msc

No. 2/2021

Error 404 – Trust Not Found

A European Survey on Digital (Dis)trust

Munich Security Brief
March 2021

Authors

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

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

Summary

A joint tech agenda is one of the key priorities of the transatlantic partnership. An exclusive survey on behalf of the Munich Security Conference (MSC) finds that to deliver on this goal, European leaders need to address a high level of digital distrust in Europe – amongst Europeans, but especially vis-à-vis the United States.

At the MSC Special Edition in Munich on February 19, world leaders including US President Joe Biden, German Chancellor Angela Merkel, French President Emmanuel Macron and British Prime Minister Boris Johnson gathered to send a strong signal of transatlantic renewal. In the wake of a joint agenda to "build back better," cooperation on technology has emerged as one of the key priorities.

However, there is a substantial hurdle: As an exclusive survey conducted in six European countries in early 2021 shows, Europeans are deeply concerned about their security and that of their personal data online. Most respondents think their governments are not doing enough to protect them in the digital world and worry about dependencies on foreign suppliers of digital technologies. The survey shows that trust in digital technology does not extend far beyond national borders: Europeans are skeptical of governments and companies from other European countries. This "digital distrust" is only exacerbated when looking across the Atlantic. Most respondents believe data stored by US entities is not secure and find their countries to be too dependent on US technology imports. Vis-à-vis China, such concerns are even more pronounced. European leaders need to address this "digital distrust" – at home and toward the United States. Otherwise, it might threaten progress on the transatlantic tech agenda and put a dent into ambitions of the European Union as a "regulatory superpower." But there is a silver lining: European leaders have a clear mandate to act. There is an opportunity to make substantial progress toward a shared democratic technology governance.

This Munich Security Brief serves as a discussion starter for working towards transatlantic digital trust. It is part of the MSC's "Road to Munich 2021" campaign, which aims to highlight key items on the agenda for renewing transatlantic cooperation.

Error 404 – Trust Not Found: A European Survey on Digital (Dis)trust

"We must shape the rules that will govern the advance of technology and the norms of behavior in cyberspace, artificial intelligence, biotechnology so that they are used to lift people up, not used to pin them down."[4]

Joe Biden, President of the United States of America, MSC Special Edition, February 19, 2021

In 2020, the Munich Security Conference chose the motto of "Westlessness" for its annual conference.[1] The developments over the last year have vindicated our diagnosis: The severity of the Covid-19 pandemic in North America and Europe as well as the absence of meaningful transatlantic cooperation to contain the pandemic and its consequences,[2] the continued erosion of liberal-democratic norms in many Western countries, and a general sense of decreasing global influence all substantiated the analysis of a weakening West – "at home" and in the world. Yet, the election of Joe Biden as US president has been the starting point for efforts to overcome the state of "Westlessness" on both sides of the Atlantic: At the MSC Special Edition on February 19, which was broadcast live to millions of viewers around the world, President Biden and European leaders jointly expressed their ambitions for a renewal of the transatlantic partnership.[3] To move forward, the partners now need to use the momentum and deliver concrete results.

A major issue on the agenda is cooperation on technology.[5] The list of pressing concerns, further heightened in urgency due to the acceleration of digitalization in the context of the Covid-19 pandemic,[6] is long and cuts through all areas of transatlantic politics: From the digital tax to competition policy, privacy, and the sharing of personal data, technology issues are front and center.[7] Discussions about secure supply chains, most prominently regarding 5G equipment, are another major bone of contention.[8] In the defense sector, data interoperability and data sharing are now critical,[9] as recent defense strategies emphasize the necessity of substantially increasing investment in emerging technologies.[10] The prevalence of an "age of perpetual cyberconflict" was showcased once more by the recent SolarWinds and Microsoft Exchange hacking incidents, allegedly perpetrated by Russia and China, respectively.[11] All of these issues have taken center stage as technology has become an arena for geopolitical competition. In particular, the increasingly fierce competition between the United States and China has put a spotlight on power and control in the digital sphere.[12]

"The ongoing global technological competition is, at its core, a competition of values."[13]

Robert O. Work, Vice Chair, National Security Commission on Artificial Intelligence, MSC Technology Roundtable, December 7, 2020

Against that background, setting future standards for the governance of the internet, data, and digital technology has been a long-held ambition for the transatlantic partners. With the election of Joe Biden and the commitment of Europe and the United States to renew the transatlantic partnership, a window of opportunity has now opened to address these issues.[14] Demonstrating the ability to foster digital trust among their citizens could act as a powerful selling point for the liberal-democratic model. The world is in a competition for the best approach to harnessing technology and the digital economy. If the world's democracies can agree on common rules, this would go a long way toward promoting a global digital order reflecting liberal-democratic values.[15]

Scorched Earth: European Digital Distrust

So is the transatlantic tech agenda set up for success? The list of policy issues on which the EU and the United States are far apart is almost as long as the list of priorities itself.[16] Moreover, the last four years have seen European digital sovereignty endorsed as a priority of EU tech policy at the highest level,[17] a development that has elicited concern from across the Atlantic.[18] European policy-makers have claimed that digital sovereignty is not defined "against" anyone else.[19] But these debates revealed that "from a European point of view, the United States is the primary 'other' that Europe measures itself against on technology."[20] The result has been little headway being made on technology cooperation over the last years – despite the multiplicity of critical issues that the transatlantic partners must address and resolve together.[21]

These hurdles can be overcome: Arguably, the perception gap on questions from competition policy to 5G is closing.[22] The European Commission proposed an EU-US agenda with proposals such as a "trade and technology council," a "dialogue on the responsibility of online platforms," or common solutions to antitrust enforcement and taxation in the digital sphere shortly after the election of Joe Biden.[23] At the virtual gathering in Munich, Commission President Ursula von der Leyen extended an offer of cooperation to the United States, repeatedly emphasizing shared values and goals – a clear departure from the strong language of European sovereignty that had dominated the previous four years and has resonated with the European publics.[24]

Given indications of willingness to cooperate from both Brussels and Washington, the time is ripe to move the ball forward. To help open the transatlantic conversation and to lay the groundwork by shedding light on the status quo, the MSC commissioned an exclusive survey on this pressing issue. Across six European countries, citizens were asked about their concerns and perspectives regarding technology with a focus on questions of security, trust, and fear of dependency. Whether trust is present, ultimately, is in the eyes of the user.[25] The survey reveals that the past decade has changed how Europeans perceive the digital world: Their perspective is dominated by concerns about their security and that of their personal data. Instead of embracing the potential for a common governance, they fear data theft, fraud, and increasing national dependency on untrustworthy foreign suppliers, both European and, to a greater degree, suppliers further abroad.

