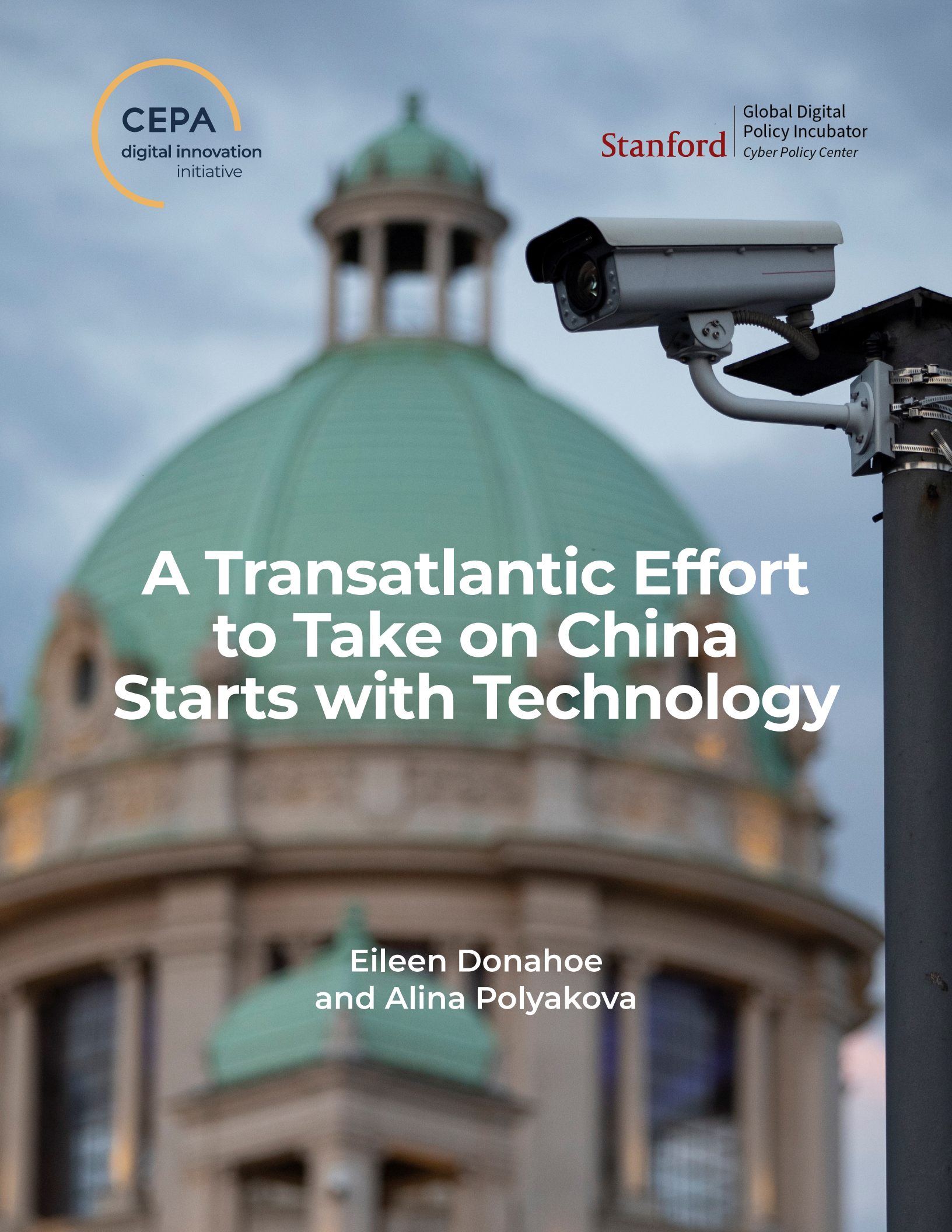


CEPA digital innovation initiative

Stanford | Global Digital Policy Incubator, Cyber Policy Center

A Transatlantic Effort to Take on China Starts with Technology

Eileen Donahoe
and Alina Polyakova

CONTENTS

ABOUT THE AUTHORS

Eileen Donahoe is the Executive Director of the Global Digital Policy Incubator (GDPI) at Stanford University, FSI/Cyber Policy Center.

Dr. Alina Polyakova is the President and Chief Executive Officer of the Center for European Policy Analysis (CEPA).

ABOUT CEPA

The Center for European Policy Analysis (CEPA) is a 501(c)(3), non-profit, non-partisan, public policy research institute. Our mission is transatlantic: to promote an economically vibrant, strategically secure, and politically free Europe with close and enduring ties to the United States. Our analytical team consists of the world's leading experts on Central-East Europe, Russia, and its neighbors. Through cutting-edge research, analysis, and programs we provide fresh insight on energy, security and defense to government officials and agencies; we help transatlantic businesses navigate changing strategic landscapes; and we build networks of future Atlanticist leaders.

This report is part of CEPA's Digital Innovation Initiative, which receives generous support from Craig Newmark Philanthropies.

Cover: A surveillance camera is seen in front of the Serbian Parliament building in Belgrade, Serbia, August 12, 2020. REUTERS/Marko Djurica.

Technology is now the epicenter of geopolitics: governments increasingly recognize that all aspects of their power — military, economic, and normative — derive in substantial part from dominance in technology. The Covid-19 pandemic has only heightened awareness of the geopolitical dimensions of technology and the inherent vulnerability of technological interdependence as supply chain fragility and demand for digital services have become more visible. In recognizing vulnerabilities, however, democracies must resist the impulse to put up digital "walled gardens." Instead of a race to the bottom, where every nation rushes to achieve technological sovereignty, democracies must develop a shared strategic approach that reflects values of openness, drives innovation, and establishes a legal framework for digital governance that prioritizes fundamental human rights.

The transatlantic alliance should be the driver of a 21st-century democratic digital agenda. But disagreements over government surveillance, private sector data collection and sharing, platform content restrictions, digital competition, and protection of fundamental freedoms like privacy and free expression, mean that Europe and the United States find themselves increasingly at odds.

The central paradox is that while the U.S. private sector has continued to dominate in size and innovation, the U.S. government has lagged in the policy realm. Conversely, the European Union (EU) has made significant efforts to establish regulatory guidelines for (mostly U.S.) tech companies operating in Europe, but few European companies are global champions. Overly proactive European regulators risk hampering innovation on both sides of the Atlantic, while a sometimes-haphazard approach to tech policy leaves the United States out of the global regulatory conversation. These uncoordinated or even clashing approaches leave tech companies

of all kinds in an increasingly ambiguous regulatory environment and weaken democratic norms worldwide.

