increase competitiveness, promote innovation, and eliminate reliance on untrustworthy vendors.[398]

Global markets present significant challenges for a coordinated transatlantic approach. Transatlantic firms are in competition with one another in many arenas, even as China will be a significant competitor, especially as its state-driven approach will allow it to undercut pricing of transatlantic firms. Governments can, however, provide useful support.

By way of example, each side of the Atlantic has undertaken actions to support the nations of the Indo-Pacific. The United States has its Indo-Pacific strategy, the EU its Connecting Europe and Asia strategy, and some nations, including France and Germany, have established their own Indo-Pacific policies. As part of these efforts, governments have provided support, including resources, to infrastructure, energy, and information technology efforts, and have developed standards and increased transparency on Chinese activities through, for example, the US Blue Dot Network.[399] These efforts are broadly in alignment, but diplomatic coordination could enhance their impact.

Moreover, additional common efforts could have significant added value, and it might even be possible to have some coordinated funding. For instance, establishing a multilateral "Blue-Green Initiative" that "focuses on climate change, environment, water, and health would be of high value."[400] The United States and the EU—along with other partners such as Canada and Japan— "could undertake a coordinated approach to providing investment and technical assistance in each of these areas."[401] As one example, a significant effort will be needed to provide vaccines and therapeutics for the coronavirus, and a common transatlantic approach would be highly valuable. Such activities would be valuable in and of themselves, and would also act as a counterpoint to the BRI.

4. Major Recommendations

i. A "Transatlantic Coordinating Council on China" should be established to provide a central forum for discussion and coordination on the multiple issues that China presents. Such a forum would include the member nations of both the EU and NATO as well as the EU and NATO as entities.

ii. For strategic sectors vital to national security or other critical national objectives, Chinese products, components, and services should be excluded from the

397 Ibid., 3.

398 See, e.g., Martijn Rasser and Ainikki Riikonen, *Open Future: The Way Forward on 5G*, Center for a New American Security, July 28, 2020, https://www.cnas.org/publications/reports/open-future.

399 US Department of State, *Blue Dot Network*, https://www.state.gov/blue-dot-network/.

400 Kramer, *Managed Competition, 3.*

401 Ibid.

supply chain unless their use is specifically approved by the government in question. For non-strategic sectors unfairly affected by China's state-directed economic practices, the United States and Europe should develop frameworks that will have selective, but effective, offsetting impact, including import restraints and/or selective focused tariffs so as to ensure a level playing field for US and European firms. For other sectors, the United States and Europe should seek to establish generally open trade for commercial products and services to commercial users, but subject to the caveats that access to the US and European markets should depend on generally comparable access to China's domestic market and that forced technology transfer should be barred.

iii. The transatlantic nations should work together to ensure that there are alternatives to China's Huawei by developing open-architecture 5G capabilities. Open architectures would allow multiple companies to provide capabilities and components to the networks and, thereby, increase competitiveness, promote innovation, and eliminate reliance on untrustworthy vendors.

iv. The United States and Europe should agree that key critical infrastructures should have a resilience plan that would avoid overdependency on China for their supply chains. A resilience plan mandate should require key critical infrastructure companies to have at a minimum non-Chinese companies in their supply chains—a "China-plus one" approach—to a sufficient extent so that China does not have an exclusive or predominant position affecting such critical infrastructures.

v. Since transatlantic companies are targets of Chinese cyber espionage, a coordinated transatlantic approach to establishing resilient cybersecurity architectures to be utilized by businesses, but run on their behalf by expert cybersecurity providers, could be a key element in providing protection and an important component of an effective transatlantic China strategy.

vi. The United States and the EU—along with select Asian allies—should work more closely together to provide investment and technical assistance in sectors related to climate change, environment, health, and water as alternatives to Chinese sponsored action.

Section B: Technology and Cyber Competition

Allied nations need to consider the trade, investment, military/security, as well as human rights challenges associated with China's rise as a technology and cyber superpower. The relative importance of these concerns is evaluated unevenly among transatlantic allies so far, with the United States and NATO being particularly concerned about the military and security implications of technology and cyber competition. Meanwhile, European allies and the EU tend to worry more about reciprocal market access, investment screening, risks to their industrial base, and data privacy protection. This may be shortsighted: Recent reports about alleged Chinese cyberattacks against India's electricity grid during the border tensions of 2020 suggest that critical infrastructures protection should be a key concern for all allies.[402]

Since technology and cyber issues intersect with several other topics that are covered in this study, the human rights-related problems of Chinese surveillance technologies and the trade, investment, and infrastructure-related challenges of technology and cyber competition with China have already been discussed in previous sections of this report. Accordingly, this section will primarily focus on the security-related aspects of technology and cyber competition with China.

Leadership on issues of high-technology and cyber innovation plays a key role for nearly all of China's strategic goals. The CCP defines progress not just in terms of the country's overall economic development but aims for ambitious technological milestones to be reached by 2049 that are to prove to the world at large, and especially to the Chinese public, the realization of the "Chinese Dream" and of the "rejuvenation of the Chinese nation." To this end, technological breakthroughs, no matter in which field, feature heavily in Chinese state propaganda. Technology-specific goals of the Made in China 2025 strategy include "70 per cent self-sufficiency in high technology industries by 2025 and global market dominance by 2049."[403] A further goal is to build a "strong military that can fight and win wars." By leapfrogging the United States and Europe, China aims to become a "science and technology superpower" and close "the gap with the West in areas such as robotics, artificial intelligence, unmanned and fully automated

402 David E. Sanger and Emily Schmall, "China Appears to Warn India: Push too Hard and the Lights Could Go Out," *New York Times* February 28, 2021, https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html.

403 Hybrid CoE, *Trends in China's Power Politics,* Hybrid CoE Trend Report, July 5, 2020, 24, https://www.hybridcoe.fi/publications/hybrid-coe-trend-report-5-trends-in-chinas-power-politics.

systems, quantum computing, space technology and hypersonic weapons."[404] Technological innovations, such as surveillance technologies, further serve as key enablers of domestic control and are also exported, thus becoming instruments of outreach for strengthening China's political and economic relations with like-minded countries.

Since 2013, China officially pursued a strategy of "civil-military integration" (CMI) that was elevated to the level of a national strategy in 2015 under a slightly changed moniker, Military-Civil Fusion (MCF), which indicated a strengthening of the concept.[405] It was bolstered in 2017 through the establishment of a Central Commission for Integrated Military and Civilian Development led by Xi himself that includes four CCP Politburo Standing Committee members in its ranks, indicating its exalted role within the Chinese government system. The goal of CMI or MCF has been described as "a comprehensive promotion of the integration of the military and civilian society in a variety of areas such as economic, science and technology, education, and human resource development."[406]

So far, this strategy has been successful: since Xi's ascent to power in 2012, a variety of technological breakthroughs have been achieved in highly prestigious fields such as moon landing, space docking, supercomputers, and quantum computing. In arms innovation, China has developed advanced aircraft prototypes and unmanned aerial and maritime systems, is constructing its second indigenously developed aircraft carrier, and has achieved an astounding overall naval fleet modernization within record time.

