American Institute for Contemporary German Studies
JOHNS HOPKINS UNIVERSITY

Europe's Digital Autonomy and Potentials of a U.S.-German Alignment toward China

Maximilian Mayer
CASSIS, University of Bonn

A concerted response to China's growing digital power is one of the most critical policy issues requiring U.S.-German coordination during the Biden administration. While approaches to cybersecurity are largely overlapping, and U.S. digital espionage in Germany has not led to concrete countermeasures, Europe's ambitions for "digital autonomy" recently widened the gap of perceptions between German and U.S. policymakers.[1] In particular, with regard to 5G networks, interests and outlook diverge to a degree that questions the ability to form a common approach to the global expansion of Chinese platform and digital equipment companies. Although the German government strengthened the technical and political oversight of 5G hardware from ZTE and Huawei, Berlin refrains from explicitly ruling out Chinese companies' participation in the country's 5G infrastructure rollout—a contentious issue for the Trump administration. However, in preparation for a post-Trump era, it is important not to overly focus on the Huawei case.

The future of technopolitical cooperation between Germany and the United States ought to be considered against the backdrop of the evolving global pattern of digital geopolitics. Its complex trajectories indicate, on the one hand, that there are converging interests and pathways for renewed cooperation not only between the Biden and Merkel administrations but also between Washington and Brussels. On the other hand, threat assessments are diverging, and although the EU has labeled China a "systemic rival," European discourses of digital sovereignty mainly targets U.S. technological dominance rather than China's. It must be expected that the United States and Germany, as its key European partner after Brexit, will face difficulties in developing a joint strategic approach toward the exclusion of Chinese technologies from German digital infrastructures. German political and economic elites, despite growing concerns about China's authoritarian tendencies, don't view technological decoupling as an option. Yet, as the upcoming inauguration of the Biden administration animates expectations of a U.S. return to multilateral and cooperative diplomacy, a possible reset between Washington and Berlin could be harnessed for a boost in transatlantic institution-building and implementing a number of concrete transatlantic cooperation projects in order to align conflicting goals related to the push for digital sovereignty and to improve digital resilience.

[1] For the purpose of this paper, the term digital is defined as pertaining to the use and deployment of computer, internet, telecommunication devices and networks.

Digital Geopolitics

The first step is to acknowledge the complexity of contemporary technopolitics. Coping with the exercise and expansion of Chinese digital power—both by commercial actors and activities of the Leninist party state—was always a mix of regulatory issues, market access, contestations over intellectual property theft, security policy, and ideological rivalry. The struggle over digital technologies became fully politicized when the Trump administration initiated a tech war against China, in tandem with the trade war, COVID-related accusations, and so on. China, on the other hand, implemented its own approach of "decoupling" by fostering self-reliance and cutting back on technological dependence through its "Made in China 2025" strategy.

Conceptually, it is helpful to distinguish between two types of digital geopolitics at play here: one is the politics of platform dominance that privileges a few large companies over all other actors in the global capitalist competition for control of user data. The other is the binary systemic confrontation of great (cyber) powers—liberal systems represented by the United States and the EU vs. authoritarian systems represented by China and Russia. As a result of both of these dynamics, digital technologies and ecosystems have been progressively instrumentalized and consumed by a competitive struggle for digital capacities and control over data collection as well as distribution among Internet giants and great powers.

State-centered digital geopolitics, in addition, is not only a driver for the securitization and militarization of emerging technologies that employ forms of artificial intelligence (AI) including face recognition and big data analysis among others. As a result, Internet governance and data flows fragment further. While China's infamous great firewall was built for purposes of information censorship on behalf of the Chinese Communist Party, its industrial policies gave China a strong position with relatively independent digital ecosystems to cope with global digital geopolitics. On the contrary, the U.S. State Department's "clean network program" is from the outset an exclusionary geopolitical strategy. What makes both approaches comparable, is that they ultimately foster the creation of separate technological spheres and thus contribute to the compartmentalization of global cyberspace. As the Trump administration made decoupling a real political option, China's agencies began to accelerate preexisting research and development efforts in digital technology areas exposed as weak points during the ongoing tech war. Of course, it remains unclear how effective the channeling of investments and state-driven venture capital will be in achieving China's official goal of more self-reliance in technologies.