Insecure Network: The Internet Is a Dangerous Place

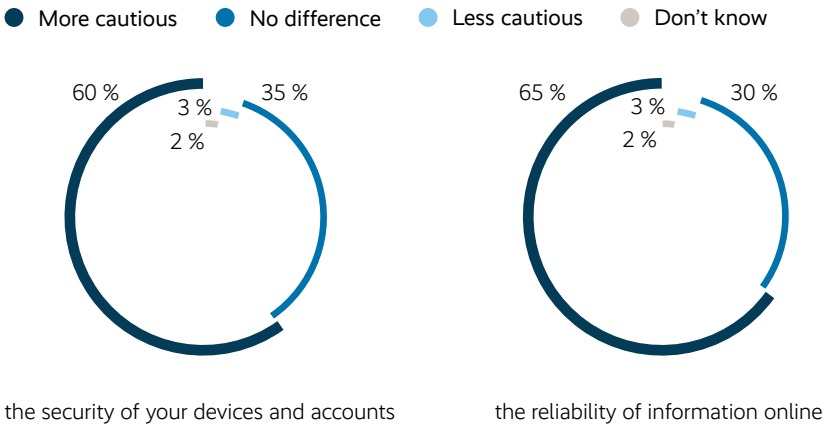
Over the last five years, European citizens have become significantly more careful when acting online (see Figure 1). This concerns both personal information and the information they interact with: Compared to five years ago, two thirds of respondents have become more cautious regarding the reliability of information they find online; 60 percent are now more cautious with respect to the security of their devices and accounts. This development of growing caution follows a broader trend of decreasing trust in the technology sector and skepticism about the veracity of information across the media landscape in recent years.[26]

On behalf of the Munich Security Conference, Kekst CNC conducted a representative survey among the general population in France, Germany, Italy, Poland, Sweden, and the United Kingdom for this report. For this survey, a total of 6,039 respondents were interviewed. The results were quota-adjusted and weighted to be nationally representative of each country surveyed. The survey was conducted in January 2021, using an online questionnaire.

Figure 1

European caution when using the internet,* 2021, percent

Compared to five years ago, are you more or less cautious regarding...



Data: Kekst CNC, commissioned by the Munich Security Conference.
Illustration: Munich Security Conference.
*General population in France, Germany, Italy, Poland, Sweden, and the United Kingdom.

"Whether from our streets or from our screens, we should be able to do shopping in a safe manner. Whether we turn pages or scroll down, we should be able to choose and trust the news that we read. And of course, what is illegal offline is equally illegal online."[29]

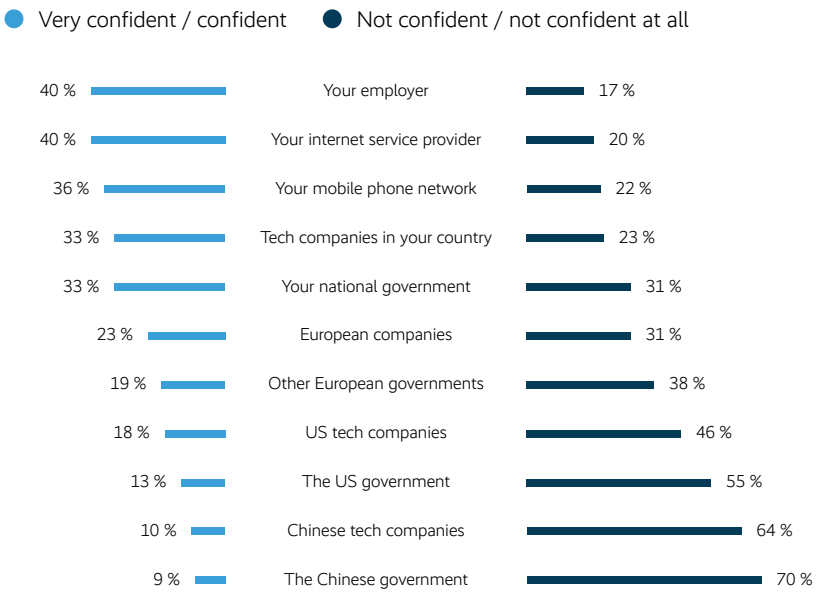
Margrethe Vestager, European Commissioner for Competition and Executive Vice President of the European Commission for A Europe Fit for the Digital Age, Brussels, December 15, 2020

Our survey also reveals how fundamentally skeptical Europeans are about the security of their personal data. Eight years after the Snowden revelations let fears about the misuse of private data skyrocket,[27] Europeans across all surveyed markets substantially doubt the ability, the willingness, or both of most institutions outside of their country to protect their personal information (see Figure 2). The private companies with which citizens interact – for example, their employers, service providers, and their national digital sector – are trusted most. In net terms, these companies were ranked as more trustworthy than national governments in all countries, except for Sweden. This may reflect prominent attacks against government institutions such as the hack against the German parliament in 2015, for which the EU levied sanctions on two Russian officials in 2020.[28]

Figure 2

European trust in safety of personal data,* 2021, percent

How confident are you in the following organizations' ability and willingness to protect your personal data?



Data: Kekst CNC, commissioned by the Munich Security Conference.
Illustration: Munich Security Conference.
*General population in France, Germany, Italy, Poland, Sweden, and the United Kingdom. Excluding "don't know" and neutral responses.