1. The Challenges

The security challenge faced by the United States and its allies from China's envisaged rise as a "tech superpower" is threefold: in the economic sphere, there is a need for allies to protect domestic technology industries against unfair competition and intellectual property theft; in the military-security sphere, there is a need to inhibit technology transfers to China that could further fuel China's military buildup and, thereby, exacerbate the existing security dilemma in the Indo-Pacific; and, last, there is a need to ensure the survivability and resilience of allies' critical infrastructures against interference, sabotage, or espionage.

a) Chinese state subsidies and the creation of a military-industrial-financial complex

To achieve the goal of becoming a science and technology superpower, China has extensively invested in research and development of emerging technologies. This was supported by a top-down industrial policy approach—a state-led and -financed effort to create a vast military-industrial-financial complex under the umbrella of large state-owned conglomerates which began in the mid-1990s under the leadership of Jiang Zemin. External shocks such as the Western arms embargo imposed on China after its massacre of pro-democracy protesters in Tiananmen Square in June 1989, the military-technological superiority demonstrated by US forces during the 1991 Gulf War, and the 1995-1996 standoff in the Taiwan Strait prompted Jiang to reconsider China's previous economic strategy that had been focused primarily on economic growth rather than military technology innovation.

Even though the lure of Chinese market access had already prompted many foreign firms to accept technology transfers within forced joint ventures, Jiang now urged China's science and technology elite to realize that "some of the world's most advanced technology is not for sale," implying it needed to be obtained by other means.[407] An indigenous innovation drive began that was funded generously by state-owned banks and, especially from the 2008 financial crisis onward, enabled Chinese companies to go on an investment spree in crisis-ridden technology sectors abroad.[408]

At the same time, China's leaders used their control of the state-owned banking sector to flood the defense-industrial base with a veritable avalanche of cash. The 12th Five-Year Plan (2011-2015) announced the government's intent to

404 Meia Nouwens and Helena Legarda, *Emerging technology dominance: what China's pursuit of advanced dual-use technologies means for the future of Europe's economy and defence innovation,* IISS-MERICS China Security Project Report, December 2018, 3-4, https://merics.org/sites/default/files/2020-05/181218_Emerging_technology_dominance_MERICS_IISS.pdf.

405 According to Audrey Fritz, "MCF can be defined as a strategy that strives to reinforce the PRC's ability to build the country into an economic, technological, and military superpower by fusing the country's military and civilian industrial and S&T resources. The strategy is aimed at promoting the sharing of resources and collaboration in research and applications, which ensures the mutually beneficial coordination of economic and national defense construction. MCF evolved from the former, more limited approach of CMI, which emphasized combining the military and civilian sectors. What distinguishes MCF from CMI is an increased level of coordination of military and civilian relations, a more balanced emphasis between military and civilian developments, and an institutional upgrade from simple combination to comprehensive integration." See Audrey Fritz, "China's Evolving Conception of Civil-Military Collaboration," *Trustee China Hand*, August 2, 2019, https://www.csis.org/blogs/trustee-china-hand/chinas-evolving-conception-civil-military-collaboration.

406 Hirofumi Kiriyama, "PLA Aims to Become a World-class Force," *East Asian Strategic Review* 2018, 70-71.

407 From a speech delivered by then-Chinese President Jiang Zemin on May 26, 1995, at the high-level Chinese National Conference on Science and Technology titled "努力实施科教兴国的战略" (Strive hard to implement the strategy of rejuvenation through science and education), http://www.reformdata.org/1995/0526/4385.shtml.

408 Sarah Kirchberger and Johannes Mohr, "China's Defence Industry" in *The Economics of the Global Defence Industry,* eds. Keith Hartley and Jean Bélin (London: Routledge, 2019), 35-68; 53.

pour $600 billion into strategic sectors within that timeframe; an IHS Jane's analysis of the publicly announced state bank loan deals to state-owned aerospace companies between 2007 and 2017 alone amounted to at least $87 billion. Individual companies, such as the shipbuilding conglomerates China State Shipbuilding Corporation (CSSC) and China Shipbuilding Industry Corporation (CSIC) or the aviation holding Aviation Industry Corporation of China (AVIC), have received loans from state-owned banks in the order of dozens of billions of dollars within a single year.[409] A non-state-owned (although founded by former military officers) company like Huawei, a rare example of a nominally private company acting as a trusted supplier of critical communications infrastructure to the People's Liberation Army (PLA), was given access to huge credit lines from state banks. In December 2019, an investigation by the *Wall Street Journal* concluded that Huawei had over the years received state aid, including tax breaks, financing, and access to cheap resources, amounting to a staggering $75 billion.[410]

By listing their subsidiaries on foreign stock exchanges to raise foreign capital, and through the creation of cross-shareholdings between Chinese defense industries and large state-owned banks, the vast financial resources available to the Chinese technology and defense-industrial base through subsidies and tax breaks have been further supplemented.[411] This state-capitalist approach to research and development (R&D) was further complemented by covert and illicit technology acquisition strategies.

China is focusing its R&D efforts especially on emerging technologies in dual-use fields such as artificial intelligence (AI), robotics, unmanned systems, and space that have potential military uses. Many emerging technologies are inherently dual-use and directly or indirectly contribute to China's military modernization, while also enhancing the CCP's capacity to control its population. Even civilian AI firms (e.g., Baidu, Alibaba, Tencent, or iFlytek) are directly engaged in the development of dual-use technologies and have established dedicated research facilities for it.[412]

Furthermore, Chinese companies' market access abroad, for example, along the BRI, is bolstered through political support and state subsidies for exports, while foreign companies do not enjoy reciprocal market access in China. Western enterprises thus operate on an uneven playing field when competing with Chinese technology entities. This circumstance, when combined with a multitude of covert and illicit methods to acquire foreign technology that range from traditional espionage to cyber espionage to seemingly innocent academic exchanges, poses grave dangers to the long-term security of the industrial bases of Western high-tech countries.[413]

b) Surveillance technologies and 'digital authoritarianism'

Domestically, to secure the CCP's power, China's leaders have created a dystopian surveillance state—a high-tech dictatorship of a previously unknown type.[414] In addition to featuring the world's most extensive system of Internet control, the "Great Firewall," in its latest form the Chinese surveillance state employs a wide range of automated, AI-supported recognition technologies. These include a pervasive use of automated facial recognition in the public sphere, even public toilets; "smart glasses" worn by police officers; and even "robotic birds"—unmanned aerial vehicles in bird shape that use gait recognition for surveilling individuals from the air.[415] These technologies are used in service of a "Social Credit System" that aims to make the individual Chinese citizen fully transparent to the state and incentivize "good" behavior while discouraging unwanted actions through a variety of punitive consequences inflicted upon individuals with a negative overall score.