Against this backdrop, Europe's discourse about "strategic autonomy" has considerably gathered steam. Although neither a single definition nor a common vision exists of "digital sovereignty" or "data sovereignty", the popularity of these notions must be interpreted as a reaction to both types of digital geopolitics. European politicians fear that Europe's position is compromised by firms and governments from both China and the United States. After Edward Snowden's revelations about the extent of U.S. surveillance activities and the systemic use of backdoors, the idea of technological sovereignty quickly turned from a fringe concern into a mainstream notion with dozens of reports and action plans published in recent years. As one

influential think tank in Berlin puts it: "The long-ignored dominance of U.S. Internet companies has forced Europe to embark on a course of digital self-assertiveness – from data protection and competition law to taxation."

Europe's Digital Autonomy and its Limitations

The EU's view on digital technology has taken on decidedly stronger political overtones. While the so-called European human-centric approach has stood out for its emphasis on the legal and ethical dimensions of digitalization and AI, leading policymakers began to frame digital technologies in competitive geopolitical terms. "If we don't build our own champions in all areas — digital, artificial intelligence," says French President Emmanuel Macron, "our choices will be dictated by others." In her 2020 State of the Union Address, EU Commission President von der Leyen proclaimed Europe's "digital decade." She notes that "Europe must now lead the way on digital – or it will have to follow the way of others, who are setting these standards for us." European politicians emphasize that their aim is not to enforce protectionist measures or digital decoupling. Still, the zeal for autonomy is energized by a twofold rationale: to hedge against the dominance of U.S. platforms and safeguard European companies against the intensifying geopolitical competition between the cyber powers China and the United States.

Currently, the EU pursues digital autonomy in three ways: infrastructure projects such as GAIA-X, data governance and antitrust regulations/laws, and legal charges against large U.S. tech companies. The EU is co-funding several mega-tech projects such as GAIA-X. But, as Amazon, Google, Microsoft, and Huawei are all part of this initiative, GAIA-X will neither undermine the hegemonic position of U.S. cloud services nor keep Chinese digital tech at bay. Another example is the European Battery Alliance that aims at decreasing the near-total dependence on Asia for battery raw materials and manufacturing. Meanwhile, voices pushing to form a technology sovereignty fund that invests in indigenous European tech startups become more frequent and louder. With respect to Gaia-X, German Economy Minister Peter Altmaier notes that "Germany and Europe need a data infrastructure that ensures data sovereignty … Germany has a claim to digital sovereignty. That's why it's important to us that cloud solutions are not just created in the U.S." Altmaier's comment, however, ignores two crucial issues: there are already European cloud solutions, but European companies do not possess crucial data processing techniques to keep up with U.S. and Chinese hyperscaling capacities – a critical gap which even the full realization of GAIA-X will not be able to close.

On the regulatory front, the EU has unveiled major initiatives. In December 2020, the EU Commission presented two comprehensive and long-awaited legal packages: the EU Digital Market Act and the EU Digital Services Act. Observers believe these future laws will eventually reshape data transfer and related business models of platform companies across the board, as their main aim is to restrict the market power of large players and ensure fair competition. Given their quasi-monopolistic position, it "is expected that the prohibitions of certain conduct and the imposition of proactive obligations will apply mainly to major U.S. platforms, not their smaller European or Chinese competitors, which may offer similar services." In fact, the vast majority of lawsuits were directed at U.S. platform companies and their monopolistic positions.

Two landmark cases brought down the EU's Safe Harbor agreement covering EU-U.S. data transfers as well as the Privacy Shield regulations (*Schrems I* and *II ruling*), thereby fundamentally reshaping the legal framework for data transfer from European users to U.S. servers. As U.S. Secretary of Commerce Wilbur Ross, among others, points out, all this might have potentially "severe economic consequences." For instance, Facebook and Google currently operate under a preliminary order by Ireland's Data Protection Commission (DPC) to suspend all personal data transfers between the EU and the United States. In contrast, there is no ongoing lawsuit or even an official statement concerning TikTok, the only Chinese social media giant with a significant user base in Europe. While a joint EU members taskforce has been formed to conduct an official investigation into the company's data privacy and data localization practices, which agency precisely has the ultimate authority over TikTok's activities remains unclear.

The biggest legal challenge to U.S. digital giants, arguably, is not the conflict between the EU's General Data Protection Regulation (GDPR) and U.S. digital surveillance practices (Cloud Act) in the evolving transnational field of data regulations, but the strengthening of Brussels' antitrust policy. Within the EU Commission, it is unclear whether this should eventually lead to breakups of big tech companies—an outcome favored by France but opposed by Germany and EU Commission Vice President Margrethe Vestager. Already in November 2020, European Union regulators filed antitrust charges against Amazon over its systematic use of non-public business data "to leverage its dominance." This is a foretaste of the much stiffer legal environment that awaits U.S. platform companies in Europe.