The winner is China. The Chinese Communist Party's (CCP's) direct support for its tech industry has created a global innovation powerhouse and a competing model of digital governance. In place of democratic norms and principles of transparency, accountability, privacy, and free expression are the state's interests in censorship, intimidation, and surveillance. China has embraced a strategy of "civil and military technology fusion" through which the authoritarian regime can control all economic sectors (government, business, and academia) but also create spillover economic benefits.[1]

A decades-long campaign to filter information and exploit new technologies for the state's benefit has attracted followers abroad. China has built a global export market for products and services that also happens to serve the CCP's other goals, notably the potential to collect personal information on foreign citizens. Decision-makers in Beijing understand that technological dominance brings greater control over global standards and norms, notably in tech standard-setting bodies. The "Global Initiative on Data Security"[2] and the "China Standards 2035" initiative[3], both launched in 2020, reflect Beijing's intention to embed the regime's values into future technologies. China's vision of cyber sovereignty, which rejects external scrutiny of its human rights record and presumes state control over private data, is also gaining traction globally.

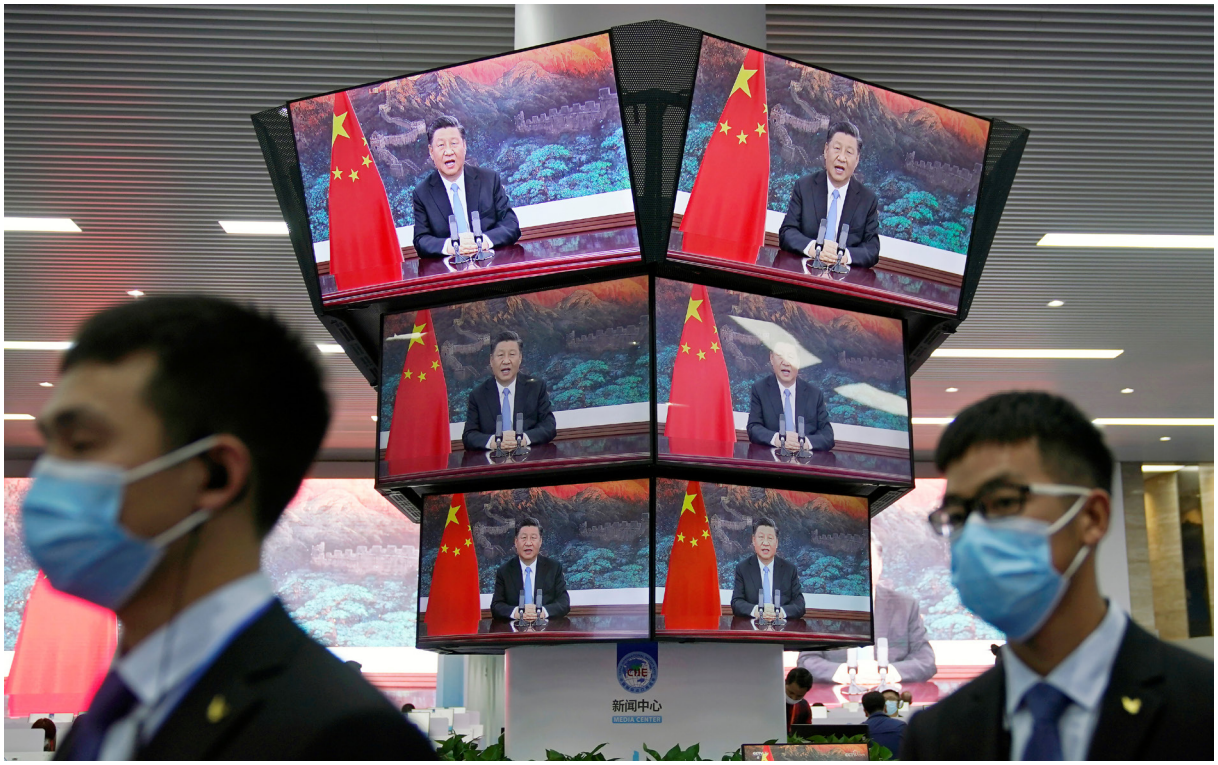
This is a geopolitical contest, playing out in the digital domain. China increasingly seeks to write and spread global rules of the road that support a digital governance model of ubiquitous, intrusive authoritarianism, data localization, and cyber sovereignty. Its target is the, already shrinking, U.S.-led vision of an open, interoperable, global internet embedded with democratic values. The window for democracies to act is closing and the stakes could not be higher.

Europe and the United States should reconcile their divisions and combine their strengths in normative leadership and innovation to craft a coherent digital agenda. Good governance combined with technological prowess will attract support from other governments seeking a positive model for the future digital society. The central point is that democratic norms should facilitate, or at least not undermine, innovation, and those same norms should strengthen the ability of democracies to compete, rather than stymie it. Protectionism, backed by discriminatory legislation, spells defeat on two fronts: it hampers competitiveness and stokes political division. Decision-makers should remember that regulation is not a goal in itself. It is the means to an end: technological innovation that reflects and promotes democratic values. Innovation must drive the regulatory agenda, not the other way around.

In this paper, we sketch out the differences between the Chinese, EU, and U.S. digital agendas and lay out a road map for a shared transatlantic approach.

China's Digital Agenda

China's digital authoritarian model is ambitious. The CCP's commitment to technological dominance is manifest in its long-term investment strategy. Artificial intelligence (AI) is a focal point because it enables innovation and supremacy in so many other fields. In 2019, China made clear its desire to be the world's leading AI superpower by 2030,[4] with a rough plan to have caught up with the United States by 2020, to surpass the United States by 2025, and to dominate globally in AI industries by 2030.[5] The immensity of the regime's investment in other emerging technologies is staggering, with no less than 16 different "Manhattan Project"-scale initiatives in fields as varied as quantum computing,



China's President Xi Jinping is seen on screens in the media center as he speaks at the opening ceremony of the third China International Import Expo (CIIE) in Shanghai, China November 4, 2020. Credit: REUTERS/Aly Song.

cryptography, 5G, facial recognition, and genomics.[6]

China has experimented with and deployed ground-breaking repressive digital technology, most notably against the Uighur minority in Xinjiang. An unprecedented system of mass surveillance monitors the movement of people, phones, and vehicles to detect behavior that merits investigation or detention. This techno-totalitarian system is being extended to other parts of China as well as exported across the world.