This approach also extends to foreigners and foreign entities in the form of the "Social Credit System for Foreign Companies."[416] Western companies have, perhaps in some

409 Jon Grevatt, "China's CSIC secures 'international credit line' worth USD7.3 billion," *Jane's Defence Weekly*, December 6, 2018.

410 Chuin-Wei Yap, "State Support Helped Fuel Huawei's Global Rise," *Wall Street Journal,* December 25, 2019, https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736.

411 Jon Grevatt, "China to Double Lending to Strategic Industries," *Jane's Defence Weekly,* March 8, 2011; Jon Grevatt, "A Great Leap Forward," *Jane's Defence Weekly,* May 3, 2017.

412 Elsa B. Kania, *Technological entanglement: Cooperation, competition, and the dual-use dilemma in artificial intelligence,* ASPI's International Cyber Policy Centre Policy Brief Report No. 7/2018, 7, https://www.aspi.org.au/report/technological-entanglement.

413 Nouwens and Legarda, *Emerging technology*; William C. Hannas and Huey-Meei Chang, "Chinese Technology Transfer: An Introduction" in *China's Quest for Foreign Technology: Beyond Espionage,* William C. Hannas and Didi Kirsten Tatlow (London: Routledge, 2020), 3-20.

414 Kai Strittmatter, *We Have Been Harmonized: Life in China's Surveillance State,* trans. Ruth Martin, (London: Old Street Publishing, 2019).

415 Sigal Samuel, "China Is Going to Outrageous Lengths to Surveil Its Own Citizens," *Atlantic*, August 16, 2018, https://www.theatlantic.com/international/archive/2018/08/china-surveillance-technology-muslims/567443/; Stephen Chen, "China takes surveillance to new heights with flock of robotic Doves, but do they come in peace?" *South China Morning Post*, June 24, 2018, https://www.scmp.com/news/china/society/article/2152027/china-takes-surveillance-new-heights-flock-robotic-doves-do-they.

416 Tom Hancock, "China to impose 'social credit' system on foreign companies," *Financial Times,* August 28, 2019, https://www.ft.com/content/726905b6-c8dc-11e9-a1f4-3669401ba76f.

Participants interact with robots at the World Economic Forum - Annual Meeting of the New Champions in Tianjin, People's Republic of China 2018. *Source:* World Economic Forum/Greg Beadle (https://creativecommons.org/licenses/by-nc-sa/2.0/)

cases unwittingly, contributed key technologies to this vast surveillance and Internet control effort.[417] The speed and scope of this development has been staggering. While the surveillance capacity in Xinjiang province is so far the most extensive, China's Ministry of Public Security has funneled billions of dollars into the "Skynet" and "Sharp Eyes" projects to enable comprehensive surveillance of the entire Chinese population, with the aid of an additional four hundred million cameras and advanced facial recognition technology.[418] The combined cost of all "internal security" measures in China has long surpassed the defense budget.

c) Exporting 'digital authoritarianism'

By exporting surveillance technologies to other BRI countries within the framework of a "Digital Silk Road," China popularizes its governance approaches and technical standards while building political leverage within countries to spread its political narratives abroad, in addition to potentially opening the door for surveillance and sabotage of critical infrastructures in BRI countries.[419] In Europe, Serbia has been at the forefront of utilizing Chinese surveillance technologies, but individual localities in the EU have also opted for "smart city" projects with Chinese partners, including Duisburg and Gelsenkirchen in Germany and Valenciennes in France. As the Australian think tank ASPI's database of worldwide Chinese technology investments shows, the twenty-three largest Chinese technology companies as of October 2020 had created a vast web of overseas infrastructure investments that consist, among other things, of terrestrial and undersea data cables, research centers, R&D labs, manufacturing facilities, satellite calibration centers, 5G networks, and smart city-public security

417 Yaya J. Fanusie, "Don't sleep on China's new blockchain internet," *Lawfare*, November 10, 2020, https://www.lawfareblog.com/dont-sleep-chinas-new-blockchain-internet.

418 Fergus Ryan, Danielle Cave, and Vicky Xiuzhong Xu, *Mapping* More *of China's Tech Giants: AI and Surveillance,* ASPI International Cyber Policy Centre Issues Paper Report No. 24/2019, November 28, 2019, 17, https://www.aspi.org.au/report/mapping-more-chinas-tech-giants.

419 Hybrid CoE, *Trends*, 25.

projects.[420] Chinese surveillance technical solutions have been exported to at least ninety-six countries, while Chinese 5G network technology is used by least forty-five countries, and, so far, at least 115 smart city-public security projects exist in seventy-one countries in Europe, Africa, Asia, and South America. In Europe, non-EU countries Serbia, Bosnia and Herzegovina, Moldova, and Turkey, but also EU member states such as Hungary, the Netherlands, France, Germany, the Czech Republic, and Italy, have smart city projects in partnership with Huawei.[421]

d) Cyber connectivity and defining global technology standards

China's cyber innovation and control strategy, according to Nigel Inkster, has "the potential to shape the future of the internet at a global level," a fact that "has attracted little attention from the West's top policymakers." In a recent non-paper on EU cyber diplomacy, EU members Estonia, France, Germany, Poland, Portugal, and Slovenia warn against the danger of "major actors that are increasingly willing to shape the digital environment and the discussion surrounding it, meaning that the EU and its Member States have to assert themselves in international cyberspace norm-setting and technological standard-setting bodies." Furthermore, the non-paper points out that: "States with an authoritarian outlook are increasingly trying to enforce their interests in cyberspace and in the technological realm and the EU and its Member States have to react by promoting their values and interests, which include human rights, prosperity, security and Europe's digital sovereignty."[422]

China's cyber strategy leverages the sheer size of the Chinese user community to force foreign companies active in China to "comply with Chinese restrictions and technical criteria," concretized in a new Cybersecurity Law in 2017. China purposefully nurtures indigenous technology companies such as Huawei, ZTE, or Alibaba to become global giants, exports Chinese network technology to developing countries, creates "cyber-security partnerships" (e.g., with Russia in 2015), cooperates with Shanghai Cooperation Organisation countries within the United Nations to further an International Code of Conduct for Information Security, and promotes concepts such as "cyber sovereignty" and "information security" to defend its right to censor and control the Chinese Internet.[423]

China is pursuing a top-down approach to invest heavily in supercomputing and quantum computing and is among the technological leaders in other quantum technologies, such as quantum cryptography and quantum radar, all of which have military applications.[424]

A further aspect is China's promotion abroad of its indigenous Global Navigation Satellite System (GNSS), BeiDou, within the context of the BRI Space Information Corridor. BeiDou, a system crucial to China's military development that was purposefully developed into a dual-use infrastructure enabling a wide variety of civilian applications, reached full global coverage ahead of schedule and earlier than its European rival, Galileo, in mid-2020 and, according to a study, 85 percent of the world's capital cities in 195 countries already have more frequent SatNav connection with BeiDou satellites than with US GPS satellites.[425] BeiDou is further partnering with the Russian GNSS system GLONASS by using the same chipset system, which allows users to combine the signals of at least forty satellites, enhancing reach and resolution.[426]

As European governments and the EU increasingly recognize, there is indeed a danger that through the Digital Silk Road and the BRI Space Information Corridor and by partnering with Russia and other authoritarian countries, China will define technical standards in vast stretches of the globe.[427]

420 ASPI International Cyber Policy Centre, *Mapping China's Tech Giants Public Database*, https://chinatechmap.aspi.org.au.

