POLICY BRIEF

Forging a Transatlantic Technology Alliance: Opportunities and Challenges Related to ICT and Cloud

Daniel S. Hamilton

The United States and the European Union (EU) have recently launched various initiatives to manage their competition and enhance their cooperation on trade and technology issues. The Transatlantic Leadership Network's Trade and Technology Working Group addresses these topics in its work, including recommendations for more effective action. This policy brief discusses U.S.-EU opportunities and challenges related to information and communications technologies (ICT) and cloud services. While I have benefit from discussions with Working Group members, the proposals presented here are my responsibility alone. All products from the TLN Working Group may be found at https://www.transatlantic.org/transatlantic-technology-and-trade-working-group/.

Working Group 4 – Information and Communication Technology and Services (ICTS) Security and Competitiveness: The Information and Communications Technology and Services working group is tasked to continue to work towards ensuring security, diversity, interoperability and resilience across the ICT supply chain, including sensitive and critical areas such as 5G, undersea cables, data centers, and cloud infrastructure. The working group is tasked to explore concrete cooperation on development finance for secure and resilient digital connectivity in third countries. The working group is tasked to seek to reinforce cooperation on research and innovation for beyond 5G and 6G systems. The United States and the European Union, in close cooperation with relevant stakeholders, could develop a common vision and roadmap for preparing the next generation of communication technologies towards 6G. The group is also tasked to discuss data security.

- U.S.-EU Trade and Technology Council Inaugural Joint Statement, September 2021 [1]

Introduction

The digital transformation is becoming the single most important means by which both sides of the North Atlantic can reinforce their bonds and position themselves for a world of more diffuse power, intensified competition and disruptive challenges. Information and communications technologies (ICT) and cloud services will be critical to this transition.

The transatlantic theatre is the fulcrum of global digital connectivity.[2] The United States and Europe are each other's most important commercial partners when it comes to ICT-enabled services. Transatlantic flows of data continue to be the fastest and largest in the world, accounting for over one-half of Europe's global data flows and about half of U.S. flows. North America and Europe generate about 75% of digital content for internet users worldwide. The United States and Europe each hosts more data centers than Asia, Africa, the Middle East and Latin America combined. Transatlantic cable connections are the densest and highest capacity routes, with the highest traffic, in the world. Moreover, as the EU has noted, the digital

revolution is about more than hardware and software: “it is also about our values, our societies and our democracies.”

Information and communications technologies are the beating heart of the wider digital economy. Deeply intertwined ICT and ICT-enabled trade, investment and research links make the transatlantic economy the geo-economic base for an emergent U.S.-European technology alliance.

Transatlantic Ties in ICT-Enabled Trade

The top global hubs for imports and exports of ICT-deliverable services are the United States, Germany, Ireland, the Netherlands, France and the UK. In 2019, ICT-enabled services accounted for 59% of all U.S. services exports, 50% of all services imports, and 76% of the U.S. global surplus in trade in services. America’s main commercial partner was Europe, to which it exported over $245 billion in ICT-enabled services and from which it imported an estimated $133 billion. U.S. exports of ICT-enabled services to Europe were about 2.7 times greater than U.S. ICT-enabled services exports to Latin America, and roughly double U.S. ICT-enabled services exports to the entire Asia-Pacific region.

The 27 EU member states collectively exported €1.1 trillion in ICT-enabled services to countries both inside and outside the EU in 2019. EU27 imports of ICT-enabled services were also €1.1 trillion in 2019. Excluding intra-EU trade, EU member states exported €585 billion and imported €622 billion in ICT-enabled services. ICT-enabled services represented 55% of all EU services exports to non-EU countries and 63% of all EU services imports from non-EU countries. The United States is the EU’s most important partner when it comes to ICT-enabled trade, accounting for 22% of the EU27’s ICT-enabled services exports to non-EU countries, and 27% of EU digitally-enabled services imports from non-EU countries in 2019.

ICT-enabled services are not just exported directly, they are embedded in manufactured goods and used to produce goods and services for export. Over half of the ICT-enabled services each partner imports from the other is used to generate products for export, thus generating an additional value-added effect on trade that is not easily captured in standard metrics.

ICT-Enabled Services Supplied Through Foreign Affiliates

Far more important than trade, however, is the delivery of digital services by U.S. and European foreign affiliates – another indicator reinforcing the often-overlooked fact that foreign direct investment, not trade, is the major driver of transatlantic commerce. U.S. services supplied by affiliates abroad were $1.704 trillion, roughly double global U.S. services exports of $875.83 billion. Moreover, half of all services supplied by U.S. affiliates abroad are ICT-enabled. 52% of the $938 billion in services provided in Europe by U.S. affiliates in 2018 was ICT-enabled. In 2018 U.S. affiliates in Europe supplied $490.51 billion in ICT-enabled services, whereas European affiliates in the United States supplied $273.78 billion in ICT-enabled services. ICT-enabled services supplied by U.S. affiliates in Europe were almost double U.S. ICT-enabled exports to Europe, and ICT-enabled services supplied by European affiliates in the United States were double European ICT-enabled exports to the United States.

The significant presence of leading U.S. service and technology leaders in Europe underscores Europe’s position as the major market for U.S. digital goods and services. In 2018, Europe accounted for 69% of the $289.6 billion in total global information services supplied abroad by U.S. multinational corporations through their majority-owned foreign affiliates. U.S. overseas direct investment in the “information” industry in the UK alone, for instance, was more than double such investment in the entire Western Hemisphere outside the United States, and 33 times such investment in China. Equivalent U.S. investment in Germany was four times more than in China.