Countries as varied as Zimbabwe, Uzbekistan, Pakistan, Kenya, and the United Arab Emirates have bought Chinese surveillance technology.[7] Many others have received training in topics like proactive censorship, or "public opinion guidance." China also exports digital information infrastructure, such as Huawei's 5G telecommunications systems, under the guise of the Belt and Road Initiative (BRI). These deals create long-term leverage. Even nominally private Chinese companies are obligated by law to provide unquestioning, immediate, and confidential support to the country's intelligence and security agencies. As U.S. Sen. Mark Warner (D-VA) noted, "any supposedly safe Chinese product is one firmware update away from being an insecure Chinese product."[8]

On the diplomatic front, China has made huge efforts to dominate multilateral bodies and agendas in pursuit of regulatory and normative dominance.[9] Chinese nationals now lead four of the 16 U.N. agencies, including the International Telecommunications Union (ITU), the United Nations Industrial Development Organization (UNIDO), the International

Civil Aviation Organization (ICAO), and the Food and Agriculture Organization (FAO). In its latest push to coopt multilateral institutions, China has led an effort, together with Russia and Saudi Arabia, to place a more pliant head of the U.N. Human Rights Council (UNHRC) and undermine the consensus candidate favored by democracies.[10]

China recognized very early that it could have significant influence if it sought out leadership roles at tech standard-setting bodies. It adopted an aggressive strategy to push for first-mover advantage for its protocols that can provide a powerful edge to its businesses and sway the global tech community to adopt its protocols for emerging technologies.[11] Furthermore, China recently secured a commitment from 14 other countries in the Regional Comprehensive Economic Partnership (RCEP) trade agreement not to challenge its Great Firewall and other digital restrictions. The RCEP is the largest trade pact in world. It cements China's central role in global supply chains, particularly in high tech. By flexing its economic muscles to gain international political influence, China is winning the global narrative battle about cyber sovereignty and the advantages of its techno-authoritarian model of governance over the U.S.-led democratic one. This brings not only political benefits but significant long-term advantages to Chinese tech firms.

China has even succeeded in normative realms like the UNHRC, where a Chinese representative gained a seat on the influential Consultative Group, which oversees the selection of candidates for U.N. human rights expert roles.[12] As the United States has withdrawn from the UNHRC and the EU has been preoccupied with its own problems, China was able to convince the majority of delegations at the council to support declarations that its use of technology in both Xinjiang and Hong Kong are consistent with human rights principles.[13] In his speech to the 2020 U.N. General Assembly meeting, Chinese President Xi Jinping positioned China as a responsible stakeholder in the international system, while criticizing "major countries" for not doing enough to contribute — a critique long directed by the United States against China. Xi also announced that China will set up a "U.N. Global Geospatial Knowledge and Innovation Center" and an "International Research Center of Big Data for Sustainable Development Goals" as part of the U.N.'s 2030 Agenda for Sustainable Development,[14] positioning China as a hub for international collaboration on technology.

Europe's Digital Decade?

While China invests in its technological future, Europe has, self-admittedly, lagged behind in preparing for a digital present. To move European tech innovation forward, the EU set forth an ambitious agenda to catch up and make the 2020s "Europe's digital decade." European Commission (EC) President Ursula von der Leyen called on Europe "to lead the way on digital — or face having to follow the way of others, who are setting these standards for us." Indeed, von der Leyen's EC has made tech policy its top priority on par with climate change.[15]

But Europe already finds itself in the middle of a potential "tech cold war"[16] between the United States and China, as the two countries increasingly dominate the market for digital technologies.[17] The pandemic starkly highlighted Europe's dependence on technologies from the United States and China. In particular, exposure of supply chains' fragility and the rapid move toward cloud and online conferencing platforms underscored the shortage of homegrown competitors and left many Europeans feeling at the mercy of foreign countries and companies.

The instinct to become walled-off digital garden nations makes it difficult, if not impossible, for democracies to jointly counter competition from authoritarian states.

No digital silver bullet

Calls for Europe to have "mastery and ownership of key technologies," as President von der Leyen put it, have heightened with the duration of the pandemic. "Digital sovereignty" is a cornerstone of the EU's vision to be able to "act independently in the digital world."[18] While the meaning of digital sovereignty in the EU context remains murky, in practice it encompasses at least the following:

- Strengthening Europeans' control over personal data, often through data localization efforts;
- Reducing Europeans' dependence on foreign technology, particularly in critical areas; and
- Increasing European industry's competitiveness in digital technologies.

There are several issues with the digital sovereignty model. First, the interests of individuals and states differ. While sovereignty at the level of the individual or user can enable digital privacy, security, and autonomy, sovereignty at the national or state level can be an impediment to autonomy and democratic self-governance. Nor does the concept distinguish between tech companies that are state-owned or controlled (such as Huawei) and genuinely private firms – de facto treating U.S. and Chinese tech companies as equals. EU Commissioner Thierry Breton referred to digital sovereignty as a response to "the 'technological war' being waged by the United States and China."[19]

Second, moving toward a digital sovereignty model would legitimize Chinese and Russian efforts at establishing a "splinternet" vision of the digital domain, thus setting a precedent for increasing digital fragmentation. It also distances the EU from the transatlantic alliance, entrenching a position of moral equivalence. This may be a sound approach from the lens of pure market competition, but it overlooks national security concerns.

Lastly, despite the affirmation (especially made by German Chancellor Angela Merkel) that digital sovereignty is not about protectionism and that it would take into account global interdependencies, some policymakers see digital sovereignty as an argument for introducing protectionist measures.[20] At the same time, 20 percent of the EU's Covid-19 recovery funds are earmarked for national-level digital transformation efforts, which will serve the digital sovereignty model.[21] As with many industrial policy frameworks, the desire to increase European firms' competitiveness may in fact merely help inefficient firms. The instinct to become walled-off digital garden nations makes it difficult, if not impossible, for democracies to jointly counter competition from authoritarian states.