421 Ibid.

422 German Federal Foreign Office, "EU Cyber Diplomacy — working together for a free and secure cyberspace," November 19, 2020, https://www.auswaertiges-amt.de/en/aussenpolitik/themen/eu-cyber-non-paper/2418984.

423 Nigel Inkster, *China's Cyber Power* (Oxon: Routledge, 2016), 14-15.

424 Michael Raska, "China's Quantum Satellite Experiments: Strategic and Military Implications," RSIS Commentary No. 223, September 5, 2016, https://www.rsis.edu.sg/rsis-publication/rsis/co16223-chinas-quantum-satellite-experiments-strategic-and-military-implications/; Paul Verhagen and Erik Frinking, *Understanding the Strategic and Technical Significance of Technology for Security: Implications of Quantum Computing within the Cybersecurity Domain*, The Hague Center for Strategic Studies, September 18, 2019, 17, https://hcss.nl/report/understanding-strategic-and-technical-significance-technology-security-implications-quantum; Sebastien Roblin, "No More 'Stealth' Submarines: Could Quantum 'Radar' Make Submarines Easy to Track (And Kill)?" *Buzz,* April 27, 2019, https://nationalinterest.org/blog/buzz/no-more-stealth-submarines-could-quantum-radar-make-submarines-easy-track-and-kill-54547.

425 Toru Tsunashima, "In 165 countries, China's BeiDou eclipses American GPS," *Financial Times,* November 30, 2020, https://www.ft.com/content/58fd14f0-4fba-4242-bf25-3f493979125e.

426 Mark Episkopos, "Is this the real Russia-China alliance America should fear?" *Buzz,* December 16, 2018, https://nationalinterest.org/blog/buzz/real-russia-china-alliance-america-should-fear-38762.

427 Sam Olsen, "China is winning the war for global tech dominance," *The Hill,* October 4, 2020, https://thehill.com/opinion/technology/518773-china-is-winning-the-war-for-global-tech-dominance; Daniel H. Russel and Blake H. Berger, *Weaponizing the Belt and Road Initiative,* Asia Society Policy Institute Report, September 2020, 8, https://asiasociety.org/policy-institute/weaponizing-belt-and-road-initiative.

e) Threats to allied critical infrastructures

Concern over the security of allies' critical infrastructures, such as data cables, 5G networks, electricity grids, transport and logistics infrastructures, satellite systems, etc., has alarmed NATO sufficiently for its secretary general, Jens Stoltenberg, to comment in 2020 that "China is coming closer to us, we see that in the Arctic, we see they are heavily investing in critical infrastructure in Europe, and we see of course China also operating in cyberspace," pointing out that NATO's new approach to China "is not about deploying NATO into the South China Sea, but responding to the fact that China is coming closer to us."[428] These remarks also reflect increasing concern regarding Chinese investments in ports in the Mediterranean and on European Atlantic coasts—not merely because of possible PLA Navy (PLAN) access, but also because of the potential for sabotage and surveillance of allied military vessels that routinely use these ports.[429] Further concerns exist regarding data cable security, e.g., a planned "Arctic Connect" data cable linking Asia and Europe through the Northern Sea Route along the Arctic Coast as part of the "Digital Silk Road."[430] Among the approximately 385 active undersea fiber-optic data cables that carry about 95 percent of global Internet traffic, Huawei Marine, a daughter company of Huawei, has already worked on ninety cable projects worldwide—potentially offering it the ability to "attach devices that divert or monitor data traffic—or, in a conflict, to sever links to entire nations."[431]

A particularly problematic infrastructure project in the European Arctic is the fully Chinese-built and -operated China Remote Sensing Satellite North Pole Ground Station in Kiruna, Sweden, that was opened in 2016 and aims to bolster China's military remote sensing satellite constellations—Yaogan and Gaofen—by enhancing the data download rate significantly and, thereby, according to Chinese experts quoted on the issue, significantly boosting China's "capability for global data surveillance."[432] Sweden was apparently chosen because it is not a NATO member, and it seems the implications of this station for enhancing China's military remote sensing capabilities were deliberately hidden from Swedish counterparts during the negotiations, as were the military affiliations of the Chinese project leaders.[433]

Infrastructure security concerns in Europe have grown more acute due to an intensifying Sino-Russian military cooperation that encompasses increasingly sophisticated types of technological cooperation in strategic fields, ranging from cyber control and 5G to unmanned systems development, joint submarine development, the abovementioned GLONASS-BeiDou navigational satellite systems cooperation, and even ballistic missile early warning.[434] Since Russian President Vladimir Putin no longer rules out the possibility of a full-fledged Sino-Russian military alliance,[435] the United States and its allies need to consider the implications of increasing strategic technology and cyber coordination between China and Russia. They should especially consider its meaning for the security of critical infrastructures in Europe in the event of tensions with Russia, should they have been built with the help of Chinese technology partners such as Huawei that are subject to party-state control via embedded CCP party cells

428 Reuters staff, "NATO chief says on Huawei: UK review of 5G security is important," Reuters, June 10, 2020, https://www.reuters.com/article/us-britain-huawei-nato-idUSKBN23H0US.

429 *Maritime Executive*, "Study: 'Belt and Road' Ports Align with China's Military Interests," April 19, 2018, https://www.maritime-executive.com/article/study-belt-and-road-ports-are-intended-for-china-s-navy; Devin Thorne and Ben Spevack, *Harbored Ambitions: How China's Port Investments Are Strategically Reshaping the Indo-Pacific,* C4ADS Report, April 17, 2018, https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5ad5e20ef950b777a94b55c3/1523966489456/Harbored+Ambitions.pdf; Yonah Jeremy Bob, "China wins on Haifa port, but fights with US for the future - analysis," *Jerusalem Post*, December 12, 2019, https://www.jpost.com/israel-news/china-wins-on-haifa-port-but-fights-with-us-for-the-future-analysis-610510; Joanna Kakissis, "Chinese Firms Now Hold Stakes In Over A Dozen European Ports," *Morning Edition*, NPR, October 9, 2018, https://www.npr.org/2018/10/09/642587456/chinese-firms-now-hold-stakes-in-over-a-dozen-european-ports; Stanislav Abaimov and Paul Ingram, *Hacking UK Trident: A Growing Threat,* British American Security Information Council (BASIC), June 2017, http://www.basicint.org/wp-content/uploads/2018/06/HACKING_UK_TRIDENT.pdf.