The U.S., Europe and the Cloud

Cloud technologies are a driver of the digital economy. The Covid-19 pandemic has accelerated use of the cloud as industries adapt to support a more digital workforce and to cater to digitally-focused customer needs. Accenture reports that as of 2020, 36% of European workloads, and 31% of U.S. workloads, were on the cloud (China: 37%).[3] While cloud computing is still only estimated to account for 5-10% of the global IT market, adoption of cloud services is likely to accelerate as companies understand that the cloud is more than a cost-efficient alternative to data centers – it is a key enabler of advanced digital technologies.

Three developments in the deeply intertwined transatlantic cloud market bear watching. First is the shift in providers of cloud-like services from European and U.S. telecoms companies to "hyperscalers," mainly from the United States. While European providers have more than doubled their cloud revenues since 2017, their market share in Europe has declined from 27% to under 16%, whereas Amazon Web Services (AWS), Microsoft Azure and Google Cloud now account for 69%.[4] This has generated concerns within Europe about U.S. dominance, which could inhibit some possible avenues for deeper transatlantic cooperation.

Two other trends have the potential to mitigate such concerns, depending on how they unfold: migration to the "edge;" and the evolution of "cloud-as-a-service" to "cloud-as-a-product."

Today, most cloud computing still happens in centralized rather than decentralized data centers. By 2025, this trend will reverse: 80% of all data is expected to be processed in smart devices closer to the user, known as edge computing. This could open opportunities for European providers able to offer multi-cloud options that ensure local control over data with the amplified possibilities that come from hyperscaled connections. Cloud/edge computing is likely to be critical to the EU's ability to realize its European Green Deal, particularly in areas such as farming, mobility, buildings and manufacturing.[5]

These opportunities are likely to be influenced by the evolution of the cloud from being a platform on which a business runs, to becoming the product itself. Rather than considering hyperscalers as direct competitors, some European telecoms operators and companies in a range of other businesses now see their biggest opportunities in the cloud building on top of the basic infrastructure already rolled out by U.S. companies. For instance, Siemens is building an ambitious "industrial cloud platform" on top of the basic cloud infrastructure provided by Amazon, to enable it to become a key player in digital industrial manufacturing services. Thales, a French defense company, is forming a joint company with Google to provide a sovereign hyperscale cloud service in France. Vodaphone has also formed a partnership with Google, and AWS will soon start selling private 5G networks direct to businesses.[6]

The U.S. Domestic Setting

The United States, under different administrations, has expressed a commitment to promoting an open, interoperable, reliable and secure Internet; protecting human rights online and offline; and supporting a vibrant, global digital economy. Achievement has not always matched aspiration, however, as national security concerns have influenced U.S. approaches to digital technologies, and as speed-of-light innovations have outpaced speed-of-law legislation in a politically polarized society.

Despite their many differences, partisans of left and right remain concerned about the terrorist threat to the United States, and are united in their alarm that authoritarian countries, particularly China, seek to leverage digital technologies and other instruments to gain unfair commercial advantages and to threaten the security of the United States and its allies. The United States has taken various ICT-relevant actions to counter such

efforts. Notable examples include Section 702 of the Foreign Intelligence Surveillance Act, Executive Order 12333, Presidential Policy Directive 28, and the U.S. Cloud Act, which guide and enable intelligence agencies to collect and use the personal data of individuals and conduct digital surveillance activities both inside and outside the United States. [7]

In 2019 President Trump issued an executive order declaring the threat posed to the U.S. information and communications technology and services (ICTS) supply chain to be a "national emergency," and prohibiting U.S. companies from using foreign telecommunications equipment deemed to be a national security risk. Three other orders followed. The Trump administration prohibited transactions with various Chinese ICT firms, notably Huawei, and placed China's Semiconductor Manufacturing International Corporation (SMIC), China's most advanced maker of computer chips, on the Entity List, shutting off its access to U.S.-made tools, semiconductor designs, and software. It also pressured non-U.S. companies such as Dutch ASML and Japanese Electron to stop sales to SMIC.[8] On June 9, 2021 President Biden, while recognizing "the ongoing national emergency," revoked and replaced the Trump-era orders with his own executive order directing the use of an evidence- and criteria-based decision framework to address the risks posed by ICTS transactions involving software applications related to foreign adversaries.[9]

The Committee on Foreign Investment in the United States (CFIUS) is an interagency committee tasked with reviewing foreign inbound investments for national security risks. In 2018, Congress expanded CFIUS's authority via the Foreign Investment Risk Review Modernization Act (FIRRMA) so it had the capacity to focus on Chinese companies' access to U.S. critical technologies and Americans' personal data. The Biden administration and the Congress have largely continued the Trump administration's efforts. The 2021 U.S. Innovation and Competition Act of 2021 (USICA), for instance, broadens CFIUS's jurisdiction to certain gifts to, and contracts with, universities. [10]

FIRRMA also authorizes the Treasury Department to exempt specific "foreign states" from CFIUS's expanded jurisdiction. Currently, Australia, Canada and the UK have received these exemptions, largely because of their intelligence-sharing and defense base industrial integration with the United States.[11] Neither the EU nor individual EU member states are exempt. The Biden administration is considering ways to share information on potentially troubling investments with key allies, including through the U.S.-EU Trade and Technology Council (TTC) and the Indo-Pacific Quad (Australia, Japan, India and the U.S.).