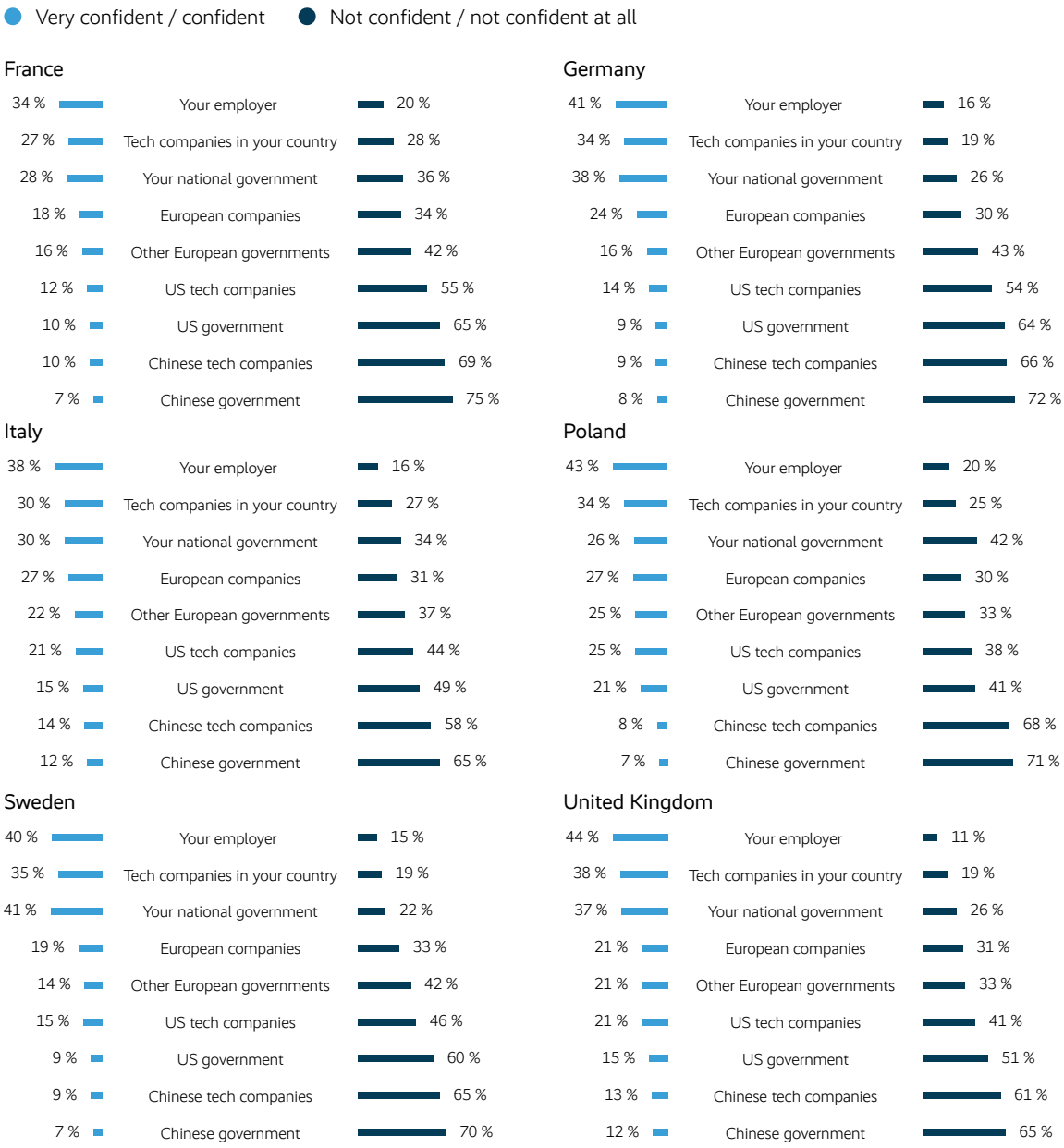
A lack of trust in the governments' ability and willingness to protect their citizens' personal data could hinder building more digitally capable bureaucracies, a goal identified by many European governments during the Covid-19 pandemic. A detailed look at the data at the national level offers a more differentiated picture (see Figure 3). Some national governments have managed to maintain citizens' trust in their handling of personal data: Swedish (by a margin of 19 percent), German (12 percent), and British (11 percent) authorities are more trusted than distrusted by their publics when it comes to safeguarding personal data.

The fact that European citizens have less trust in their national governments than in companies from their countries to protect their personal data coincides with a broader downturn in public confidence in government institutions in Europe over the last years.[30] Further, early research indicates that Western governments' scrambled response to the pandemic is likely to further undermine overall public trust in government institutions.[31]

Figure 3

European trust in safety of personal data, 2021,* percent

How confident are you in the following organizations' ability and willingness to protect your personal data?



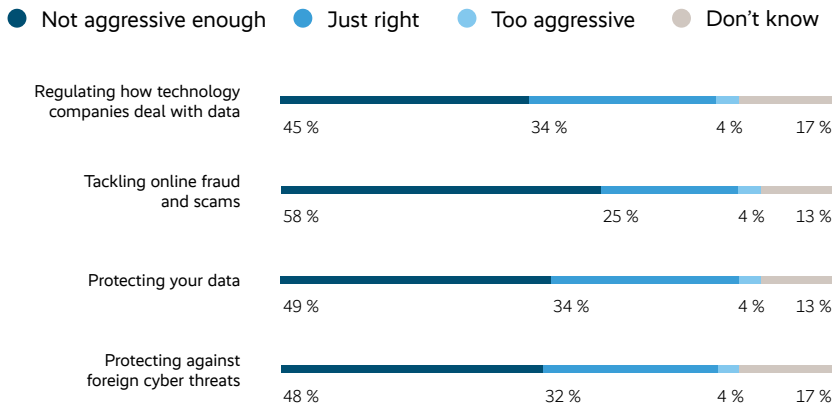
Data: Kekst CNC, commissioned by the Munich Security Conference. Illustration: Munich Security Conference.
*Excluding "don't know" and neutral responses.

A proximate cause for a low level of trust may be the perception of a distinct lack of government action felt by a large part of the public. Across all countries, our survey finds that either an absolute majority or a plurality of respondents think that their national government is not acting aggressively enough on a range of security and privacy related issues (see Figure 4).

Figure 4

Public opinion on government action, 2021,* percent

Do you think your government is being too aggressive or not aggressive enough regarding...



Data: Kekst CNC, commissioned by the Munich Security Conference.
Illustration: Munich Security Conference.
*General population in France, Germany, Italy, Poland, Sweden, and the United Kingdom.

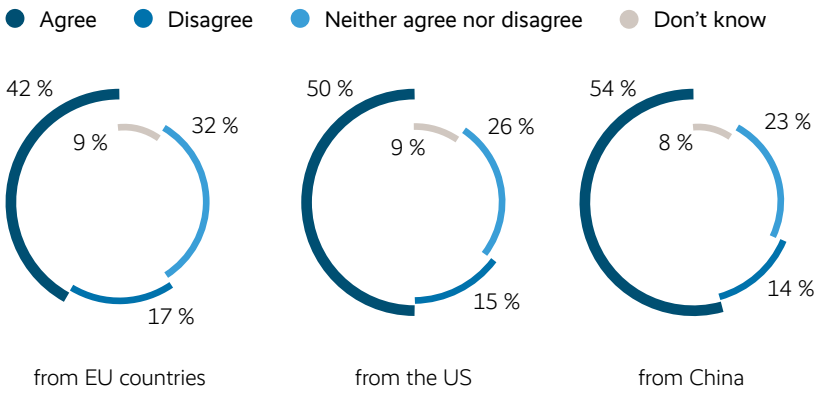
Ideas of "Techno-nationalism" as a Threat to European Action

Moreover, our survey reveals that while there is a moderate trust deficit in some publics toward their own national governments, the lack of digital trust is much more prevalent toward the rest of Europe. Overall, respondents were significantly (by a margin of 18 percent) less trusting of private companies from elsewhere in Europe than of companies in their home country, and even less trusting of other European governments (see Figure 2). A notable exception is Poland, where respondents were especially skeptical of their own government, even more so than of others in Europe (see Figure 3). Among the rest, the gap between the perceived trustworthiness of other European governments and one's own ranged from a margin of 11 percent in Italy to 47 percent in Sweden.