430 Frank Jüris, *Handing over infrastructure for China's strategic objectives: 'Arctic Connect' and the Digital Silk Road in the Arctic,* Sinopsis Policy Brief, March 7, 2020, https://sinopsis.cz/en/arctic-digital-silk-road/.

431 Jeremy Page, Kate O'Keeffe, and Rob Taylor, "America's Undersea Battle With China for Control of the Global Internet Grid," *Wall Street Journal*, March 12, 2019, https://www.wsj.com/articles/u-s-takes-on-chinas-huawei-in-undersea-battle-over-the-global-internet-grid-11552407466.

432 Stephen Chen, "China launches its first fully owned overseas satellite ground station near North Pole," *South China Morning Post,* December 16, 2016, http://www.scmp.com/news/china/policies-politics/article/2055224/china-launches-its-first-fully-owned-overseas-satellite; Xiao-Ming Li et al., "Capabilities of Chinese Gaofen-3 Synthetic Aperture Radar in Selected Topics for Coastal and Ocean Observations," *Remote Sensing*, November 30, 2018, 3, doi:10.3390/rs10121929.

433 Sam Olsen, "China is learning how to lose friends and alienate countries," *What China Wants*, December 14, 2020, https://whatchinawants.substack.com/p/china-is-learning-how-to-lose-friends.

434 Samuel Bendett and Elsa B. Kania, *A new Sino-Russian high-tech partnership: Authoritarian innovation in an era of great-power rivalry,* ASPI International Cyber Policy Centre Policy Brief Report No. 22/2019, https://www.aspi.org.au/report/new-sino-russian-high-tech-partnership; Caleb Larson, "Russia and China Want to Build a 'Non-Nuclear' Submarine Together," *Buzz,* August 28, 2020, https://nationalinterest.org/blog/buzz/russia-and-china-want-build-non-nuclear-submarine-together-167911; Tracy Cozzens, "Russia passes law on GLONASS-BeiDou cooperation," *GPS World,* July 29, 2019, https://www.gpsworld.com/russia-passes-law-on-glonass-beidou-cooperation/; Rajeswari Pillai Rajagopalan, "Russia-China Strategic Alliance Gets a New Boost with Missile Early Warning System," *Diplomat*, October 25, 2019, https://thediplomat.com/2019/10/russia-china-strategic-alliance-gets-a-new-boost-with-missile-early-warning-system/.

435 Associated Press, "Putin: Russia-China military alliance can't be ruled out," *Yahoo News*, October 22, 2020, https://news.yahoo.com/putin-russia-china-military-alliance-173246293.html; Jun Mai, "Beijing gives cautious welcome to Vladimir Putin's hint over Russia-China military alliance," *South China Morning Post,* October 25, 2020, https://www.scmp.com/news/china/diplomacy/article/3107027/beijing-gives-cautious-welcome-vladimir-putins-hint-over.

and beholden to the Cybersecurity Law and the National Security Law of the People's Republic of China.[436] When weighing cost factors against security implications in critical infrastructure development, allies should err on the side of caution.

f) Dual-use high-tech exports aiding China's military buildup

A 2019 C4ADS report that analyzed import records and investment transactions of 1,655 companies linked to China's defense-industrial base warns that there is "a clear risk that foreign strategic technologies and expertise could inadvertently contribute to China's growing military capabilities," thereby aggravating the existing security dilemma in the Indo-Pacific.[437]

In some cases, transfers have occurred legally through mergers and acquisitions (M&A). According to IHS Jane's, at least a dozen Western commercial aerospace companies were taken over by Chinese counterparts between 2009 and 2014;[438] but an especially striking case of transferred dual-use technology with potentially grave repercussions was the 2008 takeover of the British firm Dynex Semiconductor by a Chinese railway company, the Hong Kong-listed Zhuzhou CSR Times Electric, which is a subsidiary of the large state-owned enterprise China South Rail (CSR). This takeover seems to have enabled the PLA to manufacture insulated-gate bipolar transistor (IGBT) semiconductors, a critical component in electromagnetic aircraft launch systems (EMALS) used on next-generation aircraft carriers as well as in railguns. This technology is subject to EU export controls and since 2009 was listed under Category III of the UK Strategic Export Control Lists as part of the EU Council Regulation 428/2009. Nevertheless, in 2008, the UK government did not block the takeover of Dynex Semiconductor.

China's unexpectedly early acquisition of EMALS technology could now mean that it will be able to skip past the stage of steam catapults for its future carriers, a significant military advantage.[439] In many other cases, Western companies have legally exported dual-use technologies that have military applications which are not immediately apparent when seen in isolation. For instance, by combining foreign-sourced hydrographic survey equipment, other technologies that enable oceanographic research, unmanned maritime systems, and navigational equipment with AI and supercomputing, China has begun to create an underwater surveillance network in the South China Sea whose purpose is the enhancement of territorial control over a contested maritime area.[440] The degree to which European technologies, technology investments, and technology cooperation have been directly benefitting China's military buildup is, so far, a largely overlooked aspect of the challenge posed by China's technology acquisition strategy. It should be reviewed.

g) Illicit and covert technology transfers

Next to R&D, China has long been engaged in a massive effort to overcome technology bottlenecks through espionage, both cyber and traditional. Documented cases reveal that the focus lies on acquiring aerospace technologies, military electronics, unmanned systems, rockets, space systems, source codes, and also particular military-grade materials and subcomponents. Military cyber espionage is conducted by specialized units of the PLA.[441] Recently published studies of Chinese illicit and covert technology acquisition methods have further shown that a multitude of instruments are used across a wide range of countries to supplement outright espionage. These range from United Front Work Department (UFWD) activities, talent programs such as the "1000 Talents Program," and academic exchanges to the insertion of active PLA personnel posing as civilian researchers at Western high-tech research facilities and universities.[442] This is an area where allies would benefit from stronger monitoring and data-exchange efforts; for instance, the relationships between National Key Laboratories, key S&T university

436 Mathieu Duchâtel and François Godement, *Europe and 5G: the Huawei Case, Part 2*, Policy Paper, Institut Montaigne, June 2019, https://www.institutmontaigne.org/en/publications/europe-and-5g-huawei-case-part-2.

437 Marcel Angliviel, Benjamin Spevack, and Devin Thorne, *Open Arms: Evaluating Global Exposure to China's Defense-Industrial Base,* C4ADS Report, October 17, 2019, 3, https://www.c4reports.org/open-arms.

438 Tate Nurkin, "Catching Up: China's Space Programme Marches On," *Jane's Defence Weekly*, July 30, 2015.

439 Angliviel, Spevack, and Thorne, *Open Arms*, 47-50; Paul Huang, "By Snatching Up British Company, China Closes Gap on US Naval Supremacy," *Epoch Times,* December 15, 2017, updated February 4, 2018, https://www.theepochtimes.com/by-snatching-up-british-company-china-closes-gap-on-us-naval-supremacy_2389025.html.