Another interagency committee focused on Chinese ICT practices is Team Telecom, created in 1997 and formalized in a 2020 executive order by President Trump. Team Telecom's recommendations have been instrumental in the revocation of a number of existing authorizations and denial of new authorization applications by Chinese entities.[12]

Having largely missed out on 5G development, U.S. companies only account for minor shares of the 5G market. The exception is Apple, which accounts for almost 30% of the global 5G smartphone market. Having largely shut out Chinese providers, the U.S. faces 5G reliance on Sweden's Ericsson and Finland's Nokia, which together account for 30% of the global 5G market. Ericsson's $8.3 billion partnership with Verizon Communications is a leading example of transatlantic interlinkages in the 5G sector. Samsung's $6.65 billion contract with Verizon for network equipment and services that covers 5G and 4G infrastructure is another potential game-changer due to interconnections with the United States.[13]

Faced with foreign dominance of its 5G market, the U.S. has emphasized the need for 5G vendor diversity and is fostering a 5G alternative by promoting Open RAN, a new technology based on open standards that promises lower-cost equipment, more flexibility, and greater opportunities for more vendors. Despite their promise, though, such vendors still control just a fraction of the market share for 5G equipment.[14] The Department of Defense's 5G-to-xG program is investing $600 million into 5G networks at select U.S. military installations.[15]

The experience with 5G and heightened concerns about China's technological advances have generated broader bipartisan U.S. political support for more directive government policies to shape technological developments, and telecoms in particular.

The European Setting

Europe's fragmented governance structure has hampered its ability to capitalize fully on its inherent technological strengths. Many issues related to ICT/cloud innovation, security and resilience are in the hands of EU member states rather than the European Commission. Moreover, the UK has left the EU, aligning more closely with the United States and embarking on a different approach to these issues than most EU countries. For instance, in 2019 the U.S. and the UK entered into the world's first-ever Cloud Act Agreement, which allows law enforcement agencies of both countries to demand, with proper authorization, electronic data regarding serious crime directly from tech companies based in the other country. The two countries have also signed a robust bilateral science and technology partnership on 6G.[16]

The key transatlantic challenge continues to be differences over privacy regulations related to personal data. On July 16, 2020, the Court of Justice of the European Union (CJEU) invalidated the U.S.-EU Privacy Shield framework that regulated some transatlantic flows of personal data for commercial purposes. It determined that FISA Section 702 and E.O. 12333 do not meet the standards of necessity and proportionality under the EU's General Data Protection Regulation (GDPR), and do not provide EU citizens with effective judicial redress. The judgment (dubbed Schrems II) threatens to chill the $6.3 trillion transatlantic economy. Since then, companies have turned to another tool – standard contractual clauses – to transfer personal data. This practice has not yet been put to the test, but in its judgment the Court ruled that such mechanisms can work only for transfers to jurisdictions whose privacy protections are EU-equivalent. The United States plausibly fails this test. The European Commission and the U.S. Department of Commerce are in the midst of renegotiating the Privacy Shield. Failure to reach an understanding on these matters threatens to chill the $6.3 trillion transatlantic economy.[17]

After initial transatlantic turmoil generated by U.S. efforts to oust Chinese 5G telecoms from critical networks, not only at home but in Europe and elsewhere, many – but not all – European allies have also acted to marginalize those companies' presence in their networks.[18] Greater transatlantic alignment on this challenge is still required.

Beyond these issues, the European Commission is seeking to boost the EU's technological capacities, and to tame the power of dominant non-EU companies, through various mechanisms. Europe's Recovery & Resilience Facility (RRF) identifies 5G as a flagship area for a significant share of its targeted €150 billion digital budget to finance 5G network infrastructures, and Europe's Digital Compass target aims to deliver 5G for all by 2030.[19]

The EU's cybersecurity agency ENISA seeks to finalize in 2022 a new cloud cybersecurity certification that would impose tougher cybersecurity rules on non-EU cloud providers. Authorities in France and some other EU member states want to go further by preventing non-EU cloud providers from providing EU data to U.S. authorities if asked or, failing that, excluding non-EU cloud providers entirely from critical sectors such as health case and financial services.[20]

The European Commission is deploying what EU Internal Market Commissioner Thierry Breton calls a "regulatory arsenal" of initiatives, such as the Data Governance Act, the Artificial Intelligence Act, the Digital Services Act (DSA) and the Digital Markets Act (DMA).[21] The Commission is also slated to unveil a standardization strategy in coming months. "Who makes the standard holds the market," says Breton. He has singled out 5G, batteries, hydrogen, and quantum computing as sectors where the EU wants to become

a "standard maker."[22] The Commission is also behind an edge and cloud industrial alliance, where membership and access is limited to those who can prove that they abide by EU laws and are not subject to laws of any third country. [23]

In contrast, other European initiatives launched initially to dilute the influence of non-EU ICT/cloud providers have now been opened to non-EU companies. GAIA-X, a Franco-German initiative launched in June 2020 to enhance the EU's "digital sovereignty," has now accepted as members U.S. global cloud players such as Amazon, Google, IBM, Microsoft and Salesforce, and Chinese providers Huawei and Alibaba.[24] Germany's "sovereign cloud" will be run by Deutsche Telekom together with Google, which will offer its services but with local controls over the data.[25] France's *cloud de confiance*, or "trusted cloud," similarly combines commitment to data protections under French law with an openness to participation by foreign companies, and to French companies using licensed foreign technologies. France's "Bleu" partnership between Capgemini and Orange, for instance, offers Microsoft services through a new, local entity that offers clients "immunity" from U.S. extraterritorial law.[26]

