msc

No. 3/2021

Update Required

European Digital Sovereignty and the Transatlantic Partnership

Munich Security Brief
July 2021

Authors

Simon Pfeiffer
is a Policy Advisor
at the Munich Security
Conference.

Randolf Carr
is a Senior Policy Advisor
at the Munich Security
Conference.

Summary

European policymakers have made explicit commitments to strengthening Europe's digital sovereignty, especially where dependencies affect security. Europe clearly has its strengths, but there is a significant opportunity for targeted interventions to secure Europe's core digital capabilities for the future. Bolstering its technological capabilities could serve not only Europe, but also the transatlantic partnership.

Policymakers on both sides of the Atlantic are taking steps to advance cooperation on issues of technology. However, Europe needs to ensure potential weaknesses in certain technological areas do not dampen growth or create dependencies in defense, intelligence, and national security.

To understand how Europe can achieve this, a clear-eyed view of its key domestic digital capabilities is required. These capabilities can be summarized to be in five areas: connectivity, data gathering and integration, data storage and processing, analytics and artificial intelligence (AI), and cybersecurity. Europe has strengths in some of the technologies critical to these capabilities, and has the opportunity to accelerate the pace of innovation, commercialization, and adoption in others.

If Europe shows deficiencies on core capabilities, significant risks to transatlantic security and the common digital agenda of the transatlantic partnership might emerge. It is in the partnership's interest that Europe remains capable of building secure supply chains, achieving data interoperability in intelligence, cooperating on cybersecurity, and enabling joint NATO military operations. Europe could benefit from promoting the commercialization of research, using the security sector as a catalyst for innovation, and leveraging European cooperation in procurement, data sharing, and ambitious common projects.

Update Required – European Digital Sovereignty and the Transatlantic Partnership

"European freedom of action requires economic and digital sovereignty. It is Europe's job to define the framework for regulation that it imposes on itself, for it is a matter of protecting the individual freedoms and economic data of our companies, which are at the core of our sovereignty, and of our concrete operational capacity to act autonomously."[3]

Emmanuel Macron, French President, Speech on the Defense and Deterrence Strategy, February 7, 2020

As digital technologies become increasingly important in government, industry, and daily life, Europeans are becoming more concerned about their reliance on foreign technology providers. Many believe their governments are doing too little to protect them from a loss of control in the digital world.[1] In a survey of more than 6,000 Europeans in six countries commissioned by the Munich Security Conference, 50 percent of respondents agreed that their country is too dependent on digital technologies from the United States; 54 percent thought the same about technology from China.

More than four in ten respondents said they expected European technology to fall behind that of China and the US over the next ten years; only one-third believe Europe will be on par, and six percent think Europe will take the lead.[2] A survey for the recent Munich Security Report 2021 shows that, around the world, including in Europe, the vast majority of people believe the US and China will be the leading tech powers in 50 years' time, not the European Union.[4]

This idea does not sit comfortably with citizens, who clearly prefer some control and thus sovereignty in their digital affairs. They worry that their countries have become too dependent on foreign digital technologies.[5] At the same time, only 13 percent of Europeans today believe their data is in safe hands with the US government, and nine percent with China's government.[6]

Consequently, "digital sovereignty" has emerged as a strategic priority among European policymakers – at both the European and the national level.[7] While there is a range of competing definitions and alternative concepts, digital sovereignty can be understood as a state's ability to make decisions and act in a self-determined manner in the digital space.[8]

On the one hand, this concerns the demand side of digital technology – how it is procured and used.[9] This includes the EU's central measure on data privacy, the General Data Protection Regulation and flagship initiatives such as the Digital Services Act and the Digital Markets Act.[10] Another example is the "European Strategy for Data," put forward by the European

"In the face of growing tensions between the United States and China, Europe will not be a mere bystander, let alone a battleground. It is time to take our destiny into our own hands. This also means identifying and investing in the digital technologies that will underpin our sovereignty and our industrial future."[14]

Thierry Breton, EU Commissioner for Internal Market, Speech at Hannover Messe Digital Days, July 15, 2020

"Digital Sovereignty gives trust and security for our citizens, it's important to develop it in cooperation with our Western values-based partners, like the United States."

Nicola Beer, Vice President of the European Parliament, MSC Technology Roundtable, July 6, 2021

Commission in 2020, aimed at improving the use of data in the EU and tackling major roadblocks for the vision of a common European data space, such as fragmentation between member states.[11] In April 2021, the EU proposed an "Artificial Intelligence Act" with a comprehensive regulatory structure for a range of AI use cases.[12]

Now, on the other hand, concerns about the strength of the European private tech sector – the supply side of technology – are also front and center. A new focus on industrial policy emerged with initiatives such as the "Franco-German Manifesto for a European Industrial Policy Fit for the 21st Century", the provision of 7.5 billion euros for supercomputing, artificial intelligence, cybersecurity, advanced digital skills as well as the setup of Digital Innovation Hubs under the Digital Europe Programme. Most recently, the European Commission's Digital Compass set out concrete industrial targets, including not just the adoption and availability of technology, but also, for example, a doubling of the EU's share in the global production of cutting-edge semiconductors.[15]

Increasing cooperation on technology has been a key item on the transatlantic agenda, including setting governance standards for the internet, data, and digital technology – a long-held and shared ambition.[17] After US President Joe Biden and European leaders expressed their ambitions for a renewal of the transatlantic partnership at the MSC Special Edition on February 19, 2021, steps are now being taken toward closer alignment on an expanding range of issues, most notably with the recent establishment of the high-level US-EU Trade and Technology Council.[18] Issues in focus include the introduction of a digital tax, competition policy, and rules for sharing personal data, but increasingly also close cooperation on technology and security.[19] Indeed, the established transatlantic collaboration on security matters has put the issues of the security of supply chains, data interoperability and sharing in intelligence, as well as cooperation in cybersecurity high on the common digital agenda.[20] Joint operations with technologically advanced forces within NATO are likely to require institutional, procedural, and technical solutions that allow for interoperability and data sharing on a massive scale.[21]

"Europe and North America need to continue to stand together in the face of increased global competition. Economically, militarily, and technologically."[22]

Jens Stoltenberg, Secretary General of NATO, MSC 2020, February 15, 2020

A Framework for Digital Sovereignty

To understand how Europe can position itself and gauge what European digital sovereignty might mean for the transatlantic partnership, a clear view of Europe's digital technology landscape is needed, especially as it relates to security.

To be digitally sovereign – that is, to make decisions and act in a self-determined manner in the digital space – Europe requires reliable access to key capabilities, either by owning them through European companies and infrastructure or by procuring them from trustworthy partners.[23] Five key capabilities (see Figure 1) reflect the key process that cuts across digital technologies: the flow of data – how data is transferred, gathered and integrated, stored and processed before it is put to use through analytics and AI, while its integrity and security are ensured through cybersecurity measures at each step.

Figure 1

A capability-based framework for digital sovereignty

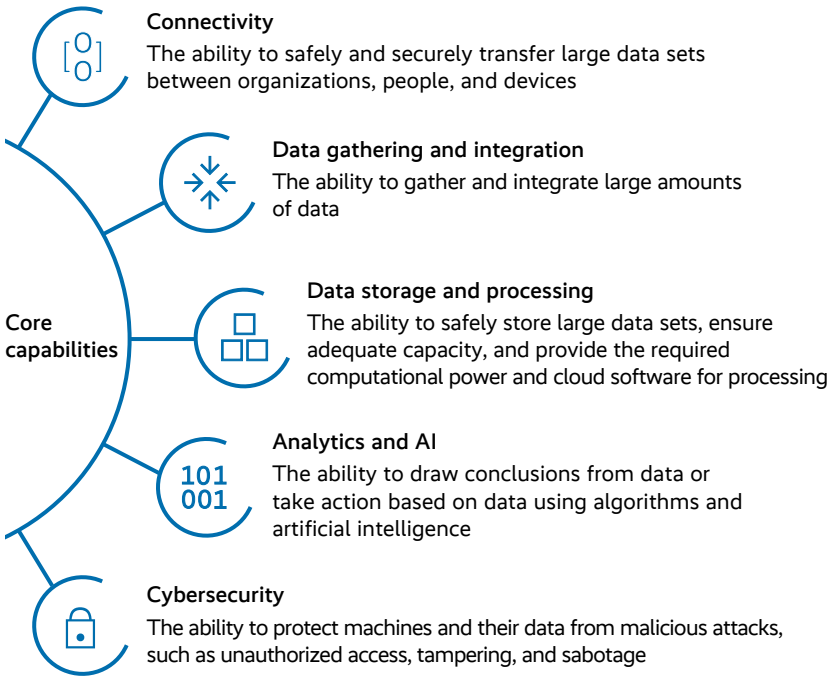


Illustration: Munich Security Conference

"Europe is going digital, right now, as we speak. Yet, I am convinced that Europe is still punching well below its weight [...]. Our investment in other fields still lags behind the US and China."[16]