An ambitious regulatory agenda

The Digital Services Act (DSA) and Digital Markets Act (DMA) seek to update Europe's framework for digital services, which is currently governed by legislation passed in 2000.[22] While the details of the DSA were not public at the time of writing, European regulators have hinted at some of its content. The DSA will put increasing pressure on large online platforms, which the EC has categorized as "gatekeepers," including enforcement mechanisms around illegal or harmful content. It is presumed that most gatekeeper firms are U.S. companies, such as Apple, Amazon, Facebook, Google, and others, that the

EU sees as stifling competition for digital services in Europe. The goal of the DSA is to increase consumer trust and safety online by increasing the liabilities and obligations of platforms. Critics of this approach are concerned that a more restrictive approach to online content would not only require greater resources (resources that not all companies necessarily have) but would also inevitably lead to illegal content moving to smaller less visible platforms that would escape the gatekeeper label.[23]

The DMA focuses on *ex ante* regulation, anticipating future public harm, rather than regulating to mitigate an existing harm. Such moves would blacklist a broad range of business practices, regardless of whether they affect consumer welfare positively or negatively. A proposed "new competition tool" would increase the EC's ability to take aggressive antitrust enforcement action in a manner inconsistent with U.S. and global competition norms. Both the regulations and the tool appear to lack a firm evidentiary basis. Commission officials say that the legislation will likely focus primarily on U.S., not Chinese or European, platforms.[24]

These regulatory efforts have stirred three controversies: rule-of-law concerns about government pressure to remove harmful but legal online content, questionable EU motivations for focusing regulation primarily on U.S. companies, and lack of a strategy for curbing Chinese incursions. Legal pressure on companies to take down harmful, but not illegal, content is particularly sensitive. Germany's NetzDG law, France's "Avia Law," (much of which has since been struck down),[25] and the United Kingdom's "Online Harms White Paper" all impede coherent transatlantic policy. Worse, well-intentioned regulatory efforts can legitimize the enlistment of the private sector in censorship. Not surprisingly, Russia passed a copy-and-paste version of Germany's NetzDG law imposing liability on platforms for user-generated unlawful content, knowing it would serve its aim to repress free expression and enlist the private sector in censoring speech.

The U.S. Digital Agenda — A Coherence Deficit

While the U.S. scientific and technological foundation for tech dominance is still solid, its primacy in technology is no longer unassailable. China already leads the world in:

- quantum communications;
- 5G;
- facial recognition software;
- e-commerce and mobile payments (with 700 million internet users);
- electric vehicles;
- clean power technology (wind and solar); and
- high-speed rail.

China also has the world's largest database of genetic engineering data.

On the near horizon, China is challenging U.S. technology leads in AI, genetic engineering, quantum computing, and quantum sensors.[26] The Pentagon's new Defense Innovation Unit (DIU) aims to accelerate adoption of commercial technology by the military and include companies with cutting-edge technology in the military supply chain. Yet, decades of underinvestment have taken their toll. The United States has let its federally funded R&D drop to 0.7% of GDP, down from 2% at the height of the Cold War.[27]

Missing in action on policy

As home to many of the world's largest tech companies, the United States should be leading the international discussion on setting the norms for a free and open digital domain. Instead, it has remained on the sidelines. While several states have enacted privacy protection measures, such as the California Consumer Privacy Act, the federal government has been slow to act and a gridlocked Congress has been unable to pass any meaningful tech legislation.

The most significant digital regulatory moves involve competition concerns. In October 2020, the federal government filed suit against Google for anticompetitive practices, alleging that the company had illegally installed its search engine service on Apple's iPhone operating systems, and removed the ability for the search engine to be uninstalled on its own Android operating system. Similar lawsuits by state authorities are expected to follow. Facebook remains under federal government investigation for its purchases of Instagram and WhatsApp.[28] Pursuit of antitrust cases against large tech firms has garnered rare bipartisan support. The Google suit was filed by the Republican Trump administration but cheered by Democratic members of Congress. A Democratic-led committee in the U.S. House of Representatives has also released its own recommendations for more aggressive antitrust action.[29] (In Europe, by contrast, regulatory proposals aim not to increase competition for the consumer's benefit, but to spur the growth of European champions by limiting their U.S. competitors.)

In the United States, like analogous European laws, Section 230 of the Communications Decency Act exempts internet services from liability for content posted by users on their platforms. It has drawn critical attention from U.S. politicians on both sides of the aisle, including the two major U.S. presidential candidates in 2020, but for contradictory reasons: Republicans have threatened its revocation as retaliation for perceived anti-conservative political bias, while Democrats want to amend it for its perceived failure to combat disinformation and other harmful content. Many would agree that additional measures (regulatory or voluntary) are now needed to update this legislation, which dates from 1996. Almost two dozen legislative reforms have been proposed so far, ranging from revocation of Section 230 to allowing platforms to earn immunity through removal of disinformation or other forms of harmful content. The Federal Communications Commission (FCC) has signaled that it may review Section 230, but these proposals are likely to be rethought by the Biden administration and the new Congress. A key concern is to avoid unintended damage to core principles of online freedoms.[30]

The Rift

The EU and the United States thus find themselves on different trajectories.[31] It is time to change course. While the EU has carved out a critical role in global tech policy development, innovation rather than regulation should drive Europe's future tech policy. Building a burgeoning and competitive marketplace for digital technologies should be the top priority. The U.S. experience in engendering innovation will be instructive.

For its part, the United States should take a leading role in influencing global technology policy developments that reflect democratic values and provide clear rules of the road for industry. The leadership vacuum created by its absence means that global advocacy for an open, democratic approach to technology policy is waning, while the authoritarian agenda of control through technology advances.

A transatlantic digital technology strategy would combine innovation and competitiveness with democratic norms. If

European Executive Vice-President Margrethe Vestager and European Commissioner for Internal Market and Services Thierry Breton (not seen) give a news conference on the Data Governance Act at the European Commission in Brussels, Belgium November 25, 2020. Credit: Stephanie Lecocq/ Pool via REUTERS.

Europe aims to lead on digital regulation, it must work with, rather than against, the leader in digital innovation: the United States. A jointly crafted digital agenda will attract wide international support, competing with China on both the technological and normative fronts. The new EU-U.S. agenda for global change, announced in early December 2020, introduces a constructive set of ideas on transatlantic cooperation on technology and is a significant step in the right direction.[32]

A long agenda on tech cooperation

The immediate priority is to avoid collision looming on at least three fronts. **First is data governance,** which includes challenges around personal data privacy as well as cross-border data sharing. Despite general agreement that protection of private and personal data must be a core part of digital policy, there is disagreement on how to provide user control, and how to regulate the use of large data sets essential for AI development. The desire to protect individual user data has often been at odds with the broader need to allow free data flows between the United States and Europe.