While new data and antitrust laws in Europe (and China) could fundamentally alter how platform companies operate, the drive for Europe's digital autonomy, aside from regulatory strength, faces serious technical hurdles and resource limitations. According to a widely-held view among policymakers, analysts, and industry chiefs, the central obstacle is the lack of thriving indigenous big IT and platform companies. However, this sentiment tends to underestimate Europe's position with regard to digital technologies. Nokia and Ericsson are leading global 5G infrastructure solutions aside from Huawei. Fraunhofer's basic research into AI is highly competitive. And Europe controls parts of the strategic production chains of semiconductors. Still, the bloc's skilled labor force—e.g. only 10% of top-tier AI researchers—is insufficient; innovation dynamics are, except in the field of "Industry 4.0," lagging behind the United States and China. European firms remain vulnerable against cyber attacks in general and largely unprotected against industrial espionage from China. Without the leverage of large platform companies, it appears difficult for the EU to realize the dream of digital sovereignty in the near future. Patent data reveal that manufacturing and services in Germany, in particular, will increasingly have to rely on intellectual property from abroad due to the declining application numbers for information technology and machine learning patents by German companies. Hence, in contrast to the bombast of the EU's policy rhetoric, the actual trends underpinning Europe's "digital decade" point towards more asymmetric interdependencies rather than more autonomy.

Germany's Interdependence with China

Although the EU has commissioned various studies on the platform economy, the political effects of the one-sided dependence on U.S. and Chinese technology require more attention. Germany has a very strong market position in software solutions for industrial and manufacturing systems. Yet, U.S. platforms provide all key non-industrial software components and cloud services to Germany, which makes the country highly reliant on digital infrastructures delivered and maintained by U.S. companies. At the same time, many large and medium-sized German firms are becoming more economically dependent on China. COVID-19 induced shifts have demonstrated that the future prospects of German car companies are tied to the Chinese market even more intimately. Some describe this as a "trap." Others stress that the overall dependency of Germany's economy on China remains small. Whether the narrative of dependency is correct, big German companies with significant political heft clearly have no plans to divest from China. Volkswagen's decision to massively increase R&D investments in China and Daimler's announcement to build engines there indicate that Germany-based transnational companies believe they will only continue to thrive if they become more integrated into the Chinese market.

The extensive presence of German companies in China drives the growing necessity to integrate with Chinese digital ecosystems, cloud services, and other data applications to be able to operate autonomous vehicles, automated factories, and industry 4.0 applications. In other words, decoupling in the digital field—be it manufacturing, automobiles, or machinery—is impossible for leading German companies. Instead, they will move towards deeper integration into various Chinese digital infrastructures with all subsequent legal and political liabilities. This choice follows an established path, as Western companies continue to enjoy the economic advantage of having authoritarian governments in control of their countries' labor force (Foxconn's model). But technological integration is also a precondition for German companies to offer autonomous driving or Internet of Things (IoT) applications for Chinese costumers. This bargain was perhaps never more salient than in the present moment when China enjoys a considerable technological momentum and its growth expectations are robust. Foreign firms strive to avoid being excluded from the Chinese market in the light of the economic policy shifts following the new five-year plan focused on technological self-reliance, domestic substitution, and domestic consumption ("dual circulation").

In Germany, a powerful dependency mindset assumes that it is vital for German industries, even a question of survival, not to alienate the Chinese leadership. Consequently, the idea of getting into a situation in which German companies are torn between two emerging tech ecosystems—being forced to decide between different digital spheres—haunts businesses. But from a wider perspective, Germany's flexibility seems greater than this binary scenario suggests. There are multiple points of divergence and agreement between the United States and Germany when it comes to dealing with China. Germany's limited digital capacity and necessity to consider its digital autonomy in the broader context of evolving economic and political relations, especially in the interest of repairing transatlantic ties, could push the German government to weigh U.S. preferences in cyberspace carefully when it comes to China.