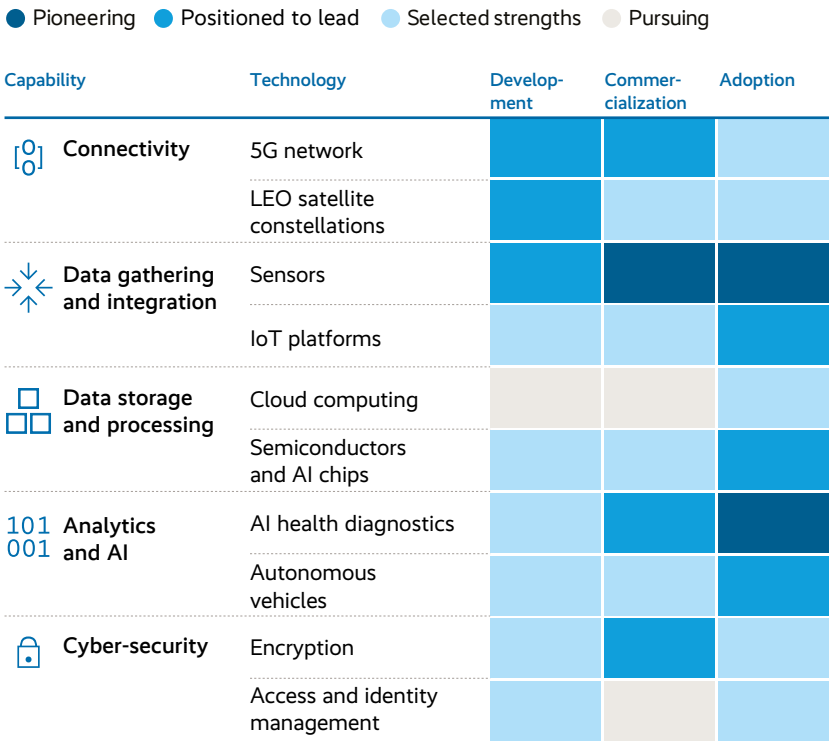
Ursula von der Leyen, President of the European Commission, Masters of Digital 2021 Event, February 4, 2021

Analyzing selected technologies that are critical for each capability can help identify priorities for Europe's own supply of digital technologies. Considering technologies at different levels of maturity provides a comprehensive perspective of Europe's capabilities and how it will fare in technologies where large-scale commercialization and adoption have only just begun (see Figure 2).

This touches on another key aspect of digital sovereignty: the technologies in question are constantly changing. Connectivity, for example, requires industrial and technological resources for a range of technologies at different stages, like terrestrial 5G and constellations of satellites, along with undersea cables and other connectivity-related technologies.[24] Technologies are emerging and evolving at a rapid pace, and startups as well as agile corporations are commercializing them before they are widely adopted.

Figure 2

Overview of Europe's position in key technologies



Data and illustration: Munich Security Conference

It is critical to assess Europe's position in selected technologies, including a range of indicators surrounding their development, commercialization, and adoption.

Connectivity

The *fifth generation of wireless networks*, or *5G*, will enable machine-to-machine communication at a groundbreaking scale.[25] With a broad range of applications, the technology is considered a key enabler of AI, cloud usage, and edge computing.[26] For the military, 5G could lead to improvements in the speed and fidelity of transported information, especially in intelligence, surveillance, and reconnaissance systems.[27] The advance of 5G may have implications on secure supply chains: several countries have restricted the provision of 5G network equipment or services to suppliers that are deemed secure or trustworthy.[28] The US "Clean Network" initiative, which aims to safeguard the nation's assets "from aggressive intrusions by malign actors," has the support of 27 of NATO's 30 members,[29] and the European Commission has asked member states to diversify their purchasing strategies for 5G equipment.[30]

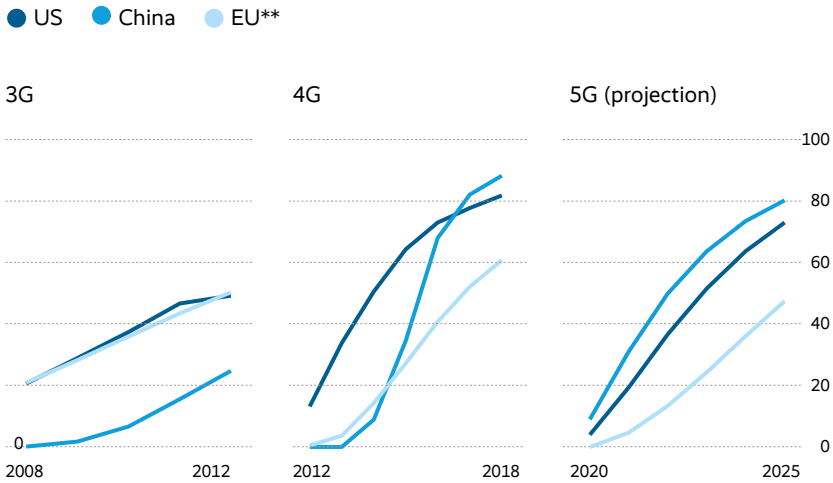
> Europe has historically been a leader in wireless connectivity and is strong in development and market share.

While it is hard to isolate the 5G market, the overall global telecommunications network equipment market can give an indication of the market structure: In 2020, European firms shared around more than one third of the market, while Chinese companies owned about 40 percent, and with Cisco the US had only a minor player accounting for roughly 5%.[31] Europe's share of wireless connectivity comes largely from two legacy players: Ericsson and Nokia. The EU is still relatively strong in the development of 5G technology: together with the United Kingdom, European companies accounted for 23 percent of 5G patents granted in 2018, compared to 20 percent for China and 13 percent for the US.[32]

However, only about five percent of all startups active in 5G network equipment are based in the EU or UK, compared to 40 to 50 percent in China and the US, respectively.[33] Further, having been at the global forefront of 3G adoption from 2008 to 2012 and on into 2018 (see Figure 3), penetration rates are expected to reach only 48 percent in the EU by 2025, if there are no strategic interventions, compared to 80 percent in China and 73 percent in the US.[34]

Figure 3

Adoption rate of selected wireless network technologies, 2008–25, percent of connections*



*Share of active connections using the specified network technology
**EU and United Kingdom; Cyprus, Malta, and Luxembourg excluded
Data: Company reports from DB Research. Illustration: Munich Security Conference

Low earth orbit (LEO) satellite constellations are revolutionizing space-based connectivity. These fast-moving networks of small, affordable, and resilient satellites can provide an alternative to ground-based wireless networks and current satellite-based connectivity. The highly reliable LEO constellations are also key for military applications, especially in locations where other communication channels are not available, such as the Arctic, or when adversaries jam other means of connectivity.[35] The rise of space-based connectivity has gained political attention, given its prospective impact on economies and the military, and more broadly as part of a "new space race."[36] Thierry Breton, the EU's Internal Market Commissioner, recently suggested that a LEO constellation project should be Europe's next priority in space after the Galileo and Copernicus projects.[37] When the UK government acquired a major stake in satellite firm OneWeb in 2020, Europe became home to one of the major players in LEO constellations; the other two, SpaceX and Iridium, are based in the US.[38]

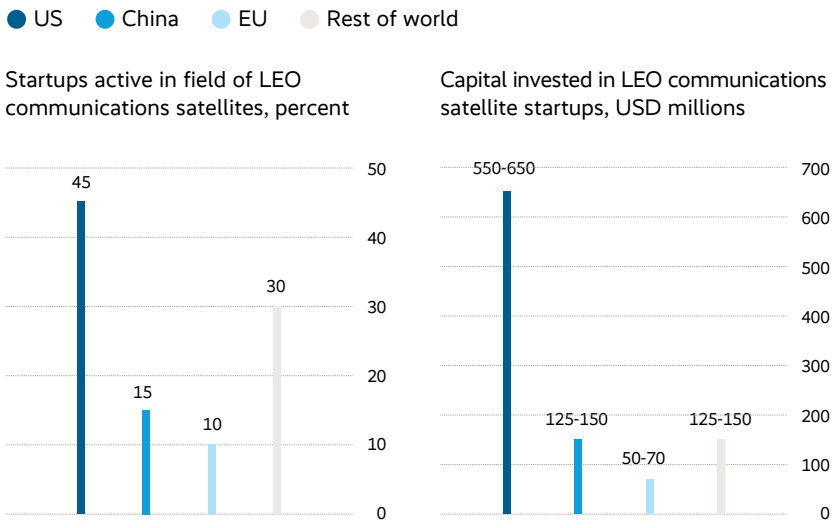
Europe has an opportunity to begin developing its own major space-based connectivity industry.

However, other metrics suggest that Europe is now trailing in the development, commercialization, and adoption of LEO-based connectivity: 58 percent of patents granted and pending relating to LEO satellite technology stem from the US, with China accounting for 45 percent and the EU and UK for only 18 percent.[39] The US is also home to the largest share of startups active in the LEO communications satellite space (see Figure 4). While US-based companies had over 1,000 active LEO satellites in January 2021, the EU together with the UK only had 112, and China trailed with a low two-digit figure.[40] The EU together with the UK, including OneWeb, had 112.