In July 2020, the Court of Justice of the European Union (CJEU) found that the EU-U.S. Privacy Shield, which allowed for data sharing between the United States and Europe, is invalid under the EU Charter of Fundamental Rights. This ruling honed in on U.S. intelligence practices while failing to recognize that a number of EU member states employ broadly similar surveillance regimes. Ironically, a key factor in this ruling was inadequate protection for EU

citizens from U.S. government surveillance, even as European governments seek more access to citizens' data from private companies. In 2020, the Privacy Shield facilitated $7.1 trillion in trade and was used by thousands of companies on both sides of the Atlantic.[33] Without it, digital trade will be significantly diminished, with profound implications for research and development of AI and cloud computing technologies. Companies subject to enforcement actions have argued that they will not be able to serve users in the EU if the ruling is enforced, and numerous trade associations have challenged the ruling.[34] This leaves the debate on data sharing in uncharted territory, as the solution may require changes in U.S. government surveillance law and policy.

The second front for potential collision relates to monopoly power and tech competition. While both European governments and the United States have pushed forward antitrust investigations, legislation, and legal cases, the motivation driving these efforts is starkly different. In Europe, the biggest factor limiting the scale of technology development (and one reason why U.S. companies have gained market share) is the failure to complete the Digital Single Market. While some initiatives, such as the cloud computing effort GAIA-X, aim to establish a sovereign European data infrastructure, the nationally splintered marketplace undermines Europe's potential collective leverage. Unfortunately, initiatives such as GAIA-X appear to be designed first and foremost to push back against U.S. (and Chinese) tech companies' market dominance in cloud computing, and only secondarily to promote market harmonization. By contrast, in the United States, concerns over competition have less to do with concerns over non-U.S. firms and more to do with the lack of transparency around data collection and unfair market practices. These issues can likely be better addressed with more targeted regulatory efforts rather than broad antitrust legislation.

What is often missing in both Europe and the United States is a broader geopolitical vision of how significantly constraining large U.S. tech firms could benefit their Chinese competitors. Any antitrust legislation or legal action must be paired with an assessment of how such market changes might allow China greater market dominance. Such a strategic approach would also assess potential economies of scale from combining U.S. and European data and markets.

The third front is the regulation of online content. While there is general agreement that illegal content, such as child pornography, should not appear on digital platforms, there is no consensus on what constitutes harmful content. European countries tend to have an expansive view of harmful content that can be subject to legal adjudication. The United States, by contrast, has far more expansive protections for free speech — hate speech, for example, is protected speech in the United States but not in most European states. But even in Europe, any policy actions that aim to regulate online speech will likely be contested in court, and some laws aimed at curtailing online hate speech have already been found not to pass muster. The French "Avia law," for example, was struck down by a French high court in June 2020 as a violation of freedom of expression. France's Constitutional Council determined that the law was "not necessary, appropriate and proportionate."[35]

Establishing a common glossary of terms for harmful content and a shared understanding of whether such content should be the subject of regulation, legal adjudication, or user-prompted removal by platforms is a long-overdue first step. But a series of national-level laws paired with broader European initiatives leaves the future of a shared approach to harmful content regulation ambiguous.

Overcoming the Transatlantic Tech Policy Divide

The United States and the EU should develop a shared strategic vision for innovation and governance of digital society and a joint plan of action to address the threat posed by China's growing techno-authoritarian influence. Rather than deepening the transatlantic rift, they should focus on shaping a wider global democratic agenda. Such an agenda could involve elements of a "digital trade zone,"[36] a "technology alliance,"[37] a "world data organization,"[38] or a more informal forum for policy development among "techno-democracies."[39] The EU's proposal to launch a joint EU-U.S. tech agenda calls on the transatlantic partners to "join forces as tech-allies to shape technologies, their use and their regulatory environment" based on "shared values of human dignity, individual rights and democratic principles."[40] This is an important entreaty that the new U.S. administration should seriously consider. The EU, for its part, should solicit U.S. input on broad regulatory packages, such as the DSA and DMA, prior to implementation.

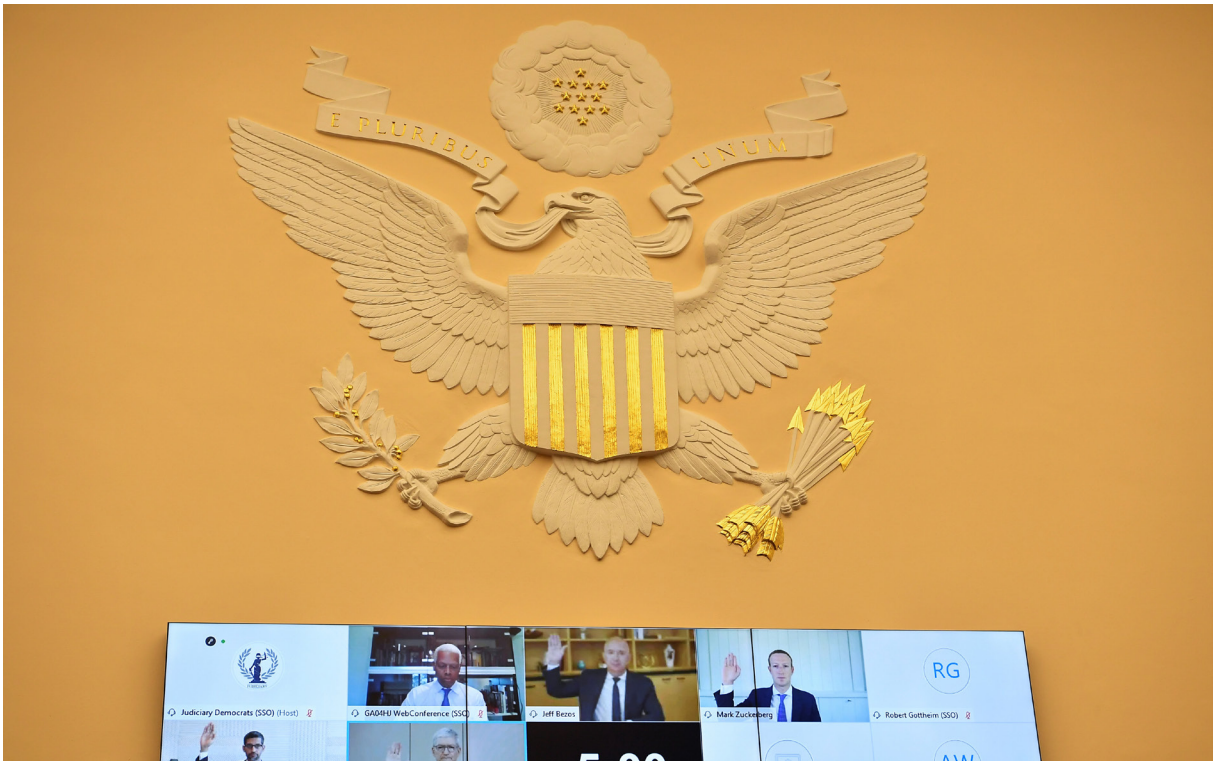
Practical progress must begin in three core areas. As a first step, concrete mechanisms for U.S.-EU cooperation focused on innovation with a primary focus on emerging technologies must be established. Second, a joint action plan must articulate a shared democratic approach to governance of digital society consistent with universal human rights principles. Third, transatlantic partners must develop a coordinated strategy to combat the rise of digital authoritarianism with an emphasis on reenergizing international diplomacy. To these ends, Europe and the United States should:

Develop a joint strategic approach to critical and emerging technologies

An essential responsibility of democratic governments seeking to protect their innovative capacity is to lead in the development of emerging technologies and protect supply chains for critical technologies, such as 5G and microprocessors. The varying approaches to Chinese firms like Huawei exemplify the lack of coordination within Europe and between Europe and the United States. European-level initiatives to limit foreign firms' market dominance in the tech sector have mostly placed U.S. and Chinese firms in the same category, or worse, depicted the United States as the greater threat. Private companies from democratic states deserve to be evaluated differently from authoritarian state-owned or state-influenced companies.

Recommendations:

- The United States and Europe must commit to leading the world in new technologies, including AI, quantum computing, Internet of Things (IoT), bioengineering, and semiconductors.[41] A shared strategic approach to critical technologies should include increased investment in emerging tech research and development. Governments should work with the private sector and research institutions to channel resources toward joint efforts aimed at jumpstarting and sustaining commitments to innovation. The United States and Europe should establish a network of joint "Centers of Excellence" based in major tech centers on both continents and funded through public-private partnerships to serve as collaboration and coordination centers where European and U.S. researchers, engineers, and public servants could learn from each other and take on joint research projects.



Witnesses Amazon CEO Jeff Bezos, Facebook CEO Mark Zuckerberg, Google CEO Sundar Pichai, and Apple CEO Tim Cook are sworn-in before a hearing of the House Judiciary Subcommittee on Antitrust, Commercial and Administrative Law on «Online Platforms and Market Power», in the Rayburn House office Building on Capitol Hill, in Washington, U.S., July 29, 2020. Credit: Mandel Ngan/Pool via REUTERS.

- Europe and the United States should establish a joint funding mechanism to identify gaps in research and development. The mechanism should be open to all democracies to join with contribution levels based on countries' GDP. A "Transatlantic AI Agreement," as proposed by the EU, could be the foundation for establishing such a joint funding mechanism. The European AI Fund is a nongovernmental initiative and a step in the right direction, but governments, particularly European governments, must overcome secondary political concerns to significantly increase their investment in emerging technologies. Previous successful efforts, such as the Manhattan Project and the U.S. Moonshot, which formed closer relationships between public funding and innovation, could serve as models. This format would allow the United States and Europe to combine forces on essential technologies where they do not want China to gain a foothold. The joint EU-U.S. fund could:
  - Identify market niches/gaps that European "champions" can enter to more effectively leverage the strengths of EU firms;
  - Encourage a bottom-up approach — investment should focus on removing barriers to entry for tech startups, attracting private venture capitalists, building closer relationships between federal funding and innovation (and in Europe's case, commercialization); and

  - Build relationships of trust and reliable information sharing between European and U.S. tech sectors as well as governments.
- The EU should delineate a more precise mandate for its newly established foreign investment screening mechanism, which came into force in October 2020, to focus on issues related to Chinese investment. The mechanism establishes a coordination function between EU member states and the EC, but it lacks the mandate of the Committee on Foreign Investment in the United States (CFIUS) to deny certain investments due to national security concerns. EU and U.S. agencies should work closely together to assess the risks posed by specific Chinese and other state-controlled entities.
- The United States should take up the EU proposal to establish an "EU-U.S. Trade and Technology Council (TTC)" in order to have a platform for discussion, honing regulation, and avoiding digital regulatory divergence.

Develop and articulate a shared democratic approach to governance of digital society

Democratic governments embrace a fundamental obligation to protect the liberty and security of their citizens. But in a connected, digitized society, new security vulnerabilities have arisen, leaving democratic governments struggling to balance security and freedom, and arguing with each other about trade-offs between fundamental rights in tension with each other. As a result, confidence in the feasibility of adhering to human rights' principles in the digital realm has eroded. Authoritarian governments gladly reinforce this narrative.

Recommendations:

- Individual countries should get their own houses in order, particularly when it comes to their collection and use of data; their application of technology, especially for surveillance or government decision-making; as well as their approach to technology regulation. When democratic governments fall short, it is hard to criticize authoritarians for violations of fundamental rights.
- National policies do not need to be homogeneous, but they must be harmonious. Europe and the United States must start by finding a shared solution for cross-border data transfers that protects both sharing and privacy. Failure to do this reinforces "data protectionism."
- A new democratic digital coalition could coordinate and reconcile norms for digital technologies, along with a dramatic boost of investment and high-level government engagement in the existing Freedom Online Coalition (FOC). Both the FOC and the new forum would benefit from greater engagement from civil society and the private sector. The coalition should address norms on the use of data and technology for governance purposes, the responsibility of tech companies to protect the democracies in which they operate, and the development of private sector transparency and accountability, including human rights impact assessments.

Develop a coordinated strategy to counter the rise of digital authoritarianism with an emphasis on international diplomacy

- In addition to leading in technology innovation and development of democratic norms for digital society,

democracies must combat the growing threat of digital authoritarian influence around the globe. Such malign influence is manifest in a wide variety of arenas, ranging from tech standard-setting bodies such as the ITU, to international normative arenas, such as the UNHRC. Bilateral trade and infrastructure investment agreements often serve as vehicles for gaining tremendous long-term leverage. Democracies must develop a robust plan of action to help other democratically inclined nations resist these entreaties and ward off illiberal influences on their societies.