Figure 5

Share of Europeans who think their country is too dependent on foreign digital technologies, 2021,* percent

Do you agree or disagree with the following statement: My country is too dependent on digital technologies...



Data: Kekst CNC, commissioned by the Munich Security Conference.
Illustration: Munich Security Conference.
*General population in France, Germany, Italy, Poland, Sweden, and the United Kingdom.

This prevailing trust gap between the national and the European level raises questions about how the efficacy of European frameworks and institutions to govern the issue of data privacy has been received by citizens. It also questions whether the EU will be able to deliver on its ambition to be a "regulatory superpower."[32] The EU's flagship measure on data privacy, the General Data Protection Regulation (GDPR), in particular, has been noted as an "export hit."[33] Measured against that level of ambition, the implication that the much-discussed GDPR has so far been unsuccessful in building confidence among Europeans that their data is protected equally throughout the EU should be cause for concern. The "unique selling point" of digital regulation "made in Europe" will only materialize if it also succeeds in gaining public acceptance at home.

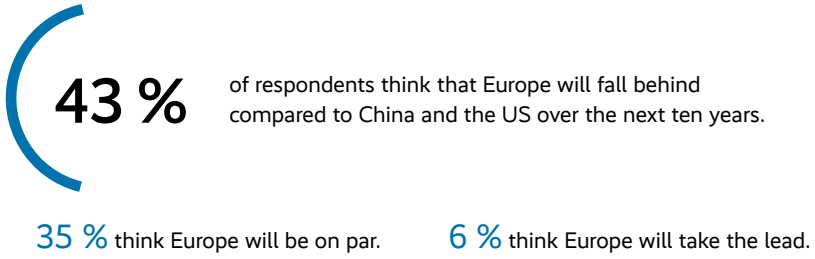
Europeans' concern about technology actors beyond their national borders is not limited to the handling of their personal data. The survey reveals a widespread sense among Europeans that their countries are too reliant on technologies from elsewhere, even from other European countries. What is more, our findings carry a worrying implication for how the EU is seen (see Figure 5): Overdependence on EU neighbors is seen as a problem by nearly as many Europeans as overdependence on the United States or China is. Following this train of thought could lead to a mistaken idea of "going it

alone." Such "techno-nationalism" that erroneously assumes EU countries could or should claim national control over digital issues would hinder efforts to deepen European integration in the digital space. Respondents to our survey are not optimistic about Europe's chances of reversing the trend of technological overreliance on the US and China. Overall, 43 percent expected Europe to continue falling behind the United States and China over the next ten years. Another 35 percent at least believe Europe will be on par with the competition in 10 years, but just six percent expect Europe to take the lead. These numbers hint at an underlying skepticism that Europe will manage to create the fertile environment for innovation in digital tech necessary to compete. Given the digital economy's critical importance to future growth, this should raise concerns for Europeans' optimism about the overall prospects for European prosperity.

Figure 6

Europeans' perspective on how Europe will fare in digital technologies,* 2021, percent

How will Europe fare in international competition on digital technologies compared to China and the US over the next ten years?



Data: Kekst CNC, commissioned by the Munich Security Conference.
Illustration: Munich Security Conference.
*General population in France, Germany, Italy, Poland, Sweden, and the United Kingdom. Excluding "don't know" responses.

The results underscore the importance of long-standing priorities on the European technology agenda to enforce a positive perspective for Europe in the digital sphere: The Digital Services and Digital Markets Acts, the completion of the Digital Single Market, and the strengthening of Europe's digital ecosystem. Europe needs to foster its market power in the digital sphere through combining member states' weight to achieve more influence and prosperity. By achieving tangible results, the EU can counter the narrative that Europe does not deliver for its citizens when it comes to the digital economy. Otherwise, European national leaders could be confronted with

increased political pressures to attempt greater "digital independence" from the rest of the European Union, which could drive a greater wedge between member states.

The Transatlantic Partnership: Deeply Distrusted?

"In recent years, however, we have seen the abuse of personal data – the over-exploitation of data by companies in pursuit of profit. Or by states, like in China, for the purpose of controlling their citizens. […] Citizens will not accept to be transformed into objects, to see their personal and consumption choices guided by secret algorithms."[34]

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

The skepticism among Europeans toward European companies and governments was compounded when our survey asked them to look across the Atlantic. The sharp decline of European confidence in the United States between 2016 and 2020 is well documented.[35] In the digital space, however, the trend has roots that predate and go beyond the presidency of Donald Trump. The trust in the transatlantic partnership on data issues clearly has suffered continuous damage from a cascade of disputes and scandals. The 2013 Snowden leaks about the National Security Agency's (NSA) "Prism" program, including illegal "eavesdropping" on German Chancellor Merkel's mobile phone, was a watershed,[36] but issues like the controversy around Cambridge Analytica's reported leveraging of social media data and numerous widely publicized spats between US tech giants and European regulators have reinforced the trend.[37] Moreover, it is not just that European citizens are suspicious of the US government; business relations with the United States in the tech sector are strained, too, as a recent German study finds.[38] In some European countries today, as former Swedish Prime Minister Carl Bildt writes, US tech giants are dramatized as "mortal threats to the European way of life."[39]

This dramatic assessment is to some extent borne out by our polling. The US tech sector and, even more so, the US government are severely distrusted by European publics with respect to their regard for data privacy and security, even compared to the low levels of trust in domestic and other European actors (see Figure 3).