European policymakers have a range of options for future-proofing European capabilities in connectivity. Firstly, these include continuing to support secure open standards for disaggregated 5G networks.[41] Though it remains unclear how much interoperability is achievable and what it might mean for performance and security, technology-neutral standards could allow network technology suppliers to work together more freely and thereby diversify the supplier landscape.[42] They could serve as a major push for the European 5G startup ecosystem and make better use of Europe's lead in 5G-related patents, realizing that innovation in 5G comes from the collaboration of smaller and bigger players

Figure 4

Estimated LEO satellite startups and funding by region, 2020*



* Data retrieved in November 2020", has not been reviewed by PitchBook analysts
Data: PitchBook Inc. Illustration: Munich Security Conference

in the ecosystem. Military and intelligence stakeholders could be involved in these efforts, perhaps modeled on approaches of the US Department of Defense such as its 5G Challenge to develop an open 5G ecosystem that can support its missions.[43] Secondly, policymakers could support the swift deployment of base stations, especially along critical transportation corridors and urban centers as, for example, envisioned by the Connecting Europe Facility 2.0 programme. As our analysis shows, slow adoption is Europe's "Achilles heel" in connectivity.[44] First steps could include speeding up the 5G rollout by holding spectrum auctions earlier and on schedule, and by reducing prices. More European countries should also consider aiming for lower prices in spectrum auctions – like Finland and France – in exchange for faster rollout or coverage in more remote areas.[45] Finally, a consortium selected by the European Commission is already assessing the feasibility of a European LEO constellation.[46] The EU and its member states could increase their efforts to build, own, and operate a LEO constellation, boosting development, commercialization, and adoption across the entire European space ecosystem.

Data Gathering and Integration

Data gathering and integration transform observations about the real-world environment, for instance through sensors, into digital data – and then turn diverse types of data from many such sources into usable data sets. *Smart sensors* combine sensing and computing abilities, making them a key technology for more efficient data gathering from smartphones over medical devices to industrial robots. As miniaturized sensors proliferate, they will yield unprecedented volumes of data and enable a myriad of new products and applications. The defense sector is especially interested in innovation in advanced sensors because of their high impact in military and security domains.[47] China has made smart sensors a focus of industrial innovation as part of its Made in China 2025 strategy.[48] In 2019, the European Commission published a report on the wide-ranging impact of the Internet of Things (IoT), where connected sensors play an integral role.[49]

In smart sensors, Europe could slip from its good competitive position if there is a lack of innovation.

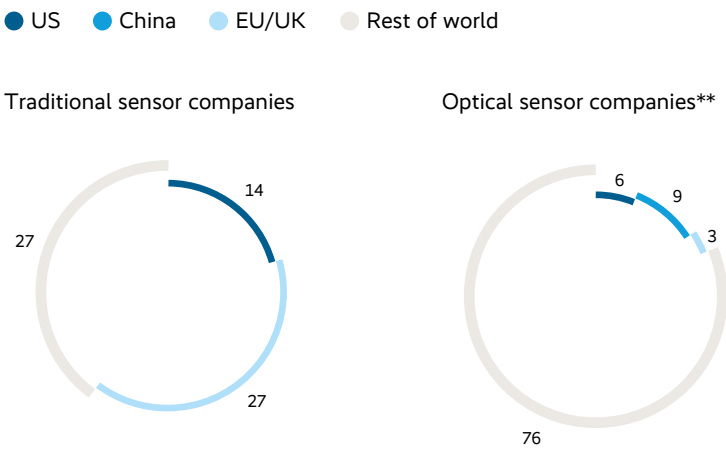
European companies are home to than a quarter of the worldwide market for "traditional" sensors (see Figure 5).[50] Estimates show that Western European countries alone may spend roughly 428 billion US dollars on IoT hardware modules and sensors between 2020 and 2025, roughly on par with China at 410 billion and well ahead of the US at 278 billion.[51]

In terms of innovation and the development of smart sensors, which are increasingly software-based rather than hardware-based, Europe is currently providing eleven percent of patents filed in the smart sensor space.[52] The startup picture is similar, with one billion US dollars invested in sensor technology startups in Europe in the past five years, half the amount invested in such startups in China, and a small fraction of the eight billion invested in the US.[53]

The proliferation of smart, sensor-enabled, and connected devices that make up the IoT creates another challenge: coordinating these devices to act in concert and integrating the data they capture in ways that make it easy to use in applications. *IoT platforms* are a key technology for solving this conundrum. They form the "plumbing" for civil IoT projects such as smart grids or smart cities and also have significant implications for the military in the nexus of command, control, communications, computers,

Figure 5

Market share of the top ten sensor companies, 2018, percent



*Top ten companies account for 70% of the overall market
**Top ten companies account for 94% of the overall market

Data: IDC. Illustration: Munich Security Conference

intelligence, surveillance, and reconnaissance. Political decision-makers have been alerted to the centrality of IoT platforms for national security and sovereignty as concerns arise over data platform providers from outside Europe serving European law enforcement agencies.

> With few startups, low investment, and low market share, European companies have yet to carve out a space in the market for IoT platforms.

About one in five – IoT platform startups are based in the EU or the UK. On average, US-based startups receive almost 20 times more investment than those based in the EU or UK.[54] The overall market share of established European companies paints a similar picture. An analysis of the top 20 IoT platform providers shows that vendors from the EU and the UK hold only about a ten percent market share, while US-based providers command more than half of the market.[55] US dominance in this field is another illustration of the speed with which "hyperscalers" such as Amazon Web Services and Microsoft can corner the market on new technological solutions.

Across data gathering and integration, there are several options for strengthening Europe's position. Governments could make more funding available for smart sensors and IoT startups, for example under the new European Innovation Council or similar national programmes, particularly those focused on defense or intelligence use cases, to ensure these capabilities are available from European suppliers and can drive innovation in other applications. Another option for European governments is promoting cooperation between publicly owned companies and European startups in sensor technology and IoT platforms, for example to modernize public infrastructure. Europe could also do more to ensure that European vendors can provide data integration capabilities in the intelligence and security sectors. A good tool to achieve this might be investing in overarching data integration platforms for the military, as large contracts in this space can help build champions equipped to deliver critical IoT platforms.[56]

Data Storage and Processing

Data storage and processing are increasingly linked. Data is stored and processed at the "edge," that is, in individual, connected devices, or in the virtual decentralized space of the cloud. In both cases, processing and storage capacity is driven by continuous advances in the microchips that power all computing devices. *Cloud computing*, the technology for storing and processing data in decentralized cloud structures, is of significant strategic importance. It allows for

"The development of a sovereign European data infrastructure is a key project for the competitiveness and digital innovative strength of our economy and to future-proof jobs in Germany and Europe."[57]

Peter Altmaier, Federal Minister for Economic Affairs and Energy, On the establishment of GAIA-X AISBL, September 15, 2020

easier scale-up, up-to-date security systems, and more flexibility in IT and business applications. Its advantages also make it a prerequisite for more advanced technologies, such as AI applications in civilian and military contexts. Its strategic importance is underscored by the adoption of dedicated cloud strategies, such as the European Commission's Cloud Strategy from 2019 and China's inclusion of cloud computing in the "Internet Plus" component of its Made in China 2025 strategy.[58] Flagship initiatives such as the Franco-German push for a European cloud service called GAIA-X have ignited public debates, but have yet to demonstrate larger-scale innovation potential in practical applications.[59]

No European firm commands a significant share in the technology's development or commercialization.

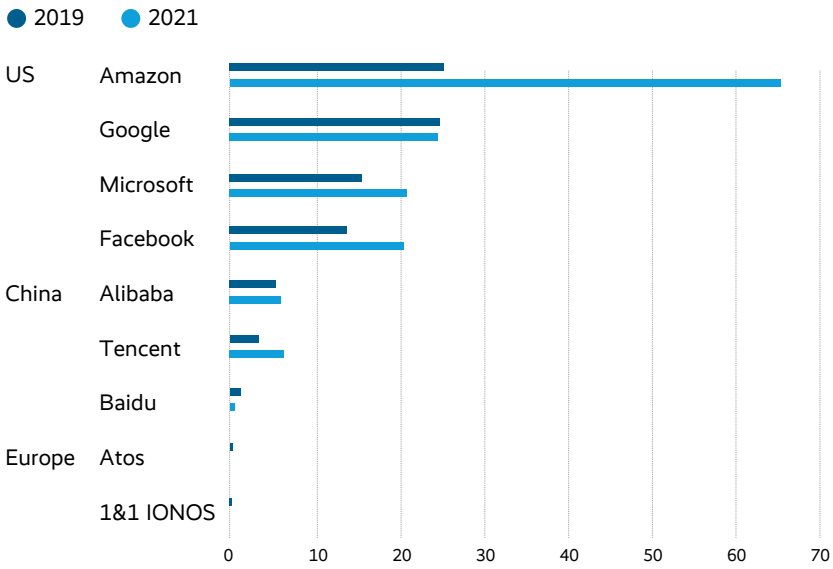
Europe's is struggling to keep up with innovation and development. Five percent of cloud computing patents granted between 2010 and 2020 originated in Europe, compared to about 50 percent in China and 30 percent in the US.[60] The sums invested in cloud computing startups in Europe amount to around one percent of investments in US and Chinese startups.[61]

The barriers preventing European companies from advancing in the cloud computing market are exacerbated by the market dominance of a few huge non-European players, who lead in capital expenditure on cloud services (see Figure 6). In 2019, US-based Amazon Web Services and Microsoft covered nearly two-thirds of the market (see Figure 7). Europe's adoption of cloud computing, while slower, is not too far behind that of China and the US. In other words, many European companies and the public sector rely heavily on US suppliers for cloud-based IT infrastructure – and will do so for many years to come, barring any major changes.