Recommendations:

- The United States and the EU should coordinate on outreach to potential democratic allies, centering on principled resistance to China's export of digital information infrastructure. Rather than simply pressuring allies, the United States and the EU must explain the security risks of reliance on Chinese infrastructure.[42] Other goals include a stronger cyber nonproliferation regime and more effective export controls on repressive technologies.
- The United States should leverage the combined power of coalitions of democracies in multilateral institutions to push back against China's encroaching influence. China has not won, yet. Many countries share concerns over Chinese intellectual property theft. The United States harnessed such concerns to sway support away from the Chinese-favored candidate for leadership of the World Intellectual Property Rights Organization (WIPO).[43] In much of the world, U.S. norms-based leadership is preferred over China's heavy-handed lobbying.
- The United States and Europe should prioritize tech innovation as part of international development efforts. Agencies such as the U.S. Agency for International Development (USAID) and the EU's Directorate-General for International Cooperation and Development (DG DEVCO) should establish a joint program aimed at empowering and providing funding to tech entrepreneurs in the Global South, and especially in countries where China has made significant investments.
- The United States and Europe should prioritize support for independent media in countries around the world where China is actively working to co-opt and influence the narrative. U.S. and European governments should, especially, work together to support local-language independent media efforts in Taiwan and Hong Kong to undermine the CCP's efforts to exert control over these regions.

Conclusion

Healing the rift on digital policy between Europe and the United States must be a top a priority for governments on both sides of the Atlantic. A democratic digital domain is an asset that democracies must not only protect but also invest in strategically. More than that, the digital agenda should be a core part of the underpinnings of the transatlantic alliance, on par with collective defense and democratic values. On both sides of the Atlantic, there will be objections to this proposal. Tech companies reject European meddling; European politicians dislike U.S. digital hegemony; and U.S. policymakers often resent excessive regulation. But the result of this disagreement is something all parties will like even less: a Chinese-led global digital governance model. Delay and division are luxuries. They spell defeat.

Endnotes

1 Michael Brown, Eric Chewning, and Pavneet Singh, "Preparing the United States for the Superpower Marathon with China," Brookings Institution, April, 2020, p.4.https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_superpower_marathon_brown_chewning_singh.pdf

2 Shannon Tiezzi, "China's Bid to Write the Global Rules on Data Security," The Diplomat, Sep. 10, 2020, https://thediplomat.com/2020/09/chinas-bid-to-write-the-global-rules-on-data-security/

3 Arjun Kharpal, "Power is 'up for grabs': Behind China's plan to shape the future of next-generation tech," CNBC, Apr. 26, 2020, https://www.cnbc.com/2020/04/27/china-standards-2035-explained.html

4 Yasim Tadjdeh, "China Threatens U.S. Primacy in Artificial Intelligence," National Defense Magazine, Oct. 30, 2020. https://www.nationaldefensemagazine.org/articles/2020/10/30/china-threatens-us-primacy-in-artificial-intelligence

5 Peter Diamandis, "China Is Quickly Becoming an AI Superpower," Singularity Hub, Aug. 29, 2018. https://singularityhub.com/2018/08/29/china-ai-superpower/

6 Tai Ming Cheung et al., "Planning for Innovation: Understanding China's Plans for Technological, Energy, Industrial, and Defense Development," U.S.-China Economic and Security Review Commission, July 28, 2016. https://www.uscc.gov/sites/default/files/Research/Planning%20for%20Innovation%20-%20Understanding%20China's%20Plans%20for%20Tech%20Energy%20Industrial%20and%20Defense%20Development072816.pdf; and Brown, Chewning, and Singh, "Preparing the United States for the Superpower Marathon with China."

7 Steven Feldstein, "The Global Expansion of AI Surveillance," Carnegie Endowment for International Peace, Sept. 17, 2019. https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

8 Madeleine Albright, Mark Warner, and Derek Mitchell, "Democracy, Technology & China: U.S. Strategy for Innovation in the 21st Century," National Democratic Institute, Sept. 16, 2020. https://www.ndi.org/democracy-technology-china-us-strategy-innovation-21st-century

9 Tung Cheng-Chia and Alan Yang, "How China is Remaking the UN in Its Own Image," The Diplomat, Apr. 9, 2020. https://thediplomat.com/2020/04/how-china-is-remaking-the-un-in-its-own-image/; Yaroslav Trofimov, Drew Hinshaw, and Kate O'Keeffe, "How China Is Taking Over International Organizations, One Vote at a Time," The Wall Street Journal, Sept. 29, 2020. https://www.wsj.com/articles/how-china-is-taking-over-international-organizations-one-vote-at-a-time-11601397208

10 Nick Cumming-Bruce, "Leadership of UN Human Rights Body Becomes Proxy Battle for World Powers," The New York Times, Nov. 29, 2020. https://www.nytimes.com/2020/11/29/world/un-human-rights.html

11 Alan Beattie, "Technology: How the US, EU and China Compete to Set Industry Standards," Financial Times, July 24, 2019, https://www.ft.com/content/0c91b884-92bb-11e9-aea1-2b1d33ac3271

12 Eleanor Albert, "China Appointed to Influential UN Human Rights Council Panel," The Diplomat, Apr. 9, 2020, https://thediplomat.com/2020/04/china-appointed-to-influential-un-human-rights-council-panel/

13 Roie Yellinek and Elizabeth Chen, "The 22 vs. 50 Diplomatic Split Between the West and China Over Xinjiang and Human Rights," The Jamestown Foundation, Dec. 31, 2019, https://jamestown.org/program/the-22-vs-50-diplomatic-split-between-the-west-and-china-over-xinjiang-and-human-rights/; Joyce Huang, "UN Human Rights Council Divided Over China's Xinjiang Policies," Voice of America, July 17, 2019, https://www.voanews.com/east-asia-pacific/un-human-rights-council-divided-over-chinas-xinjiang-policies#; and Dave Lawler, "The 53 countries supporting China's crackdown on Hong Kong," Axios, July 3, 2020, https://www.axios.com/countries-supporting-china-hong-kong-law-0ec9bc6c-3aeb-4af0-8031-aa0f01a46a7c.html

14 Xi Jinping, "Speech at the General Debate of the 75th session of the United Nations General Assembly," China Global Television Network, Sept. 23, 2020, https://news.cgtn.com/news/2020-09-23/Full-text-Xi-Jinping-s-speech-at-General-Debate-of-UNGA-U07X2dn8Ag/index.html

15 Ursula von der Leyen, "Speech in the European Parliament Plenary Session," European Union, Nov. 27, 2019, https://ec.europa.eu/info/sites/info/files/president-elect-speech-original_en.pdf; and Tyson Barker, "Europe Can't Win the Tech War It Just Started," Foreign Policy, Jan. 16, 2020, https://foreignpolicy.com/2020/01/16/europe-technology-sovereignty-von-der-leyen/

16 Adam Segal, "The Coming Tech Cold War With China," Foreign Affairs, Sept. 9, 2020, https://www.foreignaffairs.com/articles/north-america/2020-09-09/coming-tech-cold-war-china