On Open RAN, European views have yet to coalesce. Europe is home to 13 of the 70 major global players in this field. Five of these major telcos have urged Europe to identify Open RAN as a strategic priority. They urge European leadership in standardization, and want the European Commission to create a European Alliance on Next Generation Communication infrastructures. They have called on the Commission and EU member states to offer public funding and tax incentives to operators, vendors and start-ups to support the development of European solutions along the entire Open RAN value chain. Failure to do so, they warn, risks Europe falling behind North America and Asia in the development and deployment of next generation networks.[27] However, other major European telcos, and some EU governments, are not yet convinced of Open RAN's full potential, and wary of the additional costs a major investment may require.[28] German authorities have expressed caution that "security/privacy by design/default" has not been baked into Open RAN systems.[29] Those standing to lose most from competitive Open RAN systems – including Ericsson and Nokia -- are also unenthusiastic. [30]

6G development is another matter. Led by Finland (Nokia) and Sweden (Ericsson), Europe is pushing forward with 6G R&D. In addition to a number of initiatives supported by the EU's Horizon Europe program, a consortium of 25 European players (including Intel Deutschland) launched the Hexa-X consortium in January 2021 to lay the groundwork for a long-term European investment in next-generation wireless network technologies. Nokia has the overall lead and Ericsson the technical lead for the consortium. This was followed by the EU's release of its vision for the 6G network ecosystem in June 2021. The United States has yet to set forth a 6G strategy.[31]

Key Elements of a Transatlantic Technology Alliance in ICT and Cloud

U.S. and European goals in the ICT/cloud sectors align in various areas. However, instead of building on dense transatlantic digital interconnections and the shared principles that underpin them, in recent years the two parties have allowed a series of digital disconnects to roil U.S.-European relations.

An analysis of the full technology stack unveils important opportunities for a more robust transatlantic technological alliance. Those opportunities could begin if the two parties could exploit their common ICT strengths and their relative complementarities. Whereas Europe is relatively underdeveloped compared to the United States in higher technology layers such as AI and platforms, the United States is relatively underdeveloped compared to Europe in key parts of lower technology layers such as 5G. An overall bargain could conceivably be achieved by joint efforts to enhance Open RAN, align on privacy standards, and guard against security threats and market abuses, coupled with U.S. willingness to grant European companies greater access to its domestic 5G market and European willingness to cooperate more closely on platforms and AI. Since the potential gains and pains from such an overall arrangement would affect particular

industry sectors and individual countries differently, opposition to such an overall arrangement could be significant. Yet the pieces are there.

Each side of the Atlantic has adopted defensive or punitive measures when it comes to burgeoning commercial and geopolitical competition in the ICT field. Such efforts are likely to be more effective if they were accompanied by an affirmative transatlantic agenda, which could be pursued through and beyond the TTC working group on ICTS security and competitiveness, and might include the following steps:

Conclude a Privacy Shield successor deal. The Schrems II judgment hangs over the entire landscape. Current negotiations on a successor to Privacy Shield may offer a temporary work-around, but since the Court's decision in rooted not in policy but in law, ultimately the only sustainable resolution will be revamped privacy legislation in the United States, and that could take some time.

Affirm common principles and industry codes of conduct. On multiple occasions in the past the two parties have agreed on a set of shared principles to guide their activities in this space. It would be useful for both to once again affirm their joint commitment to such principles as a basis for their common work. Such principles include: transparency in legislation and regulation; the independence of regulatory authorities; open networks for consumers to access and distribute information, applications and services of their choice; the importance of a strong and competitive shared environment for ICT development and use; strong yet flexible intellectual property (IP) laws; interoperable data protection regimes that enable innovation while also protecting privacy; agreement that governments should allow foreign participation in their ICT services; affirmative policies in support of digital trade; science and technology cooperation related to digital innovation and research; and robust international cooperation to manage policy differences.[32] In addition, the two parties should foster industry Codes of Conduct for data protection in the cloud, building on efforts currently under way on each side of the Atlantic. If the two sides of the Atlantic prove able to harness their joint potential based on these principles, they could form the core of a wider technology alliance of like-minded democracies that can prove more vibrant than autocratic alternatives.[33]

Coordinate with industry on standard-setting. Industry primarily sets ICT standards across a number of bodies, with 5G technology standards primarily set in the 3rd Generation Partnership Project (3GPP) and open RAN standards set in the O-RAN Alliance. Beijing often directs its companies to vote for new standards as a bloc, privileging Chinese-drafted standards that are often not the best technological standard. The United States, EU member states and other like-minded countries should coordinate and encourage their respective companies to vote together in bodies like 3GPP and the O-RAN Alliance for the best standard, regardless of country of origin. The U.S. Commerce Department should create a carveout in its current directives to allow companies to fully engage in standard-setting bodies alongside all Chinese counterparts. Failure to do so abandons the field to China, as key companies such as Nokia do engage with Chinese counterparts, and the U.S. has no interest in sanctioning European companies while Chinese companies continue their work in such bodies.[34]

Reclaim influence in international standard-setting bodies. China has assumed control of key positions in relevant international organizations and agencies—such as the Internet Corporation for Assigned Names and Numbers and the International Telecommunication Union—which has further allowed the Chinese government to entrench its regulatory standards and surveillance practices across the world. The United States and the EU have been slow to respond to these developments. Reclaiming influence over international standard setting is critical to preserving strong democratic governance of emerging technologies.[35]

Avoid a subsidy race. As the significance of the technological revolution becomes clearer, both parties are turning to industrial policies, including subsidies and directive research funding, to shape the U.S. and EU technology sectors, and telecoms in particular. To avoid a subsidy race and additional transatlantic tensions,

and in line with agreed principles, each party should open access to such public support to U.S. companies in the EU and EU companies in the United States.