Microchips, or *semiconductors*, are the backbone of all computing in the cloud and individual devices. Newer types of chips are application-specific integrated circuits, such as *AI chips,* optimized to enhance hardware for AI. As these specialized chips become more marketable, they may become the standard for systems across the spectrum of AI use cases. As disruptions in the semiconductor industry have led to a global shortage, chips are increasingly in focus for policymakers.[62] Various investment programs have been launched in recent years, such as the CHIPS for America Act, the Made in China 2025 strategy, EU declarations on strengthening the semiconductor sector, and calls for an alliance of European companies in the context of digital sovereignty.[63] In the recent "U.S.-EU Summit Statement," the transatlantic

Figure 6

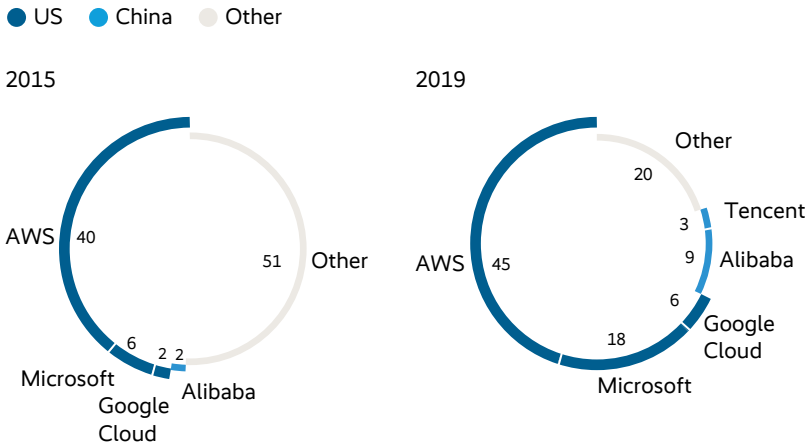
Major companies' capital expenditure on cloud services, 2019 and projection for 2021, USD billions



Data: Company reports from DB Research. Illustration: Munich Security Conference

Figure 7

Global infrastructure as a service market share,* 2015 and 2019, percent



*For Infrastructure-as-a-Service only

Data: Statista. Illustration: Munich Security Conference

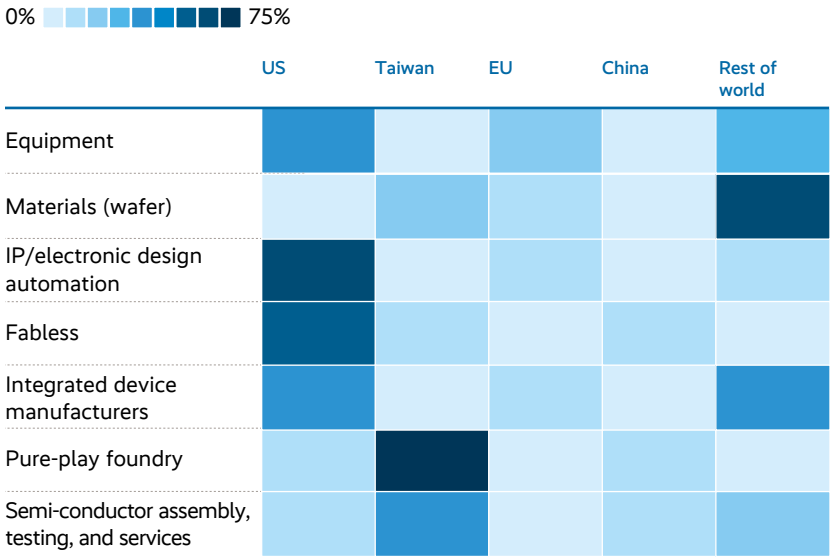
partners declared semiconductors a shared priority, aiming to "rebalance global supply chains [...] with a view to enhancing U.S. and EU respective security of supply as well as capacity to design and produce the most powerful and resource efficient semiconductors."[64]

Europe commands a notable share of almost all steps of the semiconductor value chain.

The semiconductor industry is highly specialized and geographically dispersed. US companies are represented across the board, but companies around the world, including UK-based ARM Holdings and Dutch ASML, also occupy important "choke points."[65] China, meanwhile, lacks several capabilities in design and equipment.[66] While European companies have a presence in every section of the market (see Figure 8), particularly in domains such as in larger automotive chips, Europe's design and production capacity is decreasing.[67] And when it comes to the commercialization of specialized chips, Europe's market share could drop if investments in startups are an

Figure 8

Share of sales in the semiconductor value chain by region,* 2018, percent



*Regional market share figures have been selectively adjusted to reflect market presence of very small suppliers.
Data: Analysis based on Omdia, Capital IQ data and expert interviews. Illustration: Munich Security Conference

indication: US and Chinese AI chip startups received the lion's share of investment from 2015 to 2020 – around 1.5 billion US dollars in each country, compared to only about 100 million for European startups.[68]

With regard to cloud computing, Europe should consider promoting or protecting existing homegrown capabilities that are otherwise at risk of being made obsolete by foreign market leaders. Governments could continue to invest in large-scale projects such as GAIA-X to make inroads into the cloud market – even though the analysis suggests that there is no real alternative to incorporating US hyperscalers into GAIA-X - and, as computing becomes increasingly decentralized, focus on promoting the development and deployment of edge computing capabilities as envisioned by the EU's Digital Compass. In addition to local hosting, GAIA-X could focus more closely on security in the hardware supply chain.[70]

A major question is whether Europe should invest to close the gap to the cutting edge of semiconductors. An alternative could be focusing on a growth sector such as AI-specific chips, a market projected to double in size between 2020 and 2025.[69]

Europe could preserve its manufacturing capabilities in the chip value chain by creating more favorable conditions in the European market and regulating foreign takeovers.[71] Europe could specifically focus on promoting new cutting-edge (AI) chip design – including in fabless companies, R&D, and startups.[72] Europe could also direct funding to support development under open chip design standards such as RISC-V. Promoting this could loosen European companies' reliance on established players,[73] but efforts should be coordinated with the US, which is concerned that China will have more independence under open standards.[74]

Analytics and AI

Analytics and AI are algorithmic and statistical tools used to generate insights or trigger actions based on data. AI is a general-purpose technology with many different domain-specific applications and thus has disruptive potential as far-reaching as that of electricity.[76] AI is already on the verge of disrupting businesses and societies, questioning existing ways of operating, and paving the way for new business models. Investment in AI has grown exponentially in recent years. For Europe, the opportunity is immense: If Europe were to scale up AI investments, it could add up to 2.7 trillion euros to its combined GDP until 2030. If Europe improves on its assets and competencies sufficiently to catch up with the US' AI frontier, the potential could be even higher. GDP

"Where we are today with AI is that we judge America still ahead, but China [is] investing very heavily and likely to catch up very soon. We don't say what soon is, but my personal opinion, it is a few years, not five years."[75]

Eric Schmidt, Chair of the National Security Commission on Artificial Intelligence, CBS News, April 21, 2021

growth could accelerate by another 0.5 points a year, adding an extra 900 billion euros to GDP and bringing the total potential "AI boost" to 3.6 trillion euros by 2030.[78] AI has many military use cases, from predictive maintenance to creating new AI-enabled command and control chains.[78] Not surprisingly, many governments see AI as a strategic priority. The final report of the US National Security Commission on Artificial Intelligence notes the substantial challenge that AI poses to US technological leadership.[79] European and Chinese policymakers have published AI strategies with a similar tone.[80]

Europe has seen some success in lower-complexity AI use cases, such as medical imaging, while more complex applications could prove challenging.

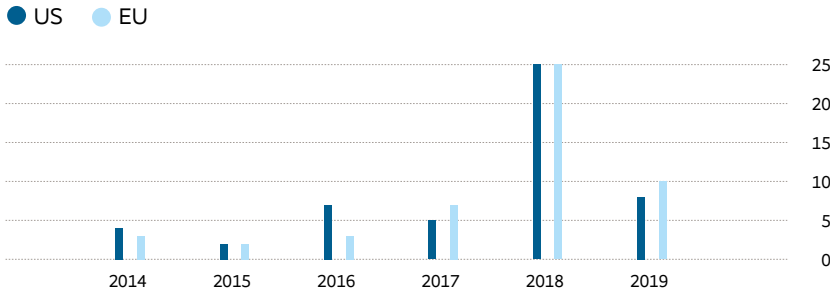
It is difficult to pin down Europe's position in AI, given the technology's wide applicability. Two distinct applications can serve as analytical lenses: AI in healthcare with a focus on medical imaging, and autonomous driving.