17 United Nations, "Digital Economy Report 2019," July, 2019, https://unctad.org/system/files/official-document/der2019_overview_en.pdf

18 Tambiama Madiega, "Digital Sovereignty for Europe," European Parliamentary Research Service, July, 2020, https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

19 xvii Thierry Breton, "Europe: The Keys to Sovereignty," European Commission, Sept. 11, 2020, https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-keys-sovereignty_en

20 xviii Charlene Barshefsky, "EU digital protectionism risks damaging ties with the US," Financial Times, Aug. 2, 2020, https://www.ft.com/content/9edea4f5-5f34-4e17-89cd-f9b9ba698103

21 European Council, "Recovery Plan for Europe," https://ec.europa.eu/info/strategy/recovery-plan-europe_en

22 At the time of writing, the European Commission planned to launch the DSA and DMA on December 15, 2020.
23 Meredith Broadbent, "The Digital Services Act, the Digital Markets Act, and the New Competition Tool," Center for Strategic and International Studies, Nov. 10, 2020, https://www.csis.org/analysis/digital-services-act-digital-markets-act-and-new-competition-tool
24 The European Democracy Action Plan (EDAP) also provides a framework for countering disinformation and broader electoral interference. The EDAP, released on December 3, 2020, sets out a road map for a more enhanced code of conduct, introduces the possibility of future sanctions on purveyors of disinformation, and doubles down on support for independent media. It is designed to work in concert with the DSA, and therefore avoids specifics on digital market regulation. Link: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12506-European-Democracy-Action-Plan
25 Laura Kayali, "French constitutional court strikes down most of hate speech law," Politico, June 18, 2020, https://www.politico.eu/article/french-constitutional-court-strikes-down-most-of-hate-speech-law/
26 Brown, Chewning, and Singh, "Preparing the United States for the Superpower Marathon with China," p.9.
27 Brown, Chewning, and Singh, "Preparing the United States for the Superpower Marathon with China," p. 11.
28 Cecilia Kang, "FTC Decision on Pursuing Facebook Antitrust Case Is Said to Be Near," The New York Times, Oct. 22, 2020, https://www.nytimes.com/2020/10/22/technology/facebook-antitrust-ftc.html
29 Cecilia Kang and David McCabe, "House Lawmakers Condemn Big Tech's 'Monopoly Power' and Urge Their Breakups," The New York Times, Oct. 6, 2020. https://www.nytimes.com/2020/10/06/technology/congress-big-tech-monopoly-power.html
30 Paul Barrett, "Regulating Social Media: The Fight Over Section 230 — and Beyond," New York University Stern Center for Business and Human Rights, Sept., 2020, https://bhr.stern.nyu.edu/section-230-report-release-page
31 Antitrust is one where there is convergence in approaches, but with quite different motivation behind antitrust legal cases and regulation in the US and Europe. There is also growing agreement that platforms should take more responsibility for content, but no common definition of what such duty of care would entail in practice.
32 High Representative of the Union for Foreign Affairs and Security Policy, "A new EU-US agenda for global change," European Commission, Dec. 2, 2020, https://ec.europa.eu/info/sites/info/files/joint-communication-eu-us-agenda_en.pdf
33 Brigitte Dekker and Maaike Okano-Heijmans, "Europe's Digital Decade? Navigating the Global Battle for Digital Supremacy," Clingendael Institute, Oct., 2020, https://www.clingendael.org/sites/default/files/2020-10/Report_Europes_digital_decade_October_2020.pdf
34 Javier Espinoza, "Tech companies urge EU not to hold them liable for illegal content," Financial Times, Jan. 6, 2020, ; Karan Bhatia, "The Digital Services Act Must Not Harm Europe's Economic Recovery," Google, Oct. 28, 2020, https://blog.google/around-the-globe/google-europe/the-digital-services-act-must-not-harm-europes-economic-recovery/; https://www.ft.com/content/8e3359a2-308f-11ea-a329-0bcf87a328f2; European Digital Media Association (now known as Dot Europe), "EDIMA feedback on proposed Directive on certain aspects concerning contracts for the supply of digital content," European Parliament, Sept. 2020, https://www.europarl.europa.eu/cmsdata/102260/EDiMA%20-%20Position%20paper.pdf; Karan Bhatia, "The Digital Services Act Must Not Harm Europe's Economic Recovery," Google, Oct. 28, 2020, https://blog.google/around-the-globe/google-europe/the-digital-services-act-must-not-harm-europes-economic-recovery/;
35 EDRI, "French Avia law declared unconstitutional: what does this teach us at EU level?," EDRI, June 24, 2020, https://edri.org/our-work/french-avia-law-declared-unconstitutional-what-does-this-teach-us-at-eu-level/
36 Robert Knake, "Weaponizing Digital Trade: Creating a Digital Trade Zone to Promote Online Freedom and Cybersecurity," Council on Foreign Relations, Sep. 2020, https://www.cfr.org/report/weaponizing-digital-trade; Richard Clarke and Rob Knake, "The Internet Freedom league: How to Push Back on the Authoritarian Assault on the Web. Foreign Affairs, August 2019, https://www.foreignaffairs.com/articles/2019-08-12/internet-freedom-league
37 Martijn Rasser et al., "Common Code: An Alliance Framework for Democratic Technology Policy." Center for New American Security, October 2020, https://www.cnas.org/publications/reports/common-code
38 Ian Bremmer, "Why We Need a World Data Organization. Now," GZERO Media, Nov. 25, 2019, https://www.gzeromedia.com/why-we-need-a-world-data-organization-now
39 Jared Cohen and Richard Fontaine, "Uniting the Techno-Democracies How to Build Digital Cooperation," Foreign Affairs, November/December 2020, https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies
40 High Representative of the Union for Foreign Affairs and Security Policy, "A new EU-US agenda,"
41 For a similar argument on the US specifically, see: Brown, Chewning, and Singh, "Preparing the United States for the Superpower Marathon with China,"
42 Andrew Grotto, "The Biden Administration Needs a Fresh Approach to Huawei and 5G," Foreign Policy, Nov. 13, 2020, https://foreignpolicy.com/2020/11/13/biden-huawei-china-5g-risk/
43 Jeffrey Feltman, "China's Expanding Influence at the United Nations – and How the United States Should React," The Brookings Institution, Sept. 2020, https://www.brookings.edu/wp-content/uploads/2020/09/FP_20200914_china_united_nations_feltman.pdf

Center for European Policy Analysis
1275 Pennsylvania Ave NW, Suite 400
Washington, DC 20004
info@cepa.org | www.cepa.org