Enhance cooperation on export controls. While outside the scope of this paper, the two parties have identified this as a priority, and work is progressing under one of the TTC working groups.

Address intellectual property (IP) concerns. IP rights foster much of the R&D that drives the digital economy. The US and EU, together with Canada, the UK and Switzerland, should strive to agree to protect the free movement of knowledge, such as by allowing companies participating in pre-competitive research to freely transfer ownership and access rights for IP to affiliates across and across their common space, and to agree on common protections for trade secrets on both sides of the Atlantic.[36]

Boost innovation. While more R&D expenditures are emanating from Asia in general, and China in particular, the United States and Europe remain primary drivers of global R&D, and bilateral U.S.-EU flows in R&D are the most intense between any two international partners.[37] In 2018, U.S. affiliates spent $33 billion on research and development in Europe. Europe accounted for roughly 56% of total U.S. R&D conducted abroad by U.S. affiliates. In the United States, R&D expenditures by majority-owned foreign affiliates totaled $66.9 billion in 2018. European firms accounted for two-thirds of the total ($45.1 billion). The digital economy has become a powerful engine of greater transatlantic R&D. Alliances, cross-licensing of intellectual property, mergers and acquisitions, and cooperation through "open" innovation networks have become more prevalent. The complexity of scientific and technological innovation is leading innovators to partner and share costs, find complementary expertise, and gain access to different technologies and knowledge more quickly. Supportive public policies, such as issuing joint calls for proposals for research and establishing cross-border research alliances, can help further deepen ties across the U.S. and European science and technology communities and advance transatlantic leadership in ICT and related activities.[38]

Foster multi-cloud/federated cloud strategies. Rules governing cloud services are likely to continue to differ among jurisdictions across the North Atlantic space. Instead of seeking to harmonize those differing regimes, industry and governments should facilitate the ability of firms and public sector institutions to operate in multi-cloud/federated cloud domains so that entities can deploy the right data/workload into the most appropriate cloud for their specific purposes, while being able to operate across differing clouds and cloud services jurisdictions.[39]

Work together on Open RAN. The Open RAN global suppliers' market is estimated to be worth €36.1 billion by 2026. According to Deloitte, Open RAN could reduce capital expenditures on RAN by 40-50%, and operating expenses by 30-40%, in addition to disrupting the telecoms oligopoly.[40] By disaggregating radio access networks into smaller components and thus enabling multiple companies to supply different parts of a modular 5G network, Open RAN holds promise to break the oligopolistic hold over the market currently enjoyed by a handful of end-to-end providers, potentially enhancing vendor diversity and lowering costs. On the other hand, 5G raises new security issues and vulnerabilities through the RAN that were not deemed critical under previous generations of mobile networks. Cooperative efforts going forward must integrate "security/privacy by design/default" and "zero trust" access models. Such efforts should also incorporate work done by the G7, under UK leadership, to stimulate greater competition.[41]

Encourage edge computing. Cloud computing means that network functions do not need to be housed in centralized data centers, but can be decentralized and dispersed to the "edge," giving customers faster response times, cheaper service tied to actual usage rather than fixed costs, and more local control over their data. Like Open RAN, edge computing holds the promise of supporting a wider range of suppliers beyond the current oligopoly of providers.[42]

Bolster ICTS Security. Fending off cyberattacks has become a grueling daily reality for most companies and countries.[43] Cyberattacks have spiked during the COVID-19 crisis as new communication paths and work environments have created new security risks. The TTC should act as enabler and supporter for increased EU-U.S. cooperation on cybersecurity certification. Private sector leaders have underscored the importance of joint efforts, given dense transatlantic interconnections.[44] Rules forcing businesses to fragment their technology operations along national borders result in less consistency and more complexity and negatively impact security and resilience.

- ***Cybersecurity and finance***. Greater collaboration between the parties, specifically on systemic risks to the financial system, would encourage mutual understanding and risk identification.
- ***Global risk identification.*** Identify common approaches to detecting, mitigating and managing cyber risk at the transatlantic and global levels. Consensus-based, international standards and industry-led best practices should be drawn upon, including on cybersecurity, cyberespionage and supply chain security.
- ***Public-private partnerships.*** Public-private partnerships should be leveraged to develop complementary and coordinated policies and to ensure that networks and systems are resilient against evolving cyberattacks.
- ***Strengthen dialogue on intelligence sharing*** in the area of cyber incidents (both pre and post cyber incidents).
- ***Promote dialogue on strengthening resilience and strengthening cryptographic methods,*** for instance by addressing "encryption backdoors," which weaken the protective effect of cryptography. Systems must integrate "security/privacy by design/default" and "zero trust" access models.