Medical imaging is a key area for AI applications.[81] In this field, US companies in the global medical imaging market had a share of 50 percent in 2019, while Europe captured 23 percent.[82] Adoption rates have been low and slow to grow, but this is set to change as the technology advances and the market matures. European regulators have been on par with the US in approving medical imaging applications for AI (see Figure 9). When it comes to AI applications in the healthcare system more broadly, Europe has relatively few startups and little investment in this space: only 17 AI startups in healthcare were based in the EU or the UK in 2020, compared with 26 in the US and 57 in China. On average, EU and UK startups received an average investment of just 7 million US dollars from 2015 to 2020, compared with 16.7 million US dollars in the US, and 5.4 million US dollars in China.[83]

The impact of AI is likely to be especially pronounced in *individual mobility*. Research suggests that roughly 65 percent of vehicles sold in Europe could be fully or partially automated by 2030.[84] Technology that harnesses AI for autonomous driving will have direct applications in the military, for example by reducing the number of soldiers needed to run a convoy,[85] and can serve as a proxy for capabilities in the broader space of autonomous systems. Europe has a low number of autonomous driving startups and they have only completed the early stages of funding (see Figure 10). Europe is home to only three of the top 20 companies in terms of "autonomous miles between disengagements" – a key metric that shows how far autonomous vehicles can travel without human intervention.[86]

Figure 9

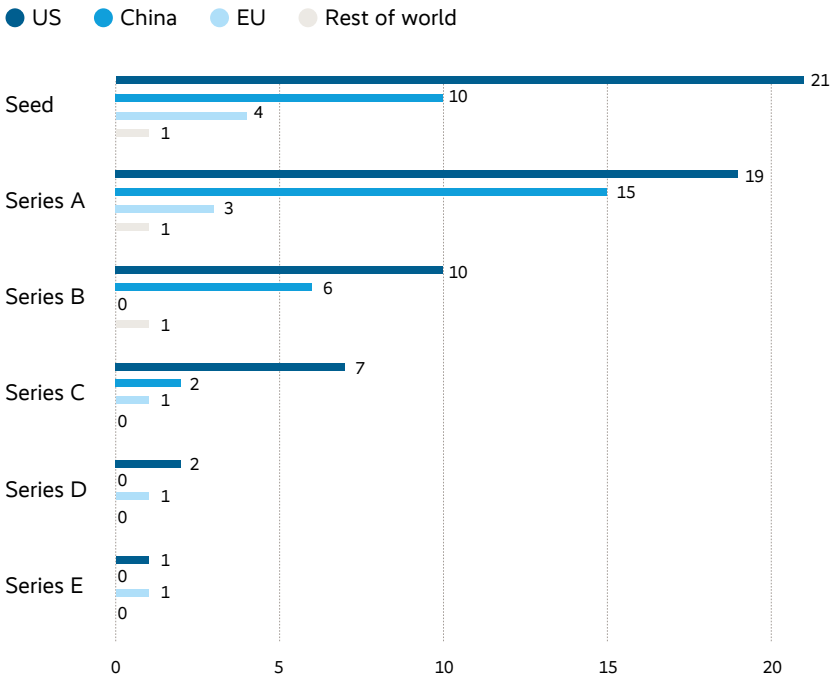
Medical imaging AI applications approved by regulators, 2014–19,* number of applications*



*Regulatory approval data as of 07/2019; rounding errors occur
Data: Signify Research. Illustration: Munich Security Conference

Figure 10

Startups active in the autonomous vehicle space by geography and funding round, 2020,* number



* Data retreived in November 2020, has not been reviewed by PitchBook analyst.
Data: PitchBook Inc. Illustration: Munich Security Conference

Europe has a chance to lead in AI, which is critical in defense and intelligence. AI on the edge and in the cloud will allow leaders in those technologies to create entirely new ways of connecting many more, much more decentralized systems into a large AI enabled command and control system. As such, total spending on AI just in the Pentagon's budget is already approaching one billion US dollars this year alone – with year-on-year growth of around 50 percent in that category.[87] Policymakers have a range of options to strengthen Europe's position. They could direct more funding for innovation in national security and defense toward complex AI applications to strengthen the startup ecosystem in this field. Particularly in R&D and new technology development programs, such spending could be allocated to AI technology development to ensure that Europe can make sovereign decisions over how such uses of AI align with its values, as defined in the recent proposal for a regulation on AI, for example.[88] What is more, investing in expanding the use of AI in the public sector more broadly would provide growth opportunities in the wider AI ecosystem.[89] Data is the key ingredient in AI applications. To help European suppliers create complex AI applications that are interoperable across member states' militaries, European policymakers could build on the standardization and cooperation in physical military mobility to enable the mobility of data between European defense organizations as well as defense suppliers.[90]

Cybersecurity

Cyberattacks and cybercrime are increasing worldwide.[91] The former head of the US Justice Department's national security division called 2020 "the worst year ever when it comes to ransomware and related extortion events."[92] Many attacks are directed at critical infrastructure but also at government agencies – making the "age of perpetual cyberconflict" a major national security challenge.[93] Cooperation on cybersecurity has long been a priority of the transatlantic partnership – most recently reemphasized in the "US-EU Summit Statement."[94] The EU's position in cybersecurity and a detailed perspective on two specific technologies – encryption and identity and access management – that are central in the military's use of data can shed more light on Europe's standing.[95]

In cybersecurity, Europe has strengths across important technologies as well as throughout development, commercialization, and adoption.

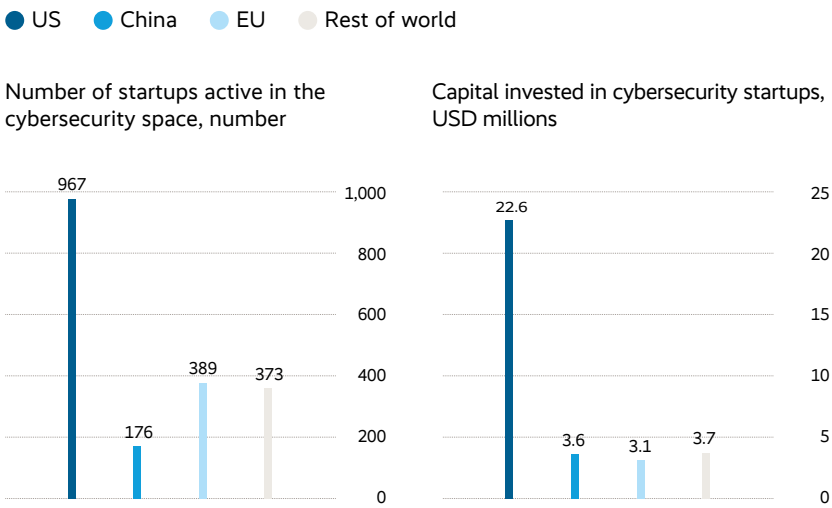
The growing relevance of cybersecurity is reflected by a growing industry, as the cybersecurity market has been growing at about ten percent per year.[96] The US leads in the development of cybersecurity technology in terms of the number of startups and the capital invested in them (see Figure 11). Europe has a 20 percent share of global cybersecurity startups.

The picture is similar in *encryption*, a foundation of cybersecurity. It allows for the secure endpoint transfer of data and thus enables secure communication – critical in a wide range of military contexts, such as a recent US army effort to secure communication with unmanned aircraft systems.[97] Three times more cryptography patents are filed in the US and five times more are filed in China than in the EU and the UK combined.[98] Commercialization seems to follow this pattern: US startups received an average of around 200 million to 240 million US dollars between 2015 and 2020, compared to 40 million to 50 million US dollars in Europe. Chinese companies, however, only received five million to 15 million US dollars in this time period.[99]

This is also reflected by key indicators regarding another technology: *access and identity management*. Across development, commercialization, and adoption, the US is leading. US startups received on average around 70 million

Figure 11

Estimated cybersecurity startups and funding by region, 2020*



*Data retreived in November 2020, has not been reviewed by PitchBook analyst.

Data: PitchBook Inc. Illustration: Munich Security Conference

"We are now witnessing the fourth wave of innovation, the deep tech, this frontier between science and innovation – Europe is a leader in science, it's time to be a leader in innovation. And we have all the assets for that."

Mariya Gabriel, European Commissioner for Innovation, Research, Culture, Education and Youth, MSC Technology Roundtable, July 6, 2021

"Digital Sovereignty means that we in Europe can make sure that our values and principles are respected by companies that can come from all over the world, but we have our unique elements of legislation in Europe."

Andreas Schwab, Member of the European Parliament, MSC Technology Roundtable, July 6, 2021

US dollars each over the past five years, compared to roughly 25 million US dollars for Chinese startups and only seven million US dollars for European startups.[100] Companies in the US command about 70 percent of the overall market in identity management and digital trust software, with a domestic market twice the size of Europe's.[101]

Europe should take steps to strengthen its positions in development, commercialization, and adoption. Member states could strengthen the cybersecurity ecosystem by doubling down on efforts to strengthen the security of European military organizations and their suppliers. They could own and operate their own cryptographic keys on a national or EU level, strengthening cooperation between encryption researchers and users in security and defense. And by harmonizing identity and access management across the continent, European countries could foster an ecosystem to help them use interoperable standards.

A Path to Digital Sovereignty in Service of Security

This analysis reveals a picture with many nuances. Europe has its strengths in terms of available capital – human and financial. Its competitiveness varies by technology maturity and relative use – from development over commercialization to widespread adoption.

Most definitively, the analysis reveals a need for action on the supply side of digital capabilities. Europe needs more domestic tech companies in all capability areas. This is especially true where the strength of European legacy companies could wane if the pace of innovation, commercialization, and adoption remains too slow. Europe's traditional strengths in manufacturing will not save the day if hardware becomes increasingly commoditized while software emerges as an increasingly differentiating capability factor. Failing to address these risks now could mean more difficult decisions down the road as dependencies grow. Europe may not find suitable domestic providers of critical technology solutions and may not have a wide range of trusted partners or suppliers to choose from, with substantial implications for its security.