Germany faces a difficult political choice over whether Huawei should be allowed to supply equipment for its 5G infrastructure. German telecommunication companies prefer Huawei's technology for its price and quality. Whilst telecommunication companies such as Telekom and Vodafone continue to collaborate closely with the Chinese firm, Huawei received permission to build its own local 5G network in Munich. Meanwhile, a growing number of European countries, including the UK, Italy, Greece, Sweden, and most Eastern European states have followed the U.S. call to ban Huawei. Berlin has so far rejected pressure from Washington to formally exclude the company. Although some of Germany's security checks are set to apply not just to the "core network" but the entire 5G network, specific security requirements and assessment mechanisms are still under consideration. As critical details of the new IT security law and other regulations remain under inter-ministerial negotiation, it's clear that the current draft of the "IT-Sic 2.0" bill will not amount to the immediate exclusion of Huawei products. Another argument against a black-and-white view on Huawei, similar to the argument against digital technologies from the United States, is that the controversy overlooks the reality that digital autonomy and cybersecurity are sometimes conflicting goals. For instance, using cloud services from Huawei or U.S. companies could enhance protection against cybercrime toward end users, even if the risk of data extraction and digital surveillance through backdoors cannot be completely eliminated.[2] Yet, there is significant opposition to Huawei among the mainstream parties in the Bundestag, and the German government may face a battle against political leaders who will try to strengthen the new law.

Areas of Disagreement between the United States and Germany

Europe's discourse on digital sovereignty has similarities with the Chinese approach fifteen years ago. From the viewpoint of autonomy, the dominance of U.S. platform companies is a vulnerability for Europe. Many Germans harbor similar suspicions against dominant U.S. and Chinese platforms, assuming the foreign governments are working with internet firms to gather information. Peter Altmaier, Federal Minister for Economic Affairs and Energy, at one point suggested a basic equivalence between U.S. and Chinese companies. The French Parliament raised similar issues regarding the U.S. data firm Palantir. Meanwhile, a "wide gulf has emerged between different blocs of democracies." The biggest regulatory differences between the United States and the EU remain the definition and protection of privacy rights and personal data. Germany's Foreign Minister Heiko Maas emphasizes the divergence and argues, "We Europeans have a decision to make. And I say in all candor that I consider neither the Chinese nor the U.S. digital model to be an option."

While initiatives for digital decoupling from China enjoy some support from the United States, European companies and governments do not want to digitally disconnect from China.[3] Germany does not entertain the idea of technological decoupling from the Chinese economy, in

[2] Personal communication with German cyber security expert, 24 November, 2020.

[3] The testing of 6G is already on the horizon and Chinese companies are poised to have a head start even more than with 5G. Hence, the same discussion might repeat itself and there's a danger for Europe to fall back even more.

which German businesses have entrenched interests. Instead, many large and medium-sized German companies are likely to become more integrated into Chinese digital infrastructures. This trend is mirrored at the political level. On September 10, 2020, the EU and China held their first "High-level Digital Dialogue" and, building on earlier cooperation, established a high-level dialogue mechanism on the environment, climate issues, and the digital sector. European and German discussions, whether in business or policy circles, aim at striking a balance between engaging with China as an economic partner, and responding to it as a systemic competitor. The State Department currently categorizes Germany as supporting the Clean Network on the basis of Germany's commitment to implementing the EU 5G Clean Toolbox and the ongoing development of legislation on IT security. Yet, under the abovementioned conditions, a wholehearted German participation in the Clean Network Initiative appears unlikely, not the least because it would run counter to Germany's longstanding emphasis on fair reciprocal market access for German companies in China. In fact, only one network provider in Germany has signed up. The German government has not yet released official statements regarding the initiative.

Furthermore, unlike the United States, European countries have a lackluster response towards the security dimension of China's global connectivity approach and overlook the accelerating Chinese civil-military fusion, which includes many Chinese tech startups, research facilities, and universities. The EU did not publish a blacklist of "Communist Chinese Military Companies" that legally sanctions business and restricts interactions with those entities. Similarly, the German government does not support the notion of "Research Security" justified by broad national security concerns that leads to severe restriction on scientific collaboration with Chinese partners or limits the influx of Chinese students, especially in the fields of artificial intelligence, supercomputing, quantum information, nanoscience, and advanced manufacturing.