Move ahead on ITA-3. The Information Technology Agreement is a plurilateral agreement to eliminate tariffs on a wide range of ICT products. ITA participants include 82 WTO members representing 97% of world trade in ICT products. In 2015, 53 countries, including the United States and EU member states, committed to eliminate over 200 additional tariffs, valued at $1.3 billion in annual global trade, on further ICT products. Given the tremendous pace of technological innovation, however, even this recent round of ITA expansion (ITA-2) now fails to cover a host of new products. An ITA-3 agreement could cover an additional 250 ICT products or components, including next-generation semiconductor technologies and manufacturing. The ITA has greatly accelerated global demand for ICT products. Expanding the ITA's geographic and product coverage would further enhance the competitiveness of U.S. and European companies and those from other partner countries.[45]

Focus on 6G: The U.S. and EU, in close cooperation with relevant stakeholders, could set a goal to be first movers in 6G communication technologies, which are slated to be commercialized by 2030 and likely to replace 5G within 15 years. 6G networks are projected to be up to 100 times faster than the peak speed of 5G, with further reduced latency, embedded AI-enabled capabilities, higher energy efficiency, and the seamless convergence of sensing, computing, and communications. China invested $180 billion over five years to cement its leadership in 5G, and investment at a similar scale is needed to lead the race to 6G. [46]

6G comprises dual-use technologies of military significance; China is likely to incorporate them into its military-civil fusion strategy, as it has with 5G. Transatlantic allies thus have both commercial and defense-related interests to cooperate more closely on 6G. Moreover, unlike 4G and 5G developments, which unfolded as part of a single global standard, 6G development is likely to unfold within a context of fragmented standards and markets – rendering transatlantic consultations and cooperation even more essential.[47] The transatlantic partners are likely to be more secure, and more commercially competitive, if they align more closely on 6G and other technological innovations, thus strengthening democratically-based standards, rather than allow competitive impulses result in an even further splintering of standards and markets, not only between them and China, but also between each other.

- ***Drive 6G eco-system development***, including via funding for 6G university research centers, 6G testbeds, and incentives to support private sector investment in 6G. The National Science Foundation's RINGS program, the EU's Horizon Europe program, the Hexa-X research project, and equivalent EU member state institutions and programs could identify opportunities for collaborative transatlantic projects to further 6G technologies, identify security risks and promote resilience.
- ***Create a Democratic 6G Network***, open to other techno-democracies, to address key issues including technology development, security, standard setting, and spectrum. A U.S.-EU-UK 6G Spectrum Working Group could identify spectrum needs for 6G rollouts and offer recommendations for spectrum access and management, including opening of additional experimental spectrum licenses.
- ***Promote transatlantic industry collaboration***. The ATIS Next-G-Alliance (NGA) in the U.S. and the 5G Infrastructure Association (5G IA) in Europe both aim to shape research and technology collaborations towards 6G. Each organization is structured around work groups on similar topics, and there is overlap in membership, reflecting the deep integration of the transatlantic innovation space. There is clear opportunity for cooperation between the two organizations at the technical level.

Use NATO's Defense Innovation Accelerator for the North Atlantic (DIANA) and its two Innovation Hubs in Europe and the U.S., and grow the Alliance's €1 billion Innovation Fund to support the development of a protected transatlantic innovation community, including via cooperation on 6G technologies, testbeds and accelerators, and assessments of vulnerabilities and threats to 6G networks.[48]

- ***Identify and resource the priority technologies affecting NATO's core tasks*** as part of Alliance's Strategic Concept review.
- ***Anchor technological issues more robustly within the Alliance.*** Allied Command Transformation (ACT) and a number of NATO-related Centers of Excellence must become tech thought leaders. Technology acquisition forecasting should be incorporated into the NATO Defense Planning Process (NDPP) and ministerial agendas. Technology literacy must be encouraged across the Alliance. Conduct an annual assessment, perhaps via NDPP, of national progress in adopting new technologies.
- ***Identify and integrate emerging and disruptive technology applications into NATO training, exercises, experimentation, plans and operations***. Approve relevant NATO standards and system interoperability requirements for such technologies.
- ***Establish vibrant connections with industry partners and with the EU institutions***, such as the European Defense Agency (EDA), DG Innovation & Research, and CERT-EU.

Notes

[1] White House, "U.S.-EU Trade and Technology Council Inaugural Joint Statement," September 29, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/29/u-s-eu-trade-and-technology-council-inaugural-joint-statement/.

[2] Data in this paper draws on Daniel S. Hamilton and Joseph P. Quinlan, *The Transatlantic Economy 2021* (Washington, DC: Johns Hopkins SAIS/Wilson Center, 2021), https://transatlanticrelations.org/publications/transatlantic-economy-2021/.

[3] Accenture, "Ever-ready for every opportunity: How to unleash Europe's competitiveness on the Cloud Continuum," September 2021, https://www.accenture.com/_acnmedia/PDF-163/Accenture-Europe-Cloud-Continuum.pdf#zoom=40

[4] Linda Hardesty, "European cloud providers take hit from AWS, Google, Azure, says Synergy," Fierce Telecom, September 23, 2021, https://www.fiercetelecom.com/platforms/european-cloud-providers-take-hit-from-aws-google-azure-says-synergy; European Commission, "Cloud computing," https://digital-strategy.ec.europa.eu/en/policies/cloud-computing.

[5] European Commission, "5G for Europe's Digital and Green Recovery," January 14, 2021, https://digital-strategy.ec.europa.eu/en/library/5g-europes-digital-and-green-recovery; Accenture, op. cit.