These challenges present risks to the common digital agenda of the transatlantic partnership: if the US and the EU are "to drive digital transformation that spurs trade and investment, strengthens our technological and industrial leadership, boosts innovation, and protects and promotes critical and emerging technologies and infrastructure," as put forward in the June 2021 US-EU Summit Statement, only a strong Europe will be able to contribute

"In the European Union, we are good at regulating our playground and influencing other playgrounds. But that's not enough. We want to see our homegrown companies take root, grow, and prosper into global leaders."[13]

Charles Michel, President of the European Council, Masters of Digital 2021 Event, February 3, 2021

meaningfully.[102] It is in the partnership's interest that Europe remains capable of building its own secure supply chains, achieving data interoperability in intelligence, cooperating in cybersecurity, and enabling joint NATO military operations. The partnership will be stronger if Europe can continue to develop technology, improve governance, and define its own alignment of technology applications with European values. Europe's partners around the world should recognize that a Europe that is better equipped to meet the challenges posed by technology will be a more reliable and capable partner.

Many regulatory priorities of the EU could already contribute to strengthening the digital capabilities of Europe. Most notably, this includes the completion of the Digital Single Market, but also transatlantic efforts such as cooperation on strengthening legal certainty in transatlantic flows of data. Still, there is a need to develop ambitious, targeted interventions as laid out above, such as accelerating the rollout of 5G through faster spectrum auctions, increasing investment in military sensors, or building better European data sharing for the development of military AI. These interventions should be based on a clear understanding of critical technologies and risks as well as a willingness to cooperate to pursue strategic priorities. What is more, European policymakers should act swiftly. The acceleration of technological progress requires that decision-making on the European level matches this speed.

Europe is strong in many areas, such as in innovation, as measured in terms of patents and startups, but it could do more in helping build new companies that have the capability to deliver on the technology side. Policymakers should turn their attention toward designing incentives for the creation and scaling up of innovative companies that can take the existing input factors – research, talent, and capital – and turn them into real capabilities. The role of the EU and European national governments could be more so to define the broad areas of need and create relevant incentives for European companies to deliver innovative solutions, using the large-scale funding available in the post-Covid-19 recovery programs. The European Commission has already taken a bold step in that direction through the program Next Generation EU, which explicitly earmarks at least 20% of its 750 billion Euro recovery funds for projects supporting Europe's digital transition. Now it is critical, that these resources are used strategically. The instruments for doing so are well established and range from competitions to targeted technology development programs.

To avoid developing technology without specific applications, the security sector can act as a catalyst for innovation through existing and future multinational and European security programs, where more cooperation can create larger scale through joint procurement or data sharing, most notably the European Defense Fund. Further acceleration of European innovation could be achieved by shifting defense budgets from legacy systems towards innovative technologies. Europe should harness common projects in the areas of space, intelligence, and defense to galvanize a new generation of technology entrepreneurs who work to close the much-talked-about gap between research and commercialization and scaling.

Many pressing dependencies in military contexts could be addressed by shifting resources and attention to weaknesses and potential future choke points, catalyzing growth in other areas. European countries can use their combined weight by pooling technology procurement, incentivizing cooperation among European companies, and sharing data. Across a range of technologies, Europe should take bolder steps, such as investing in a European LEO satellite constellation or similar programs for each of the capability areas named in this report.

In today's increasingly connected world, domestic digital capabilities are a worthy goal. But cooperation will remain crucial. Sustainable prosperity and security will not be possible without trustworthy and capable technological partners.

Key Points

1. Europe has made progress in regulating the demand side of digital technology – how technology is procured and used - and is determined to further strengthen its digital competitiveness.

2. Europe clearly has its technological strengths, but its competitiveness varies by technology and the stage of the innovation funnel. There is a significant opportunity for targeted interventions that ensure Europe's core capabilities in the future.

3. If the challenges persist and Europe's position weakens, transatlantic security and the common digital agenda of the transatlantic partnership could be at risk.

4. To strengthen European digital sovereignty, policy makers should turn their attention towards designing incentives for the creation and scaling up of innovative companies. The instruments for doing so are well established and range from competitions to targeted technology development programs.

5. The security sector can act as a catalyst for innovation through multinational and European security programs. In this context, Europe would profit from ambitious common projects in the area of space, intelligence, and defense.

Endnotes

1 Simon Pfeiffer and Randolf Carr, "Error 404 – Trust Not Found: A European Survey on Digital (Dis)trust," Munich: Munich Security Conference, Munich Security Brief 2, March 2021, doi:10.47342/REFQ1817.
2 Pfeiffer and Carr, "Error 404 – Trust Not Found: A European Survey on Digital (Dis)trust."
3 Emmanuel Macron, "Speech of the President of the Republic on the Defense and Deterrence Strategy," Paris, February 7, 2020, https://perma.cc/QA9W-W2TF.
4 Tobias Bunde et al., "Munich Security Report 2021: Between States of Matter – Competition and Cooperation," Munich: Munich Security Conference, June 2021, doi:10.47342/CYPE1056, 94.
5 Pfeiffer and Carr, "Error 404 – Trust Not Found: A European Survey on Digital (Dis)trust," 11.
6 Pfeiffer and Carr, "Error 404 – Trust Not Found: A European Survey on Digital (Dis)trust," 8.
7 See European Commission, "Shaping Europe's Digital Future," Brussels: European Commission, February, 2020, https://perma.cc/5S49-48CU; Presidency of the Council of the European Union, "Expanding the EU's Digital Sovereignty," Brussels/Berlin: Presidency of the Council of the European Union, 2020, https://perma.cc/9RNQ-GSC8.
8 Resa M. Kar and Basanta E. P. Thapa, "Digitale Souveränität als Strategische Autonomie: Umgang mit Abhängigkeiten im digitalen Staat," Berlin: Kompetenzzentrum Öffentliche IT, September 2020, https://perma.cc/Q33V-RZ2D.
9 Zora Siebert, "Digital Sovereignty – The EU in a Contest for Influence and Leadership," Berlin: Heinrich Böll Foundation, Background, February 10, 2021, https://perma.cc/Q2J7-4MVV.
10 Ann C. Riedel, "Datenschutz: Den ritualisierten Debatten entkommen," Potsdam: Friedrich Naumann Foundation, January 28, 2021, https://perma.cc/HJ43-F8FL; also see European Commission, "Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition – Two Years of Application of the General Data Protection Regulation," Brussels: European Commission, June 24, 2020, https://perma.cc/T92P-MDJT.
11 European Commission, "A European Strategy for Data: Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions," Brussels: European Commission, February 2020, https://perma.cc/K7PG-U8MN.
12 European Commission, "Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)," Brussels: European Commission, April 21, 2021, https://perma.cc/KBH3-ZBPJ; Mark MacCarthy and Kenneth Propp, "Machines Learn That Brussels Writes the Rules: The EU's New AI Regulation," Washington, DC: Brookings Institution, May 4, 2021, https://perma.cc/NLX5-XFW3.
13 Charles Michel, "Digital Sovereignty is Central to European Strategic Autonomy: Speech by President Charles Michel at 'Masters of Digital 2021' Online Event," Brussels: European Council, February 3, 2021, https://perma.cc/6M4C-3T29.
14 Thierry Breton, "Speech by Commissioner Thierry Breton at Hannover Messe Digital Days," Hannover: Europe-

an Commission, 2020, https://perma.cc/G33Z-755F.

15 European Commission, "Europe's Digital Decade: Digital Targets for 2030," Brussels: European Commission, March 9, 2021, https://perma.cc/P2YZ-44PA.

16 Ursula von der Leyen, "Keynote Speech by President von der Leyen at the 'Masters of Digital 2021' Event," Brussels: DIGITALEUROPE, February 4, 2021, https://perma.cc/DTH9-EXTJ.

17 Tyson Barker and Marietje Schaake, "Democratic Source Code for a New U.S.-EU Tech Alliance," Berlin: DGAP, November 24, 2020, https://perma.cc/BY4K-VR8W.

18 The White House, "U.S.-EU Summit Statement: Towards a Renewed Transatlantic Partnership," Press Release, June 15, 2021, https://perma.cc/5X9B-5V4Q; Joseph R. Biden, "Remarks by President Biden at the 2021 Virtual Munich Security Conference," Washington, DC/Munich: Munich Security Conference, February 19, 2021, https://perma.cc/C7K8-W7VM.

19 On these issues, see Mark Scott and Laruens Cerulus, "EU-US 'Tech Alliance' Faces Major Obstacles on Tax, Digital Rules," *Politico,* December 2, 2020, https://perma.cc/TWK3-8MET; Kati Suominen, "On the Rise: Europe's Competition Policy Challenges to Technology Companies," Washington, DC: CSIS, October 26, 2020, https://perma.cc/93K9-N3TX; Jonathan Keane, "With Biden in the White House, EU Officials Are Pushing Hard for a New Data-sharing Pact with the US," *CNBC,* April 19, 2021, https://perma.cc/T3M7-LVE8.

20 See Taisei Hoyama and Yu Nakamura, "US and Allies to Build 'China-free' Tech Supply Chain," Nikkei Asia, February 24, 2021, https://perma.cc/WW8M-WR5H; Robbie Gramer, "Trump Turning More Countries in Europe Against Huawei," *Foreign Policy,* October 27, 2020, https://perma.cc/J3X9-TRWZ; National Security Commission on Artificial Intelligence, "Final Report," Washington, DC: National Security Commission on Artificial Intelligence, March 1, 2021, https://perma.cc/27VD-3JMG; Julia Schuetze, "EU-US Cybersecurity Policy Coming Together: Recommendations for Instruments to Accomplish Joint Strategic Goals," Berlin: Stiftung Neue Verantwortung, November 2020, https://perma.cc/82LH-GR4S.