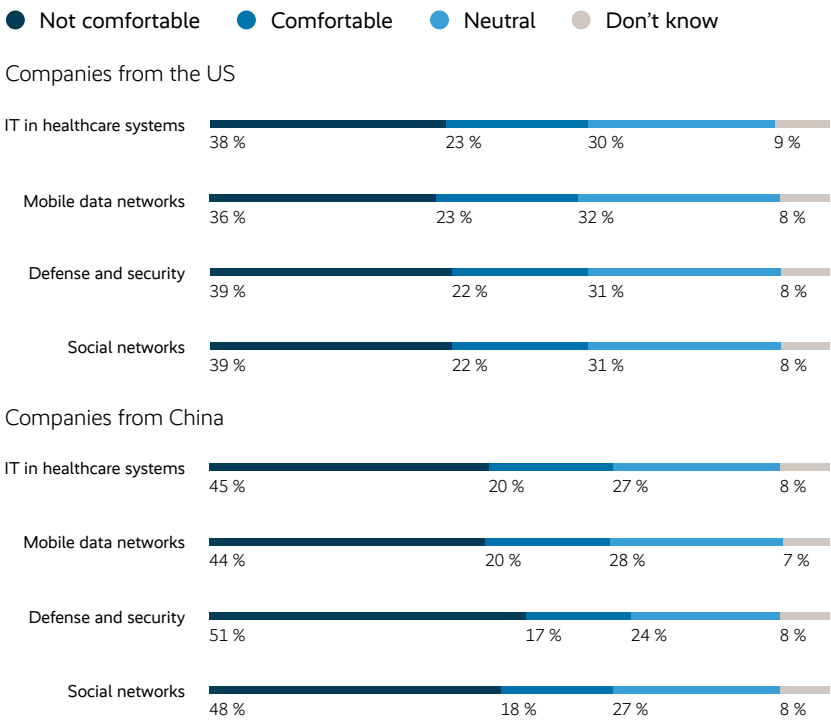
Meanwhile, a plurality of Europeans polled said they were not comfortable with US companies being involved in national critical sectors (see Figure 7). A significant share of respondents across Europe are uncomfortable with US companies being involved in social networks, mobile data, IT in healthcare, and defense and security. These concerns were heightened when extended to China. Europeans are even more uncomfortable with Chinese involvement in these sectors: Nearly half of all people surveyed are not comfortable with Chinese companies being involved in any of the areas in question. The greatest area of concern was defense and security. This underscores a trend

particularly visible in strategic decisions about technology procurement: Increasing numbers of European countries have joined the United States in practically barring Chinese suppliers from providing components to national security infrastructure and hardware (e.g., 5G equipment).[40]

Figure 7

European discomfort with foreign companies being involved in national critical sectors, 2021,* percent

How comfortable are you with foreign companies being involved in...



Data: Kekst CNC, commissioned by the Munich Security Conference.
Illustration: Munich Security Conference.
*General population in France, Germany, Italy, Poland, Sweden, and the United Kingdom.

Overall, our survey reveals a dire state of transatlantic digital trust in public opinion. A significant part of the European public is reluctant to rely on US actors to protect their personal data or provide technologies in key areas of the digital sector. In some countries, the US government is seen as just marginally more trustworthy than the Chinese government. Caution regarding China would appear warranted given its track record on surveillance and digital governance.[41] By comparison, the numbers show just how much European confidence in US rule-of-law mechanisms for tech governance and data collection lags behind what should be expected vis-à-vis a democratic partner and ally. While policy-makers have again begun to invoke a basis of common values on which transatlantic cooperation on technology and even a global democratic governance for the digital world should be built, our polls show a highly skeptical European public.

Toward Security: The Mandate for Building Digital Trust

"Our digital infrastructure must be one thing above all else, namely trustworthy. This is what users expect and, above all, this also benefits the economic development prospects of our companies. What is more, we need to strengthen our defenses against cyber-attacks [...] and against attempts to exercise influence in the digital domain at all levels, also in the political realm."[43]

Heiko Maas, Federal Minister of Foreign Affairs, Bitkom Opening Speech, October 27, 2020

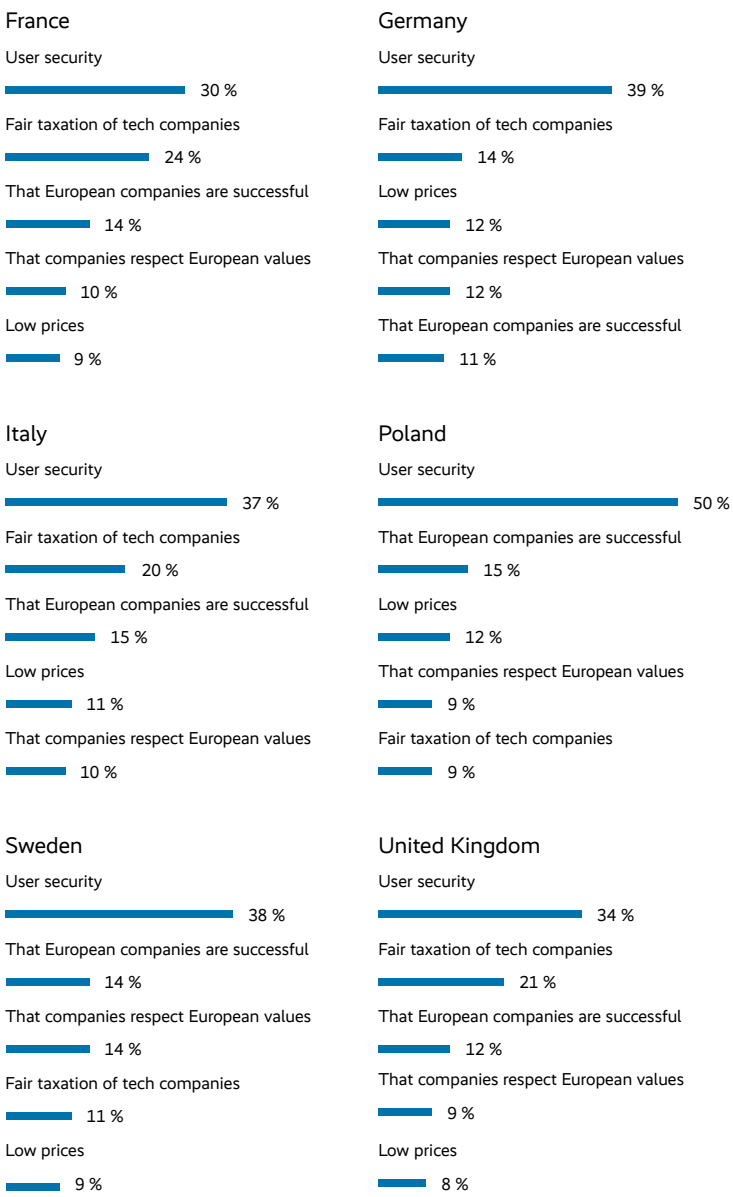
However, there is a silver lining. Our survey also reveals clear priorities among the European public, outlining the central issues European leaders need to address and signaling a mandate to take decisive action. We find that for Europeans, security is the essential element of a European, and by extension transatlantic, agenda on digital technology (see Figure 8). By a wide margin (across Europe, 38 percent of respondents name security as their first priority), the polling finds, their overriding concern is that they themselves are secure when using the internet – and they expect their governments to prioritize accordingly. Making sure tech companies "pay their fair share" of taxes garnered the next most support, while other proposed options rank much lower.