[6] Richard Waters, "Every company may soon be a cloud company," *Financial Times*, December 2, 2021; Oliver Noyan, "Europe's Cloud Dreams Come Crashing Down to Earth," Center for European Policy Analysis, https://cepa.org/europes-cloud-dreams-come-crashing-down-to-earth/; Alice Pannier, "The Changing Landscape of European Cloud Computing: Gaia-X, the French National Strategy, and EU Plans," Briefings de l'Ifri, July 22, 2021, https://www.ifri.org/sites/default/files/atoms/files/pannier_european_cloud_computing_2021.pdf.

[7] For an overview, see Chris D. Linebaugh and Edward C. Liu, "EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield, Congressional Research Service, March 17. 2021, https://crsreports.congress.gov/product/pdf/R/R46724; Ericka Johnson, "The CLOUD Act, Bridging the Gap between Technology and the Law," *The National Law Review*, March 19, 2018.
[8] Christine Fox and Thayer Scott, "Flat No Longer: Technology in the Post-Covid World," in Hal Brands and Francis J. Gavin and Hal Brands, eds., *COVID-19 and World Order: The Future of Conflict, Competition, and Cooperation* (Baltimore: Johns Hopkins University Press, 2020), https://muse.jhu.edu/chapter/2696561/pdf; "A new direction for the European Union's half-hearted semiconductor strategy," Bruegel, September 28, 2021, http://bruegel.org/reader/A-new-direction-for-the-European-Unions-half-hearted-semiconductor-strategy#a-strategic-sector-defined-by-states-support.
[9] "FACT SHEET: Executive Order Protecting Americans' Sensitive Data from Foreign Adversaries," The White House, June 9, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/09/fact-sheet-executive-order-protecting-americans-sensitive-data-from-foreign-adversaries/
[10] "S.1260 - United States Innovation and Competition Act of 2021," Congress.gov, https://www.congress.gov/bill/117th-congress/senate-bill/1260/text.
[11] Adam Chan, "CFIUS, Team Telecom and China," Lawfare, September 28, 2021, https://www.lawfareblog.com/cfius-team-telecom-and-china.
[12] Ibid.
[13] U.S. companies such as Cisco and Ciena, or non-Chinese Asian companies such as Samsung, account for only minor shares of the U.S. market. John McCormick, Meghan Bobrowsky and Dan Strumpf, "Huawei, Ericsson or Nokia? Apple or Samsung? U.S. or China? Who's Winning the 5G Races," *Wall Street Journal*, October 12, 2021.
[14] Ibid.
[15] "DOD Announces $600 Million for 5G Experimentation and Testing at Five Installations," Department of Defense (DoD) (Oct. 8, 2020), https://www.defense.gov/Newsroom/Releases/Release/Article/2376743/dod-announces-600- million-for-5g-experimentation-and-testing-at-five-installati/.
[16] U.S. Department of Justice, "U.S. And UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online," October 3, 2019, https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists.
[17] European Data Protection Supervisor, " EDPS Statement following the Court of Justice ruling in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems ("Schrems II")," July 27, 2020, https://edps.europa.eu/press-publications/press-news/press-releases/2020/edps-statement-following-court-justice-ruling_en; European Commission, "Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection," https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en; Mikołaj Barczentewicz, "Will the EU Lose Access to U.S. Data Flows and Software?" Lawfare, November 3, 2021, https://www.lawfareblog.com/will-eu-lose-access-us-data-flows-and-software.
[18] In addition to the United States, eight countries have issued outright bans of the company. Many others have taken measures that ban Huawei de facto if not explicitly. However, Huawei remains involved in 56 networks in NATO members Hungary, Iceland, the Netherlands and Turkey.
[19] European Commission, "5G for Europe's Digital and Green Recovery," op .cit.
[20]Laurens Cerulus, "France wants cyber rule to curb US access to EU data," Politico, September 13, 2021, https://www.politico.eu/article/france-wants-cyber-rules-to-stop-us-data-access-in-europe.
[21] Thierry Breton, quoted in Luca Bertuzzi, "Mastery of technology is central to the 'new geopolitical order', Breton says," Euractiv, July 27, 2021, https://www.euractiv.com/section/digital/news/mastery-of-technology-is-central-to-the-new-geopolitical-order-breton-says/.
[22] Ibid.
[23] European Commission, "Commission launches alliances for microelectronics and cloud technologies," July 19, 2021, https://digital-strategy.ec.europa.eu/en/news/commission-launches-alliances-microelectronics-and-cloud-technologies.
[24] Wenche Karlstad, "Why sovereign cloud is a hot topic – 5 tips, and the background," Tietoevry.com, November 9, 2021, https://www.tietoevry.com/en/blog/2021/11/why-sovereign-cloud-is-a-hot-topic/.
[25] David Meyer, "Germany's 'sovereign cloud' is coming—and it's provided by Google," *Fortune*, September 8, 2021.
[26] Pannier, op. cit.
[27] See the report by the five telcos -- Deutsche Telekom, Orange, TIM (Telecom Italia), Telefónica and Vodafone : In a new report, "Building an Open RAN Ecosystem for Europe," https://www.vodafone.com/sites/default/files/2021-11/building-open-ran-ecosystem-europe.pdf.
[28] While 5 companies endorsed the report, there are more than 40 operators across Europe. For a skeptical view, see Ray Le Maistre, "BT's Chief Architect skeptical about Open RAN's cost-saving potential," Telecomtv.com, November 12, 2021, https://www.telecomtv.com/content/open-ran/bt-s-chief-architect-skeptical-about-open-ran-s-cost-saving-potential-42932/.
[29] See "Open-RAN Risikoanalyse," Stefan Köpsell, Studie im Auftrag des Bundesministeriums für Sicherheit in der Informationstechnik," November 9, 2021, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/5G/5GRAN-Risikoanalyse.pdf.
[30] Ericsson, "Securith Considerations of Cloud RAN," August 2021, https://www.ericsson.com/4a67b7/assets/local/reports-papers/further-insights/doc/02092021-12911-security-considerations-for-cloud-ran.pdf; Laurens Cerulus, "Cracks appear in West's 5G strategy after Huawei, Politico, November 30, 2021, https://www.politico.eu/article/us-europe-5g-strategy-huawei/; Fox and Scott, op. cit.
[31] https://hexa-x.eu; Martijn Rasser, Ainikki Riikonen, and Henry Wu, "Edge Networks, Core Policy: Securing America's 6G Future, CNAS, December 2021, https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS-Report-6G-Dec-2021-final.pdf.
[32] European Union-United States Trade Principles for Information and Communication Technology Services, April 4, 2011, https://itlaw.fandom.com/wiki/European_Union-United_States_Trade_Principles_for_Information_and_Communication_Technology_Services;;
[33] See Nick Wallace, et al., "How Canada, the EU, and the U.S. Can Work Together to Promote ICT Development and Use," Information Technology and Innovation Foundation, June 2018, https://www2.itif.org/2018-canada-eu-us-ict-development.pdf?_ga=2.136210481.122227442.1638825802-193437476.1635703355.
[34] See Carisa Nietsche, "Opportunities for Transatlantic Cooperation on Technology Standards," Transatlantic Leadership Network, November 2021, https://www.transatlantic.org/wp-content/uploads/2021/12/11-30-2021-Nietsche_Opportunities-for-Transatlantic-Cooperation-on-Technology-Standards_v2.pdf; Ali Khayrallah & Hugo Tullberg, "US and EU approaches to 6G," Woodrow Wilson Center, July 15, 2021, https://www.wilsoncenter.org/article/us-and-eu-approaches-6g.
[35] See "China's Belt and Road: Implications for the United States," Council on Foreign Relations Independent Task Force, 2021, https://www.cfr.org/report/chinas-belt-and-road-implications-for-the-united-states/download/pdf/2021-04/TFR%20%2379_China%27s%20Belt%20and%20Road_Implications%20for%20the%20United%20States_FINAL.pdf.
[36] Ibid.