21 National Security Commission on Artificial Intelligence, "Final Report."

22 Jens Stoltenberg, "Opening Remarks by NATO Secretary General Jens Stoltenberg at the Munich Security Conference," Munich/Brussels: Munich Security Conference/NATO, February 15, 2020, https://perma.cc/V4G8-WFMK.

23 Isabel Skierka, "Stellungnahme bzgl. Fragenkatalog Anhörung des Ausschusses Digitale Agenda zum Thema 'IT-Sicherheit von Hard- und Software als Voraussetzung für Digitale Souveränität' am 11. Dezember 2019," Berlin: German Bundestag, Digital Society Institute Berlin, ESMT Berlin, December 10, 2019, https://perma.cc/C8RE-UGE3.

24 Justin Sherman, "The US-China Battle Over the Internet Goes Under the Sea," *WIRED,* June 24, 2020, https://perma.cc/HM58-UY3Q; Robert Williams, "Securing 5G Networks," New York City: Council on Foreign Relations, July 15, 2019, https://perma.cc/7VVL-JRUG; "Large LEO Satellite Constellations: Will it be Different This Time?," New York City: McKinsey & Company, May 4, 2020, https://perma.cc/T4X6-SAX5; European Parliament Policy Department for External Relations, "The European Space Sector as an Enabler of EU Strategic Autonomy," Brussels: European Parliament Policy

Department for External Relations, December 2020, https://perma.cc/ZM8C-KQ4Z.
25 Jan-Peter Kleinhans, "5G vs. National Security: A European Perspective," Berlin: Stiftung Neue Verantwortung, February 2019, https://perma.cc/C82M-78YA.
26 "The 5G Era: New Horizons for Advanced Electronics and Industrial Companies," Munich: McKinsey & Company, January 2020, https://perma.cc/LT9S-PGHZ.
27 John Hoehn and Kelley Sayler, "National Security Implications of Fifth Generation (5G) Mobile Technologies," Washington, DC: Congressional Research Service, In Focus, April 23, 2021, https://perma.cc/C3LQ-E23S.
28 Gramer, "Trump Turning More Countries in Europe Against Huawei"; Kleinhans, "5G vs. National Security."
29 Number of members as of December 2020. David Fidler, "The Clean Network Program: Digital Age Echoes of the 'Long Telegram'?," New York City: Council on Foreign Relations, October 5, 2020, https://perma.cc/JG8L-V6BT.
30 Foo Y. Chee, "EU Countries Must Urgently Diversify 5G Suppliers, Commission Says," *Reuters,* July 24, 2020.
31 Jouni Forsman et al., "Market Share: Communications Service Provider Operational Technology, Worldwide, 2020," Stamford: Gartner, June 3, 2021, (Calculations performed by McKinsey).
32 Keyword-based analysis using data from Innography, data retrieved in November 2020. Innography is a trademark of Clarivate and its affiliated companies.
33 Keyword-based analysis using data from Pitchbook Inc., data retrieved in November 2020 , has not been reviewed by PitchBook analysts.
34 Analysis using data from Analysys Mason DataHub, data retrieved in June 2021.
35 Andrew Eversden, "How Commercial Satellite Constellations Fit into the Army's Future Tactical Network Designs," *C4ISR.NET,* May 6, 2021, https://perma.cc/RW2R-8HQT.
36 Thomas Seal and Greg Ritchie, "Why Low-Earth Orbit Satellites Are the New Space Race," *The Washington Post,* July 11, 2020, https://perma.cc/92Z9-39SR.
37 Jonathan Amos, "EU Must 'Move at Speed' on Space Broadband Network," *BBC,* January 12, 2021, https://perma.cc/JR8E-LXR3.
38 Jonathan Amos, "UK Government Takes £400m Stake in Satellite Firm OneWeb," *BBC,* July 3, 2020, https://perma.cc/FJ78-M9Z9.
39 Keyword-based analysis using data from Innography, data retrieved in November 2020. Innography is a trademark of Clarivate and its affiliated companies.
40 Daniel Voelsen, "Internet from Space: How New Satellite Connections Could Affect Global Internet Governance," Berlin: Stiftung Wissenschaft und Politik, SWP Research Paper 3, April 3, 2021, doi:10.18449/2021RP03.
41 Laurens Cerulus, "Berlin's €2B Plan to Wean Off Huawei (Nokia and Ericsson too)," *Politico Europe,* February 2, 2021, https://perma.cc/MCP9-2FKD.
42 Beryl Thomas, "Why Germany's Investment in Open RAN Will not Solve its 5G Problem," Brussels: ECFR, April 6, 2021, https://perma.cc/47QW-VP3S.
43 U.S. Department of Defense, "Department of Defense and Department of Commerce Explore 5G Challenge to Develop Open 5G Systems," Press Release, January 11, 2021, https://perma.cc/6B8D-J52M.

44 Samuel Stolton, "Commission 'Disappointed' with 5G Delays in Europe; Reminds Nations of 'Legal Obligation'," Euractiv, November 18, 2020, https://perma.cc/E68K-NF9B.
45 arcep, "New Deal for Mobile: 900 MHz, 1800 MHz and 2.1 GHz Frequency Band Allocation Results," Press Release, October 25, 2018, https://perma.cc/7U9R-QYEW; Morris Lore, "Finland's High-Speed, Low-Cost 5G Auctions Send Message to Europe," *LightReading,* June 9, 2020, https://perma.cc/Z67P-YDGA.
46 Jason Rainbow, "Europe Making Progress on Sovereign LEO Constellation as OneWeb and Starlink Race Ahead," *SpaceNews,* May 20, 2021, https://perma.cc/S4FU-GP5D.
47 Alix Paultre, "Drones, Electronic Warfare, and Advanced Sensor Integration," *Evaluation Engineering,* May 27, 2020, https://perma.cc/23J6-H8D5.
48 Jost Wübbeke et al., "Made in China 2025: The Making of a High-Tech Superpower and Consequences for Industrial Countries," Berlin: Merics, Merics Papers on China 2, December 2016, https://perma.cc/M8DQ-ATJJ, 40.
49 Luca A. Remotti et al., "Study on Mapping Internet of Things Innovation Clusters in Europe," Brussels: European Commission, 2019, doi:10.2759/91028.
50 IDC, "Worldwide Sensor Market Shares, 2018: Advanced Applications and Increased Resolutions Expanding Opportunities," Needham: IDC, May 2019, https://perma.cc/PN35-FPA8. "Traditional sensors" include pressure, temperature, or flow sensors; the optical sensors market, which is dominated by Japan, Korea, and Taiwan, is excluded.
51 IDC, "Worldwide Internet of Things Spending Guide," Needham: IDC, 2021, https://perma.cc/9FEW-TRNA.
52 Keyword-based analysis using data from Innography, data retrieved in November 2020. Innography is a trademark of Clarivate and its affiliated companies.
53 Keyword-based analysis using data from Pitchbook Inc., data retrieved in November 2020, has not been reviewed by PitchBook analysts.
54 Keyword-based analysis using data from Pitchbook Inc., data retrieved in November 2020, has not been reviewed by PitchBook analysts.
55 Knud L. Lueth, "IoT Platform Competitive Landscape & Database 2020," Hamburg: IoT Analytics, December 2019, https://perma.cc/YB7D-7T8Z.
56 Vivienne Machi, "Thales, Atos Take on Big Data and Artificial Intelligence in New Joint Venture," *DefenseNews,* May 28, 2021, https://perma.cc/EYZ8-KWQT.
57 Federal Ministry for Economic Affairs and Energy, "Bundesminister Altmaier zur Gründung der GAIA-X AISBL," Press Release, September 15, 2020, https://perma.cc/ND8E-4CJF.
58 European Commission, "The European Commission Cloud Strategy," Brussels: European Commission, May 16, 2019, https://perma.cc/5L2J-EV2Q; Lehman-Brown, "Made In China 2025 & Internet Plus: The 4th Industrial Revolution: Opportunities for Foreign Invested Enterprises in China," Beijing: Lehman-Brown, August 2016, https://perma.cc/Y2DP-TRJ2.
59 Janosch Delcker and Melissa Heikkilä, "Germany, France Launch Gaia-X Platform in Bid for 'Tech Sovereignty'," *Politico,* June 7, 2020, https://perma.cc/FDS6-EDZP.
60 Keyword-based analysis using data from Innography, data retrieved in November 2020. Innography is a trademark of Clarivate and its affiliated companies.