With tangible progress on consumer security issues such as protecting users from cybercrime, reducing online fraud, and ensuring security of software and hardware products, there is a high likelihood that transatlantic cooperation can be successful. The clarity of the mandate and the priority for citizens suggest a major payoff in terms of transatlantic digital trust if progress can be achieved. Reaching out to the United States on this issue will face little in the way of resistance. Other, lower-ranking priorities could be harder to achieve. Washington has been more reluctant to levy taxes on big technology firms, despite insistence from the European Commission as well as from France, in particular. A digital services tax at the European level has so far made little headway due to opposition among member states – and, prominently, from the United States – prompting France and others to go it

Figure 8

Priorities for government action on digital technologies according to Europeans,* 2021, percent

What should be the top priority of European countries on digital technologies?



Data: Kekst CNC, commissioned by the Munich Security Conference.
Illustration: Munich Security Conference.
*Excluding "don't know" and "none of the above"

alone.[42] However, success on issues of user security could establish a baseline of trust that creates opportunity to achieve progress in other fields by demonstrating responsiveness to the Europeans' most pressing concern.

A wide range of policy options in pursuit of those priorities are popular with Europeans (see Figure 9). Consistent with their concern about personal security online, respondents strongly support a mandatory cybersecurity certification for software and hardware. Recognizing that certification plays a critical role in increasing security and, perhaps more importantly, trust among technology users, the EU is working on designing a cybersecurity certification framework for assessing different products and services.[44] While subjecting products to these schemes will remain voluntary for the foreseeable future,[45] the private sector shows promising signs of proactively addressing the concern of cybersecurity, including initiatives such as the Charter of Trust, initiated by the MSC and companies including Siemens, Allianz, and Airbus.[46]

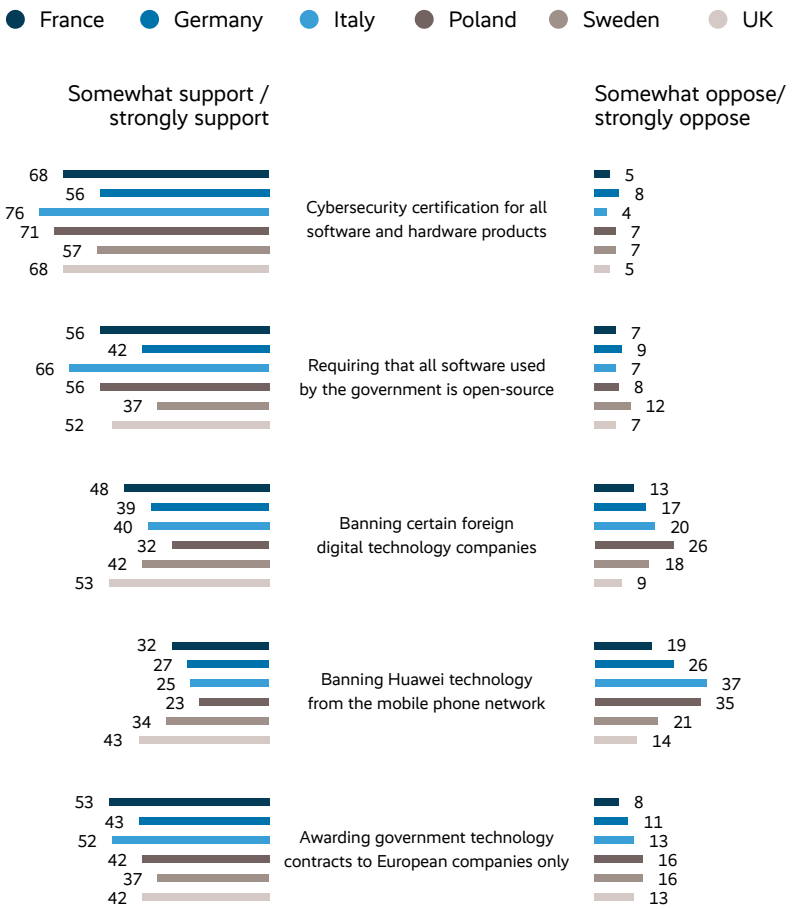
In most countries, a majority also endorses requiring governments to exclusively use open-source software. A policy measure usually not exposed to much public discussion, governments' use of open-source software is often associated with improving cost efficiency and increasing transparency and trust.[47] Awarding government technology contracts to European companies only also received significant support across countries. Notably, a similar share of Europeans also supported banning certain foreign digital technology companies.

However, the survey data also shows that for many Europeans, concerns about preventing security risks or loopholes in personal devices ends at their own pocketbooks (see Figure 10). Despite the low levels of confidence about involving US and Chinese companies in key technology areas, only a minority of respondents indicated a willingness to pay a 30-percent premium for their technology products if it meant that they were produced only by European companies (32 percent) or in accordance with certified security standards (34 percent). These findings cannot be encouraging for proponents of European "digital sovereignty."

Figure 9

Public support for government action on technology,* 2021, percent

Do you support or oppose your government taking the following measures concerning digital technology?



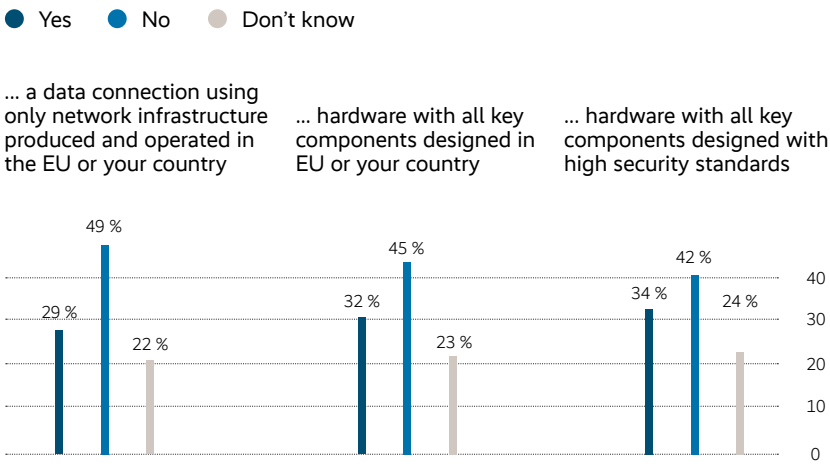
Data: Kekst CNC, commissioned by the Munich Security Conference.
Illustration: Munich Security Conference.
*Excluding "don't know" and neutral responses.