440 Jeffrey Lin and P.W. Singer, "The Great Underwater Wall Of Robots: Chinese Exhibit Shows Off Sea Drones," *Popular Science,* June 22, 2016, https://www.popsci.com/great-underwater-wall-robots-chinese-exhibit-shows-off-sea-drones; Angliviel, Spevack, and Thorne, *Open Arms,* 51-54.

441 William C. Hannas, James Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization* (London: Routledge, 2013), 250-270; Nalani Fraser et al., "APT41: A Dual Espionage and Cyber Crime Operation," *Threat Research*, August 7, 2019, https://www.fireeye.com/blog/threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html; Mandiant Corporation, *APT1: Exposing One of China's Cyber Espionage Units,* February 19, 2013, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

442 William C. Hannas and Didi Kirsten Tatlow, eds., *China's Quest for Foreign Technology: Beyond Espionage* (London: Routledge, 2020); Alex Joske, *Picking flowers, making honey: The Chinese military's collaboration with foreign universities*, ASPI International Cyber Policy Center Policy Brief, Report No. 10/2018, October 30, 2018. https://www.aspi.org.au/report/picking-flowers-making-honey.

laboratories, and commercial R&D labs is often not sufficiently well understood in Western countries, but form a key element of MCF. Searchable databases, such as ASPI's China Defence Universities Tracker, are useful tools for gaining a better understanding of a research unit's affiliation and the level of risk through exchanges with particular Chinese entities.[443]

2. Transatlantic Convergence and Divergence

Transatlantic allies have somewhat different perceptions of the Chinese technology and cyber challenge depending on their own role as either recipient or producer of technological innovations, their vulnerability toward China in a security sense, and their relative need for infrastructure investments and resulting openness to Chinese investment. No matter their orientation, it is important for allies to realize that Chinese attempts to shape and define technical standards of emerging technologies across the globe, and the willingness to use exports of technological solutions to bolster political aims, make clear that "technology is not an ethics-neutral domain, but instead is underpinned by subjective values that can be challenged."[444]

From the US viewpoint, the technology and cyber challenges posed by China have both economic and military implications because China has emerged as a peer competitor whose actions threaten to upend the postwar balance of power in Asia. While the United States is at risk of becoming involved in a military conflict with China due to extensive security guarantees for China's neighbors Japan, South Korea, the Philippines, and implicitly also Taiwan, the foundation of US supremacy—its economic and technological superiority—is being challenged by China's aggressive technological development strategy, and, as a result, the military balance has begun to tilt.

European allies tend to be far less concerned with the military risks and more focused on economic security aspects of the challenge. With the publication of Made in China 2025, a strategy for turning China into a global innovation powerhouse within just a decade, Western high-tech producers finally woke up to the challenge posed by an aggressive, state-led growth strategy intent on leapfrogging over developmental stages and harvesting the fruit of innovation at the expense of other players. The effect of this was particularly noticeable in Germany where the industry elite became aware of the risk to German high-tech leadership, realizing that China was about to become Germany's main technological rival.[445] China subsequently dropped public references to this strategy after it became apparent how much irritation it had caused abroad, but its goals were not abandoned. Rather, the silence was a purely tactical move.[446]

Countering infringements on Western technology companies' intellectual property rights is, therefore, a prime concern of European allies to be addressed with China, as is the problem of subsidized (or de facto subsidized) Chinese companies dominating markets worldwide, not just along the BRI, but within Europe itself, while China is not granting reciprocal access to foreign actors within its own market. How far such access will be improved through the CAI remains to be seen. However, a recent report by the European Court of Auditors on Chinese investments in Europe found that "it was difficult to obtain complete and timely data and thus to gain an overview of investments, which are part of the Chinese investment strategy in the EU," noting that "no formalized comprehensive analysis of the risks and opportunities for the EU" could be found. The report recommends to "improve the setting, implementing, monitoring, reporting and evaluation of the EU-China strategy" and "to coordinate the response of the EU institutions and Member States, by promoting the exchange of information."[447]

3. Possible Transatlantic Responses

The United States and its European allies share similar security concerns in terms of ensuring maximum resilience of critical infrastructures against foreign sabotage, and of maintaining the competitiveness of their own national industrial base in the face of Chinese competition.

They also share an interest in curbing Chinese state influence at the highest levels of leadership in international organizations that play a role in setting international technology and cyber standards, ranging from public health organizations such as the World Health Organization (WHO) to bodies like the International Civil Aviation Organization

443 ASPI, *China Defence Universities Tracker,* database, https://unitracker.aspi.org.au.

444 Sam Olsen, "China is winning the war for global tech dominance," *The Hill,* October 4, 2020, https://thehill.com/opinion/technology/518773-china-is-winning-the-war-for-global-tech-dominance.

445 DW, "China emerging as Germany's main economic rival," August 18, 2017, https://www.dw.com/en/china-emerging-as-germanys-main-economic-rival/a-40153468.

446 Max J. Zenglein and Anna Holzmann, *Evolving Made in China 2025: China's industrial policy in the quest for global tech leadership*, MERICS Papers on China No. 8, July 2019, https://merics.org/en/report/evolving-made-china-2025.

447 European Court of Auditors, *The EU's response to China's state-driven investment strategy*, Review No. 03/2020, September 10, 2020, 4-5, https://www.eca.europa.eu/en/Pages/DocItem.aspx?did=54733.

(ICAO), the UN International Telecommunications Union (ITU), the UN Human Rights Council (UNHRC), Interpol, and the World Intellectual Property Organization (WIPO).

a) Replace 'empty negotiations' with meaningful dialogue bolstered by enhanced capacity

Allies need to realize clearly that state-subsidized technological innovation, "digital authoritarianism," and Internet controls are instrumental for China's aims of achieving "national rejuvenation" and are strategic priorities that will not be readily abandoned in the face of international pressure or censure. Accordingly, William C. Hannas and Huey-Meei Chang believe: "Weaning China away from … predatory practices with platitudes about fairness and the respect of the world community, while hoping for the best, is more pipedream than solution." Further, they warn of complacency and point out that Western innovation superiority could prove transitory: "the West fails to appreciate that its storied penchant for breakthrough science matters little without the will, skills, and infrastructure to commercialize its abstract discoveries"—something China is poised to achieve.[448] To this end, China launched its program, China Standards 2035, in 2018, with details still to be published. According to a Federation of German Industries (BDI) analysis, this program is in line with, and effectively a technical upgrade of, Made in China 2025, aiming to enable Chinese industries to shape technical standards in the key industrial sectors identified by Made in China 2025: cybersecurity, autonomous driving, Industry 4.0, and robotics, and also energy. If Chinese industries achieve global leadership in such fields, this would effectively offer China the chance to define future technology standards.[449] Bolstering European and US domestic and joint R&D efforts, not least by vastly increased funding, is, therefore, a necessity if allies aim to strengthen their hand in negotiations with China and to effectively negotiate over standards and practices to make sure that Chinese technical standards will not become the global norm in fields that are projected to have a heavy impact on the future world economy.