[37] Hamilton and Quinlan, op. cit.
[38] Wallace, et al., op. cit.
[39] Hardesty, op. cit.; Accenture, op. it.
[40] Rasser, et al., op. cit.
[41] Hosuk Lee-Makiyama (with Florian Forsthuber), "Open RAN: The Technology, its Politics and Europe's Response," ECIPE, 8/2020, https://ecipe.org/wp-content/uploads/2020/10/ECI_20_PolicyBrief_08_2020_LY03.pdf; Köpsell, et al., op. cit.; Phil Hunter, "G7 countries grope towards coordinated approach to Open RAN ecosystem," ReThink, May 25, 2021, https://rethinkresearch.biz/articles/g7-countries-grope-towards-coordinated-approach-to-open-ran-ecosystem/; Cerulus, "Cracks…," op. cit.; Fox and Scott, op. cit.
[42] Rasser, et al., op. cit.;
[43] David E. Sanger describes in detail the grinding, daily short-of-war cyberattacks that he says "have become the new normal." See *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age (New York: Crown, 2018).*
[44] Some of these suggestions draw on stakeholder input to the TTC, especially from the American Chamber of Commerce to the EU. See amchameu.eu/trade-technology-council.
[45] Stephen Ezell and Luke Dascoli, "How an Information Technology Agreement 3.0 Would Bolster Economic Growth and Opportunity," Information Technology and Innovation Foundation, September 16, 2021, https://itif.org/publications/2021/09/16/how-information-technology-agreement-30-would-bolster-economic-growth-and; Stephen Ezell, "An Allied Approach to Semiconductor Leadership," Information Technology and Innovation Foundation, September 2020, https://itif.org/sites/default/files/2020-allied-approach-semiconductor-leadership.pdf; Magnus Nordéus, "The Information Technology Agreement –a success story," Ericsson, 2021, https://www2.itif.org/2021-ITA-Nordeus.pdf?_ga=2.184404896.704234341.1638642402-193437476.1635703355; 2021 State of the U.S. Semiconductor Industry," Semiconductor Industry Association, June 2021.
[46] Shirley Zhao, Scott Moritz, and Thomas Seal, "Forget 5G, the U.S. and China Are Already Fighting for 6G Dominance," Bloomberg, February 8, 2021, https://www. bloomberg.com/news/features/2021-02-08/forget-5gthe-u-s-and-china-are-already-fighting-for-6g-dominance; "6G: The Next Hyper-Connected Experience for All," Samsung Research, https://cdn.codeground.org/ nsr/downloads/researchareas/20201201_6G_Vision_ web.pdf; David Sacks, " China's Huawei Is Winning the 5G Race. Here's What the United States Should Do To Respond," Council on Foreign Relations, March 29, 2021, https://www.cfr.org/blog/china-huawei-5g.
[47] Drawing on Rasser, et al., op. cit.; "China's Belt and Road," op, cit.; Khayrallah & Tullberg, op. cit.
[48] I am grateful to my colleague Charles Barry and members of the NATO Task Force that I host for thoughtful insights.