Overall, our survey found a widespread lack of confidence in the entities that run and regulate the digital landscape which European citizens navigate daily. Yet, its results also indicate there is a broad basis of support for more ambitious measures that both national and European regulators can take to tackle the challenges that the digital space poses in terms of insecurity and distrust.

Figure 10

Europeans willing to pay a premium for more secure technology products, 2021,* percent

Please say if you would or would not be willing to pay 30 percent more for...



Data: Kekst CNC, commissioned by the Munich Security Conference.
Illustration: Munich Security Conference.
*General population in France, Germany, Italy, Poland, Sweden, and the United Kingdom.

Conclusion: Reducing the Trust Deficit

Against the backdrop of digital technology's indispensable and growing role across all sectors of society, our survey results indicating a pervasive sense of insecurity and skepticism toward actors in the digital arena are concerning. If Europe and the transatlantic partnership are to live up to their goals for integration and cooperation in the digital sphere, they will need to address this trust deficit. The implications for how the European and transatlantic partners can tackle digital distrust are two-pronged.

First, Europe needs to get its digital house in order. The EU and European governments have, so far, not convinced their publics of their collective capability to provide sensible, robust, and most of all trusted guardrails to the digitalization permeating citizens' lives. The goal of "protecting Europeans online" – part of the broader vision of a "Europe that protects" – has not yet been achieved.[48] Recognizing that shortcoming, EU Commission Vice-President Margrethe Vestager has said that the EU strategy for a "digital decade" has to be "as much about building trust as it is about investing in digi-

tal innovation."[49] The urgency and scale of the challenge of building trust is indeed high, but the potential rewards are also significant. On this issue, Europe needs to deliver. What is more, it needs to strengthen its foresight capabilities to identify similar challenges emerging from novel technologies early on – a goal the MSC is working toward with its recently established Security Innovation Board.[50] But Europe's performance on current challenges leads to an additional issue: Our survey finds that low confidence in Europe runs parallel to intense pressure on national governments to act. Retreating to the national level to address issues of digital technology would be counterproductive: Letting such mistaken ideas about a techno-nationalism run unchallenged would result in a "fragmented system, with different rules in different EU countries."[51] This could be especially detrimental, further weakening the EU's ability to deliver on its promise of prosperity and thereby motivating even less investment in European cooperation.

Moving beyond rhetoric, the best way to build trust is by achieving tangible outcomes for European technology users. The priority that our respondents give to the security of their experience online gives European policymakers a clear mandate for common action toward that goal and a lens through which to view initiatives like the Digital Services and Digital Markets Acts, the completion of the single digital market, and the strengthening of Europe's digital ecosystem. To what extent they shore up citizens' confidence in the digital technology landscape and in Europe's ability to effectively manage it will be a key indicator for judging the success of these initiatives. Doing so would go a long way toward backing up the popular narrative of the EU as a regulatory "trailblazer" and "superpower."[52]

Second, the transatlantic partners will have to work together to manage this lack of trust and avoid letting it derail a budding transatlantic digital agenda. As such, transatlantic cooperation in this sphere will require both policy alignment across a complex set of issues, and public outreach to "win hearts and minds," especially on the European side. The ignominious failure of the Transatlantic Trade and Investment Partnership (TTIP) is a cautionary example of the power that unfavorable public opinion wields in the potential derailment of major transatlantic initiatives. The growing drumbeat around regulating tech giants in the United States and milestones like California's data privacy act are a hopeful sign of a real "growing convergence of views on tech governance between Europe and the United States."[53] How tech companies on both sides of the Atlantic respond will play a major role. The results of our survey can be understood as call to action to the private sector to

"Together, we could create a digital economy rulebook that is valid worldwide. A set of rules based on our values: human rights and pluralism, inclusion and the protection of privacy. We need to join forces and protect these values with all our energy."[54]

Ursula von der Leyen, President of the European Commission, MSC Special Edition, February 19, 2021

shore up digital trust, too. More initiatives like the Charter of Trust can go a long way toward advancing that goal.

Creating positive momentum amidst a distrust-ridden landscape requires more than gradual convergence and conciliatory rhetoric from both sides of the Atlantic. Just as there is no turning back the clock on other transatlantic issues under the new Biden administration, there is no returning to a time before the Snowden revelations, the Trump presidency, and the European digital sovereignty debate. Thus, a transatlantic tech agenda will need to include mechanisms that assure the public that they are built not just on professions of common values, but on transparency and accountability, too.

"Digital distrust" directly impacts citizens' everyday lives. Overcoming distrust by launching a common digital agenda will be a litmus test for a transatlantic partnership that seeks to reset itself and produce tangible and effective outcomes. The pay-off would not only be a major win for transatlantic cooperation. Shaping the beginnings of a robust "digital economy rulebook" between the US and Europe – a rulebook that is trusted by their citizens – would be a step toward the goal set by the transatlantic leaders at the virtual gathering in Munich: sending a message to the world that democracies can still deliver tangible results on the major challenges of today and tomorrow.


1
2,2x
SLO-MO
VIDEO
FOTO
PORTRÄT
PANO

Key Points

1. A joint tech agenda is one of the key priorities of the transatlantic partnership. Progress on this issue will serve as a litmus test for the ability of the EU-US partnership to deliver on critical issues.

2. An exclusive opinion survey commissioned by the Munich Security Conference finds that European citizens are deeply concerned about their security and that of their personal data when online. They also worry about national dependency on foreign suppliers of digital technologies.

3. Europeans have significant digital distrust in private and government institutions from other European countries, but especially the United States and China. They worry that Europe as a whole will fall further behind in the next decade.

4. European leaders need to address their citizens' security and privacy concerns, both on the European level and within the transatlantic partnership. Otherwise, they threaten to derail transatlantic cooperation on technology and the EU's credibility as a "regulatory superpower." Succeeding, however, could promote meaningful progress toward common democratic technology governance.