b) Provide alternatives for subsidized Chinese technology and bolster allies' technology base

This new awareness might stimulate new initiatives, such as governmental efforts to subsidize or otherwise protect Western technologies that compete with Chinese-subsidized firms, or "framework nation" concepts where more technologically advanced countries can be paired with less capable ones to work through the mechanics of technological independence from China.[450] A Western equivalent might be needed to counter the influence of the Digital Silk Road and BRI Space Information Corridor that could, if unchecked, lead to a Chinese domination of global technology standards, be it in Internet Protocols ("New IP"), blockchain, digital communication, or AI.[451] The new EU Connectivity Strategy could, perhaps, become part of such an allied approach. Subsidizing Western 5G infrastructure solutions and AI development to compete with Chinese subsidized firms might become a necessity. Meanwhile, a joint EU 5G Toolbox of Risk Mitigation Measures that was adopted by the EU in January 2020 seems to have achieved the goal of strengthening and streamlining member states' evaluation processes of 5G network security, illustrating the EU's norm-setting capabilities.[452] And in the fall of 2020, the EU announced a new regulation of trade in dual-use items as an update to its 2009 export control system to address the new challenges.[453] Non-EU NATO members should adopt similar approaches where necessary.

c) Stop illicit military technology transfers

Cases of past dual-use technology transfers that have directly benefitted China's military buildup, and that were mentioned above, illustrate the difficulty of regulating this field. It can be difficult for businesses to understand the security-related implications of individual technologies—not just now, but in future applications. Evaluating the risk of such transfers is, however, an urgent concern. A recent C4ADS report points out that "the burden is on states, companies, and universities engaging with Chinese firms and institutions to proactively

448 William C. Hannas and Huey-Meei Chang, "Chinese Technology Transfer: An Introduction" in William C. Hannas and Didi Kirsten Tatlow, eds., *China's Quest for Foreign Technology: Beyond Espionage* (London: Routledge, 2020), 15.

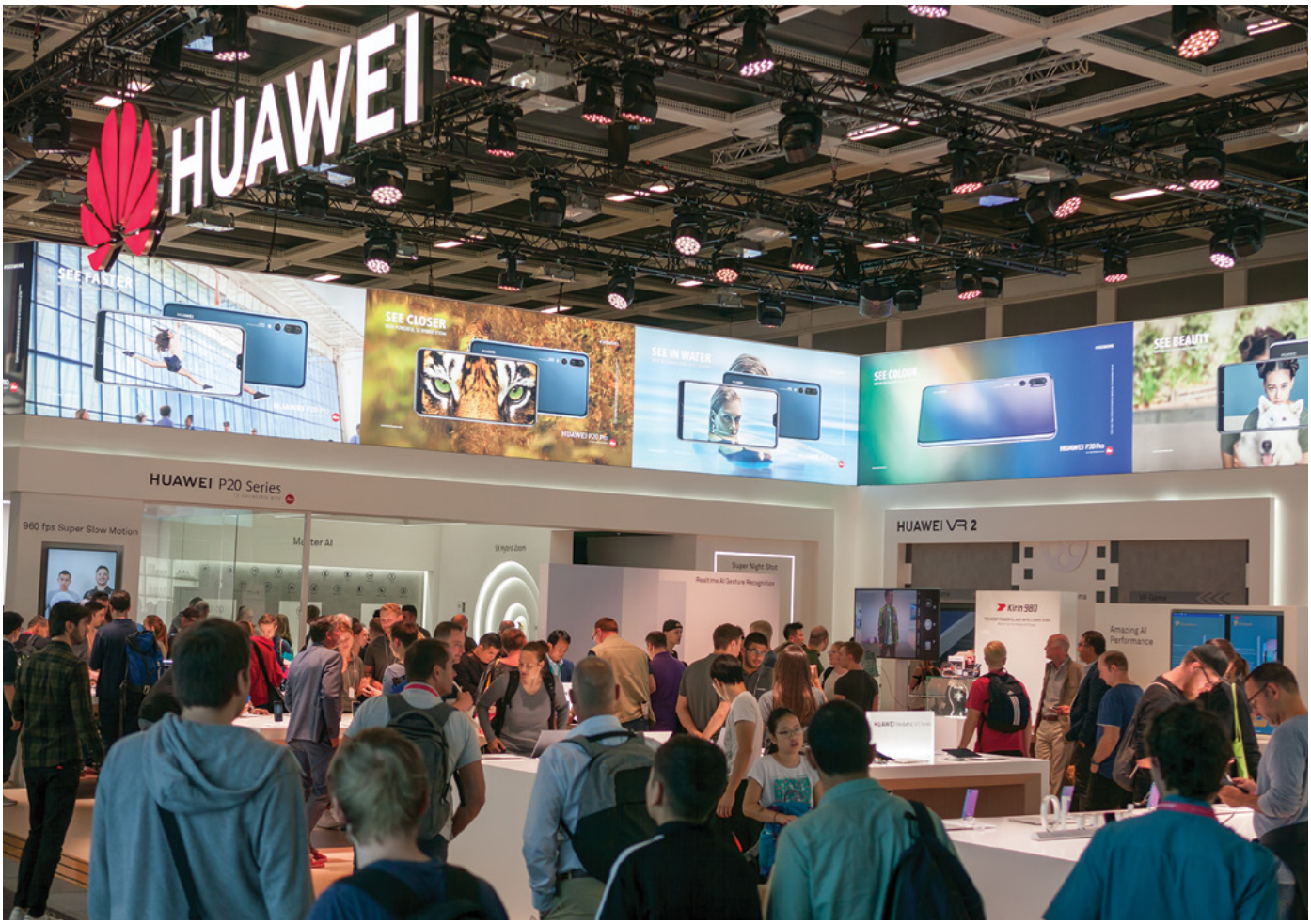
449 Ferdinand Schaff, "Chinese Creative Drive: China Standards 2035," BDI, August 13, 2020, https://english.bdi.eu/article/news/chinese-creative-drive-china-standards-2035/.

450 Hans Binnendijk, Sarah Kirchberger, and Christopher Skaluba, *Capitalizing on transatlantic concerns about China*, Atlantic Council, August 24, 2020, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/capitalizing-on-transatlantic-concerns-about-china/.

451 Olsen, "China is winning."

452 See European Commission, *Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures,* law, January 29, 2020, https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures; for a progress report on the toolbox process, see European Commission, 5G security: Member States report on progress on implementing the EU toolbox and strengthening safety measures, press release by the European Commission and the German Presidency of the Council of the EU, July 24, 2020, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1378.

453 "New rules on trade of dual-use items agreed," Council of the European Union, November 9, 2020, https://www.consilium.europa.eu/en/press/press-releases/2020/11/09/new-rules-on-trade-of-dual-use-items-agreed/; "Commission Delegated Regulation (EU) 2020/1749 of 7 October 2020 amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items," *Official Journal of the European Union* (2020) 63, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2020:421:FULL&from=EN.