61 Keyword-based analysis using data from Pitchbook Inc., data retrieved in November 2020, has not been reviewed by PitchBook analysts.
62 David Dollar and Don Clark, "What's Behind the Semiconductor Shortage and How Long Could It Last?," Washington, DC: Brookings Institution, May 24, 2021, https://perma.cc/U4NF-8A3K.
63 Library of Congress, "H.R.7178 - CHIPS for America Act," Washington, DC: Library of Congress, November 6, 2020, https://perma.cc/YJ3D-FLQV; James A. Lewis, "Learning the Superior Techniques of the Barbarians: China's Pursuit of Semiconductor Independence," Washington, DC: CSIS, China Innovation Policy Series, January 2019, https://perma.cc/5LJ5-N8UN; Thierry Breton, "Speech by Commissioner Thierry Breton at Hannover Messe Digital Days," Hannover: Hannover Messe, https://perma.cc/G33Z-755F.
64 The White House, "U.S.-EU Summit Statement."
65 Jan-Peter Kleinhans and Nurzat Baisakova, "The Global Semiconductor Value Chain: A Technology Primer for Policy Makers," Berlin: Stiftung Neue Verantwortung, October 2020, https://perma.cc/U26B-MPCQ.
66 Paul Triolo and Kevin Allison, "The Geopolitics of Semiconductors," New York: Eurasia Group, September 2020, https://perma.cc/5NKR-9J8M.
67 Kleinhans and Baisakova, "The Global Semiconductor Value Chain."
68 Keyword-based analysis using data from Pitchbook Inc., data retrieved in November 2020, has not been reviewed by PitchBook analysts.
69 "Artificial-Intelligence Hardware: New Opportunities for Semiconductor Companies," New York City: McKinsey & Company, January 2, 2019, https://perma.cc/7KK7-Y4MR.
70 Christof Kerkmann, Moritz Koch, and Stephan Scheuer, "Server-Hardware: Der blinde Fleck von Gaia-X," *Handelsblatt,* July 14, 2020, https://perma.cc/8WFF-RHD4.
71 Kaan Sahin and Tyson Barker, "Europe's Capacity to Act in the Global Tech Race," Berlin: DGAP, Report 6, April, 2021, https://perma.cc/MG8J-LU9E, 30.
72 Jan-Peter Kleinhans, "The Lack of Semiconductor Manufacturing in Europe: Why the 2nm Fab is a Bad Investment.," Berlin: Stiftung Neue Verantwortung, April 2021, https://perma.cc/Q62P-R9NX, 2f; Jan-Peter Kleinhans et al., "Who Is Developing the Chips of the Future?," Berlin: Stiftung Neue Verantwortung, June 16, 2021, https://perma.cc/8JJZ-U4U8.
73 Sahin and Barker, "Europe's Capacity to Act in the Global Tech Race," 30.
74 Caroline Meinhardt, "Open Source of Trouble: China's Efforts to Decouple from Foreign IT Technologies," Berlin: Merics, May 18, 2020, https://perma.cc/CS96-JYT6.
75 Eric Schmidt, "Tech Giant Eric Schmidt Warns China is Catching up to U.S. in AI," *CBS News,* April 21, 2021, https://perma.cc/QYY4-WEH5.
76 National Security Commission on Artificial Intelligence, "Final Report," 20.
77 "Notes from the AI Frontier: Tackling Europe's Gap in Digital and AI," n.a.: McKinsey Global Institute, Discussion Paper, Feburary 2019, https://perma.cc/SCX8-VX6S.
78 Robyn Dixon, "Azerbaijan's Drones Owned the Battlefield in Nagorno-Karabakh — and Showed Future of Warfare," *The Washington Post,* November 11, 2020, https://perma.cc/8FG5-MGHA; Teresa Hitchens, "Air Force Expands AI-Based Predictive Maintenance," *Breaking Defense,* July 9, 2020, https://perma.cc/T3RC-KDF3.

79 National Security Commission on Artificial Intelligence, "Final Report," 19.
80 European Commission, "Artificial Intelligence for Europe," Brussels: European Commission, April 25, 2018, https://perma.cc/56ZN-3TY7.
81 Alan Alexander et al., "An Intelligent Future for Medical Imaging: A Market Outlook on Artificial Intelligence for Medical Imaging," *Journal of the American College of Radiology 17:1 Pt B (2020),* 165–170, doi:10.1016/j.jacr.2019.07.019.
82 technavio, "Artificial Intelligence (AI) Market in Healthcare Sector by Application and Geography - Forecast and Analysis 2019-2023," Toronto: technavio, August 2019, https://perma.cc/JZC3-S75M.
83 Keyword-based analysis using data from Pitchbook Inc., data retrieved in November 2020, has not been reviewed by PitchBook analysts.
84 "Private autonomous vehicles: The other side of the robo-taxi story," New York City: McKinsey & Company, December 1, 2020, https://perma.cc/N2GM-URG8.
85 RAND Corporation, "Autonomous Vehicle Technology May Improve Safety for U.S. Army Convoys," Santa Monica: RAND Corporation, February 12, 2020, https://perma.cc/HV9L-F3X5.
86 State of California - Department of Motor Verhicles, "2020 Autonomous Vehicle Disengagement Reports," Los Angeles: State of California - Department of Motor Verhicles, 2020, https://perma.cc/VBC4-CQXW.
87 John Keller, "Pentagon to Spend $874 million on Artificial Intelligence (AI) and Machine Learning Technologies Next Year," *Military & Aerospace Electronics,* June 4, 2021, https://perma.cc/MEH4-VP2S.
88 European Commission, "Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)."
89 Gianluca Misuraca, "Overview of the Use and Impact of AI in Public Services in the EU," Luxembourg: Publications Office of the European Union, 2020, doi:10.2760/039619.
90 Christian Brandlhuber and Heiko Borchert, "Jump-Starting Europe's Work on Military Artificial Intelligence," *DefenseNews,* September 8, 2019, https://perma.cc/6CUV-GB3N.
91 "US Army to Improve Encryption of Drone Communications," *TheDefense-Post,* October 19, 2020, https://perma.cc/BJ5A-VH7T.
92 Dustin Volz, "Ransomware Targeted by New Justice Department Task Force," *The Wall Street Journal,* April 21, 2021, https://perma.cc/6XP9-466E.
93 Stephen Collinson, "Ransomware Attacks Saddle Biden With Grave National Security Crisis," *CNN,* June 7, 2021, https://perma.cc/J6PS-5G7G; "U.S. Government and Aid Agencies Targeted By Cyberattack Attributed to Russia by Microsoft," *euronews,* May 29, 2021, https://perma.cc/DLE2-AELW; Paul R. Kolbe, "With Hacking, the United States Needs to Stop Playing the Victim," *The New York Times,* December 23, 2020, https://perma.cc/U7EX-L4KA.
94 The White House, "U.S.-EU Summit Statement."
95 Robert Williams, "DOD's Data Decrees Aim to Preserve Military's Advantage," *GCN,* May 12, 2021, https://perma.cc/22EJ-BJXK.
96 IDC, "Worldwide Semiannual Software Tracker: Final Historical," Needham: IDC, H1 2020, https://perma.cc/H27Z-3EMM.

97 "US Army to Improve Encryption of Drone Communications," *TheDefensePost*.
98 Keyword-based analysis using data from Innography, data retrieved in November 2020. Innography is a trademark of Clarivate and its affiliated companies.
99 Keyword-based analysis using data from Pitchbook Inc., data retrieved in November 2020, has not been reviewed by PitchBook analysts.
100 Keyword-based analysis using data from Pitchbook Inc., data retrieved in November 2020, has not been reviewed by PitchBook analysts.
101 Analysis by headquarter location based on IDC, "Worldwide Semiannual Software Tracker."
102 The White House, "US-EU Summit Statement."

Image Sources

MSC/Müller
P. 14

Charles Haynes
P. 18

All other images:
MSC/Kuhlmann

Acknowledgements

A working draft of this Munich Security Brief was discussed at the MSC Technology Roundtable on July 6, 2021, in Strasbourg at the European Parliamentary Association. The authors and the entire MSC team are very thankful to all participants of the event for their input.

The conclusions of the report are those of the MSC. Analytical support was provided by McKinsey & Company. The authors would like to thank the entire team at McKinsey & Company for their support.

Imprint

Editorial Board
Ambassador Wolfgang Ischinger, Ambassador Boris Ruge,
Dr. Benedikt Franke, Dr. Tobias Bunde

Authors
Simon Pfeiffer, Randolf Carr

Managing Editors
Dr. Julian Voje, Laura Hartmann

Layout
Juliane Schäfer, Julie Zemanek

Design
MetaDesign

Stiftung Münchner Sicherheitskonferenz gGmbH
Karolinenplatz 3
80333 Munich
www.securityconference.org
research@securityconference.org

Visit our app and social media channels:
www.linktr.ee/MunSecConf

DOI: https://doi.org/10.47342/TBAA1644

Please cite as: Simon Pfeiffer, Randolf Carr, Update Required: European Digital Sovereignty and the Transatlantic Partnership (Munich Security Brief 3/2021, July 2021), Munich: Munich Security Conference, https://doi.org/10.47342/TBAA1644.

ISSN (Online): 2702-6574
ISSN (Print): 2702-6558

About the Munich Security Conference (MSC)

The Munich Security Conference is the world's leading forum for debating international security policy. In addition to its annual flagship conference, the MSC regularly convenes high-profile events around the world. The MSC publishes the annual Munich Security Report and other formats on specific security issues.

About the Munich Security Briefs (MSB)

With its Munich Security Briefs, the MSC aims at contributing to ongoing-debates on a particular issue within the broad field of international security. A much more concise format than the Munich Security Report, the briefs are meant to provide an overview of an issue or a read-out of a particular MSC event as well as a succinct analysis of its policy implications and strategic consequences. They generally express the opinion of their author(s) rather than any position of the Munich Security Conference.