Finally, Germany does not have an offensive cyber strategy and sufficient relevant capabilities. The 2018 U.S. *National Cyber Strategy* emphasizes the concept of "defend forward," which entails the option of proactive attacks. In contrast, the German approach to cybersecurity, which was traditionally focused on defense in terms of network security and infrastructure resilience, only includes "preventative measures," according to the 2016 Defense White Paper. Though Germany established a federal agency dedicated to combating cyber threats and is developing limited capacities for intelligence/data extraction, and Interior Minister Horst Seehofer uses the term "active cyber defense," the German approach is still in a transition phase from a purely defensive posture to incorporate limited offensive components. Germany remains very hesitant to employ offensive cyber measures for constitutional reasons and few Germans would favor the normalization of, for instance, methods of "hacking back" or a comprehensive militarization of cyberspace.

Areas of Agreement between the United States and Germany

Many German political leaders harbor a growing skepticism toward China. Germany plans to closely monitor Huawei and other Chinese suppliers of digital services and infrastructures. Following the "Prague Proposal," Berlin agreed to create a single set of security standards and

procedures for Germany's 5G rollout. In addition, the notion of diversification of supply chains away from Chinese companies, particularly due to shortages of medical equipment during the early phase of the COVID-19 pandemic, supported by both Washington and Berlin to avoid vulnerabilities, although Germany would prefer less aggressive rhetoric and posturing. Germany and the United States recognize the need to improve critical infrastructure security against the threat of cybercrime and against Russian and Chinese hacking activities and other hybrid threats. In 2019, EU leaders asked the European Commission to "work on measures to enhance the resilience and improve the security culture" of the bloc. In its new Security Union Strategy, the EU mentions NATO and the G7 as strategic partners to counter hybrid threats and strengthen critical infrastructure security.

Data privacy regulations could become a shared interest under the Biden administration, too. "Adding national standards for data protection to the Obama administration's Consumer Privacy Bill of Rights" is listed in the Democratic party's platform. Biden seems interested in setting privacy standards "not unlike [what] the Europeans are doing." In this regard, decision-makers on both sides of the Atlantic already apparently agree on weakening encryption requirements for communication infrastructures and social media applications to allow for law enforcement access to private communication.

The stakeholder model of global Internet Governance needs to be reinforced and improved in response to China and Russia's move to make the ITU a central player. The EU Commission's approach to see China as a "systemic rival promoting alternative models of governance" is in line with widespread views in the United States, but needs to be translated into actual diplomatic actions and presence in relevant technical and standard-setting fora. These coordination efforts could potentially include a substantive dialogue on frameworks for platform regulation to move against tax evasion and act on anti-trust policy. The U.S. policy environment has become more favorable for the latter, as the lawsuit against Facebook's monopolistic practices indicates. How to transnationally regulate platform companies could be a part of a dialogue on data governance as well as the effective protection of democratic processes between the United States and the EU, while they keep a close eye on current changes of platform regulation by China.

German-US Cyber Cooperation: the Way Forward

Several areas are apt for a structured exchange but require time to regain trust and for institution-building efforts in order to benefit from a renewal of German-U.S. cyber cooperation. To respond to the challenges posed by China's growing digital influence, while taking into account the reality of complex technological interdependencies between Germany, the United States, and China, it is helpful to think strategically and with a clear political long-term vision. The goal of strengthening the relevant institutions is not only to enable the management of cyber interdependence but also to broaden international cooperation in producing digital global public goods.

Bilateral- and Minilateral initiatives under U.S.-German / EU leadership:

- Revitalize policy dialogues to cope with diverse emerging fields of digital policy and regulation. For instance, the U.S.-Germany Cyber Bilateral Meeting should be held bi-annually with a strengthened institutional capacity and supported by stronger input from the interdisciplinary research community. Along this line, additional forums connecting think tanks, research institutes, policymakers, and other stakeholders are needed. Thematic areas which require regular exchanges via transatlantic track 1.5 discussions and high-level meetings include: anti-trust and tax policy for platform companies; combating fake news and the spread of misinformation; standards for blockchain technologies, including digital currencies issued by Central Banks, and their applications (currently pushed by China); new IP proposals from Chinese companies (interoperability); dual-use concerns for AI and Big Data.
- Begin sustained exchanges on anti-trust regulations and actions to ensure a shared approach to guarantee fair competition. This is especially important because anti-trust policies and lawsuits are being enacted in the EU, the United States, and China. The EU Commission's "human-centric approach" requires exemplification of what it means in concrete steps for digital transatlantic relations, while the United States' new anti-trust actions against big platform companies have not been strategically coordinated with the EU. Both sides should avoid parallel efforts to push their policy preferences through their respective legislative processes and only after the fact come together to compare approaches.
- Clarify transparent and shared standards for security clearance of software ecosystems, algorithms, and equipment used in critical infrastructures are needed in the United States and at the EU level. This entails also elaborating common methods and procedures for cyberattack attribution to allow a coordinated response across the jurisdictions of NATO allies and to enable lawsuits against perpetrators. With respect to China, a rational digital security policy should be based on a risk assessment approach rather than one that digitally disconnects Chinese companies and systems as a principle of faith. As the resumption of TTIP negotiations seems unrealistic, the EU has proposed a broader mechanism, and EU-U.S. Trade and Technology Council (TTC), in order to develop "compatible standards and regulatory approaches for new technologies" which Politico called Anti-China. It would make sense to start a dialogue to better respond to authoritarian digital practices in the context of "intelligence overreach" and global surveillance capitalism more generally.
- Propose concrete responses to China's Digital Silk Road that promote digital connectivity and digital platform solutions for microfinance, e-commerce, education, and healthcare in the global South. One way of doing so is to link development assistance more organically with digitalization/datafication in order to close the digital gaps in/with the global South. Here, Europe and the United States should take a page from the playbook of the Chinese government and Chinese companies to better conceptualize their visions through concrete projects. Part of this is deepening interdisciplinary expertise and data on different digital trends, innovation, sociotechnical, and regulatory in China.