Huawei exhibit at the Internationale Funkausstellung 2018, Berlin. *Source:* Wikimedia Commons/Matti Blume (https://creativecommons.org/licenses/by-sa/4.0/deed.en)

prevent misappropriation of their technology."[454] They need better guidance, and allies should find mechanisms for transnational and trans-sectoral cooperation that can increase awareness and help implement better controls. In particular, industry stakeholders should be educated on the scale and magnitude of Chinese industrial espionage and the ways in which CCP-controlled entities typically exercise influence over corporate boards, disguise party-state affiliations of individuals, and hide ties to state-owned enterprises or military-affiliated research facilities. A recent *Foreign Policy* report detailed how Chinese venture capital with connections to government entities is used as a vehicle to gain access to high-technology start-ups in Western countries, particularly in innovation hot spots such as Cambridge in the UK or Silicon Valley in California, in an undisclosed fashion.[455]

Existing monitoring instruments that can help determine the risk of cooperation and transactions, such as the ASPI database on Chinese military research institutions, should be promoted and their use popularized.[456] A recent C4ADS report contains a list of Risk Assessment Indicators (nine primary and five secondary) that point to an individual Chinese entity acting as a vehicle for the illicit transfer of sensitive technologies to China's military which could be used to refine screening mechanisms.[457] The aim should be for such screening mechanisms to enable all stakeholders to use publicly accessible data to understand Chinese technology acquisition strategies and make informed decisions on how to protect themselves and their assets. Allies should discuss and coordinate how relevant information and methods can best be gathered and made publicly available, and

454 Angliviel, Spevack, and Thorne, *Open Arms,* 3.

455 Elisabeth Braw, "How China Is Buying Up the West's High-Tech Sector," *Foreign Policy,* December 3, 2020, https://foreignpolicy.com/2020/12/03/how-china-is-buying-up-the-wests-high-tech-sector/.

456 ASPI, *China Defence*.

457 Angliviel, Spevack, and Thorne, *Open Arms,* 64-66.

how regular exchanges between government and industry stakeholders within and across countries can be facilitated.

Learning processes based on past instances of accidental military technology transfers could be initiated among allies—this should include an honest reckoning of how Western technology has contributed to the Chinese surveillance state system.[458] Allies should dissect past cases and share the lessons learned regarding deceptive strategies employed by Chinese counterparts, such as hiding party-state influence, hiding military affiliations, or obfuscating the end user of a product. Such cases should be publicly exposed and scrutinized. Regular transnational and national-level consultations should be established between military-technological specialists and industry representatives to achieve a common picture of the problem and to give companies more reliable and effective guidance. Better investment screening and monitoring mechanisms for transfers of critical technologies need to be established across Europe and coordinated with the United States to inhibit harmful technology transfers. Likewise, the various arms embargos in place among allies against China should be reviewed and harmonized, and more effective export controls also covering non-lethal military technologies such as sensor systems and propulsion plants that have so far been exempt from the embargo in some countries should be implemented in a transnational approach.[459]

d) Protect critical infrastructure

Though the risk associated with granting Huawei a role in European 5G networks was initially evaluated rather differently among allies,[460] since the COVID-19 pandemic the positions have begun to tilt strongly toward the critical stance promoted by the former Trump administration. Many allied countries have either banned entirely or limited the role of Huawei, with only a few still undecided.[461] On a subnational level, some individual telecommunication companies in undecided countries have preemptively declared their intention to avoid or phase out Huawei technology in their networks.[462] Allies hesitant to ban Huawei technology from their 5G networks should be aware that China's National Security Law of 2015 (Articles 11 and 77) compels all Chinese individuals, organizations, and enterprises to fully cooperate with Chinese authorities on all matters of "national security." This, presumably, includes an obligation to transfer user data.[463] Competitive pricing and supposedly higher quality are not very convincing arguments in Huawei's favor given the vast amount of state subsidies Huawei has received and given that a recent breakdown of a 5G core station conducted in 2020 by the Japanese newspaper *Nikkei* revealed that Huawei still relies on US-supplied technology for nearly 30 percent of the components, while the main semiconductor actually came from Taiwan.[464] National security interests should in any case outweigh pricing considerations, and European 5G champions Nokia and Ericsson should be strengthened to be better able to compete with Huawei in markets outside Europe and efforts to implement "Open Radio Access Networks" which will allow for interoperability and multiple vendors should be supported.

4. Major Recommendations

i. Understanding the complex security implications of technological cooperation with China is a challenge too big for many individual stakeholders to tackle effectively, leading to many loopholes and unintended technology transfers. A concerted effort to educate Western political and industry stakeholders on risks, past failures, and commonly employed Chinese technology transfer practices should be initiated in national and transnational as well as EU and NATO settings.

ii. R&D in strategic sectors should be massively bolstered financially and effective measures should be employed to neutralize the disadvantages encountered by allied industries in competition with Chinese state-subsidized and de facto state-subsidized industries.

iii. A strong US and allied presence in technology standard-setting bodies is needed and has to be coordinated among allies and existing transatlantic differences bridged to effectively counter the Chinese presence in these bodies.

iv. Block technology transfers to China that could further fuel China's military buildup, even indirectly.

458 P.W. Singer and Emerson Brooking, "Here's China's Massive Plan to Retool the Web," *Popular Science*, October 4, 2018, https://www.popsci.com/chinas-massive-plan-to-retool-web/.

459 Noah Barkin, *Export Controls and the US-China Tech War: Policy challenges for Europe*, MERICS China Monitor, March 18, 2020, https://merics.org/en/report/export-controls-and-us-china-tech-war.

460 Duchâtel and Godement, *Europe and 5G*.

461 Frank Umbach, *EU Policies on Huawei and 5G Wireless Networks: Economic-Technological Opportunities vs Cybersecurity Risks*, S. Rajaratnam School of International Studies Singapore, December 23, 2020, 22-31, https://www.rsis.edu.sg/wp-content/uploads/2020/12/WP332.pdf.

462 Katharina Buchholz, "Which Countries Have Banned Huawei?" Statista, January 30, 2020, https://www.statista.com/chart/17528/countries-which-have-banned-huawei-products/.

463 Frank N. Pieke, Katja Drinhausen, and Mareike Ohlberg, *Chinese Telecommunication Companies: Political and legal vulnerabilities and how Europe should deal with them*, MERICS Policy Brief, March 2019, https://merics.org/en/policy-brief/chinese-telecommunication-companies.

464 Umbach, *EU Policies on Huawei*, 8; Yap, "State Support"; Norio Matsumoto and Naoki Watanabe, "Huawei's base station teardown shows dependence on US-made parts," Nikkei Asia, October 12, 2020, https://asia.nikkei.com/Spotlight/Huawei-crackdown/Huawei-s-base-station-teardown-shows-dependence-on-US-made-parts.