Multilateral initiatives which could be promoted by the United States and Germany / the EU

- Promote open data initiatives (e.g. at the city level) that experiment with public data use and different forms of data ownership. Technical solutions should include open-source options such as ORAN. Design and test policy frameworks for public-private partnership data platforms to harvest digital technologies in a post-COVID-19 world with a focus on health, education, and public services.
- Revitalize negotiations to lay the groundwork for an international treaty on cybersecurity. European states possess limited offensive cyber capabilities and would welcome steps to deescalate tensions. An agreement on self-constraints concerning cyberattacks would facilitate the process of updating international law and is a worthwhile but challenging transatlantic project with regard to China.
- Update dialogues on multistakeholder Internet governance, which competes with state-centric Russian-Sino initiatives, in consideration of alternative stack proposals (e.g. "new IP"), standard-setting (IPv6, IoT, etc.), and extraterritorial effects of China's jurisdiction (Multi-Level Protection System, MLPS 2.0).
- Navigating the troubled waters of digital geopolitics requires networking with a diverse group of allies around the world. In line with Berlin's brand new policy guidelines for the Indo-Pacific region, Germany and the United States should engage more actively in multilateral cybersecurity initiatives and combine efforts on both internet openness and digital autonomy with regional partners such as Japan, Taiwan, South Korea, and ASEAN. Important digital "swing states" such as Indonesia and India should be included, too.

Realistic Expectations

Comparing areas of agreement and disagreement between the United States and Germany suggests it is crucial to maintain realistic expectations about the possibilities of policy coordination. Even with a rejuvenation of the transatlantic relationship, Germany won't and can't simply walk away from China. Despite growing skepticism and anxieties about China's increasingly authoritarian and anti-liberal politics among German politicians, Minister Altmeier, according to Politico, still believes in "transformation through trade," with China. Furthermore, it is prudent to acknowledge both structural asymmetries and the reality of a highly interdependent global technoscientific ecosystem that calls into question the political rationale for technological decoupling and digital autonomy. Variegated U.S. and German commercial interests toward China mean that a binary choice to decouple doesn't really exist, as Microsoft's plan to hire 8,000 researchers and developers in China suggests.

Regardless of how the 5G and other critical digital infrastructure issues evolve, Germany will continue to search for a compromise that allows the progressive deepening of interdependence between German companies and Chinese digital infrastructures. Berlin wants to avoid explicit discrimination in the German market against companies based on their national origins. Germany's emphasis on digital sovereignty and disagreements with the United States on the future of technology regulations notwithstanding, the political will in Berlin to collaborate

closely with a new U.S. administration is evident. Working from areas of broad agreement can lead to meaningful and concrete steps forward. Some of the recommendations mentioned above, such as robust exchanges on anti-trust policies, are perhaps less likely to be enacted in the early days of the Biden administration. Other proposals, such as responding to China's Digital Silk Road Initiative, need to be developed quickly, but on the basis of a shared long-term vision between the EU and the United States. Having suffered from diplomatic estrangement during the Trump administration, the U.S.-German digital policy alignment needs to prioritize (re)institutionalization of dialogues and high-level exchanges about cybersecurity practices and internet governance while recognizing the practical implications of digital autonomy.