Endnotes

1 Tobias Bunde et al., "Munich Security Report 2020: Westlessness," Munich: Munich Security Conference, February 2020, doi:10.47342/IAQX5691.
2 On the manifold consequences of the Covid-19 pandemic, see Sophie Eisentraut et al., "Polypandemic: Special Edition of the Munich Security Report," Munich: Munich Security Conference, November 2020, doi:10.47342/CJAO3231.
3 Tobias Bunde, "Beyond Westlessness: A Readout from the MSC Special Edition 2021," Munich: Munich Security Conference, Munich Security Brief, February 2021, doi:10.47342/NLUJ4791, 9.
4 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.
5 See European Commission, "A New EU-US Agenda for Global Change," Brussels: European Commission, High Representative of the Union for Foreign Affairs and Security Policy, December 2, 2020, https://perma.cc/3NKX-W4V6, 5; Joseph R. Biden, "Why America Must Lead Again: Rescuing U.S. Foreign Policy After Trump," Foreign Affairs 99:2 (2020), 64–76, https://perma.cc/BH4P-7VCB.
6 Scott Brennen et al., "Types, Sources, and Claims of Covid-19 Misinformation," Oxford: Reuters Institute for the Study of Journalism, April 7, 2020, https://perma.cc/CSY8-QK48.
7 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.
8 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.
9 National Security Commission on Artificial Intelligence, "Final Report," Washington, DC: National Security Commission on Artificial Intelligence, March 1, 2021, https://perma.cc/27VD-3JMG.
10 See Ministry of the Armed Forces France, "Strategic Update," Paris: Ministry of the Armed Forces France, January 21, 2021, https://perma.cc/GY7B-B3WS; Netherlands Ministry of Defence, "Defence Vision 2035," The Hague: Netherlands Ministry of Defence, October 2020, https://perma.cc/C744-7DK3.
11 US Cybersecurity & Infrastructure Security Agency, "Joint Statement by the Federal Bureau of Investigation, the Cybersecurity and Infrastructure Security Agency, the Office of the Director of National Intelligence, and the National Security Agency," Washington, DC: US Cybersecurity & Infrastructure Security Agency, January 5, 2021, https://perma.cc/9VXK-TDAQ; Paul R. Kolbe, "With Hacking, the United States Needs to Stop Playing the Victim," *The New York Times,* December 23, 2020, https://perma.cc/XH3F-N7JV; Microsoft Threat Intelligence Center, "HAFNIUM Targeting Exchange Servers with 0-Day Exploits," Redmond: Microsoft Threat Intelligence Center, March 2, 2021, https://perma.cc/CVT7-ZZW3.
12 Ulrike Franke, "Upstaged: Europe's Struggles to Play the Great Tech Game," London: ECFR, Commentary, February

25, 2020, https://perma.cc/4RXF-6FE9; Gramer, "Trump Turning More Countries in Europe Against Huawei."

13 Munich Security Conference, "MSC Technology Roundtable: A Transatlantic Agenda in Technology and Digital Policy," Munich: Munich Security Conference, December 7, 2020, https://perma.cc/73BN-WPPC.

14 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.

15 European Commission, "A New EU-US Agenda for Global Change," 5–6.

16 Scott and Cerulus, "EU-US 'Tech Alliance' Faces Major Obstacles on Tax, Digital Rules;" Ulrike Franke, "Artificial Divide: How Europe and America Could Clash over AI," London: ECFR, Policy Brief, January 20, 2021, https://perma.cc/J46A-NLG9.

17 See European Commission, "Shaping Europe's Digital Future," Brussels: European Commission, February 2020, https://perma.cc/5S49-48CU and Council of the European Union, "Expanding the EU's Digital Sovereignty," Brussels: Council of the European Union, 2020, https://perma.cc/9RNQ-GSC8.

18 Tyson Barker, "Europe Can't Win the Tech War It Just Started," *Foreign Policy*, January 16, 2020, https://perma.cc/RCC4-9N9Z.

19 European Commission, "Shaping Europe's Digital Future," 3; Axel Voss, "Ein Manifest für die digitale Souveränität und geopolitische Wettbewerbsfähigkeit Europas," Brussels: Group of the European People's Party in the European Parliament, 2020, https://perma.cc/6WDP-8MMQ; Emmanuel Macron, "Emmanuel Macron in His Own Words: The French President's Interview with The Economist," *The Economist*, November 7, 2019, https://perma.cc/7B4P-JGKZ; Annegret Kramp-Karrenbauer, "Second Keynote Speech by German Federal Minister of Defence," Berlin: Federal Ministry of Defence, 2020, https://perma.cc/E78U-MBG7.

20 Franke, "Artificial Divide."

21 Nicholas Vinocur, "'We Have a Huge Problem': European Tech Regulator Despairs Over Lack of Enforcement," *Politico*, December 27, 2019, https://perma.cc/CG9P-FH4B; Nicholas Vinocur, "Europe and the US Are Drifting Apart on Tech. Joe Biden Wouldn't Fix That." *Politico*, November 3, 2020, https://perma.cc/RL5T-DRQY.

22 Barker and Schaake, "Democratic Source Code for a New U.S.-EU Tech Alliance;" Gramer, "Trump Turning More Countries in Europe Against Huawei."

23 European Commission, "A New EU-US Agenda for Global Change," 7.

24 Catrina Schläger, "Survey on European Sovereignty," Berlin, Paris: Friedrich Ebert Stiftung and Fondation Jean Jaurès, March 2, 2021, https://perma.cc/ACR3-JKZE; Ursula von der Leyen, "Speech by President von der Leyen at the Special Edition 2021 of the Munich Security Conference," Brussels/Munich: Munich Security Conference, February 19, 2021, https://perma.cc/R95H-MDDT.

25 Bhaskar Chakravorti, Ajay Bhalla, and Ravi S. Chaturvedi, "How Digital Trust Varies Around the World," *Harvard Business Review*, February 25, 2021, https://perma.cc/28B8-B69J.

26 Edelman, "Edelman Trust Barometer 2020: Special Report: Trust in Technology," Frankfurt am Main: Edelman, February 2020, https://perma.cc/HES9-STNE; Pricewa-

terhouseCoopers, "Vertrauen in Medien," Düsseldorf: PricewaterhouseCoopers, 2018, https://perma.cc/RB2Z-AJWZ, 9; Megan Brenan, "Americans Remain Distrustful of Mass Media," Washington, DC: Gallup, September 30, 2020, https://perma.cc/W3B2-X9PD.

27 Initiative D21 e.V. and Institute for Public Information Management, "eGovernment Monitor 2013: Nutzung und Akzeptanz von elektronischen Bürgerdiensten im internationalen Vergleich," Munich: Initiative D21 e.V. and Institute for Public Information Management, April 2013, https://perma.cc/SYV7-LFV2.

28 Robin Emmott, "EU Imposes Sanctions on Russian Military Intelligence Chief," *Reuters*, October 22, 2020, https://perma.cc/RA8F-KM8K.

29 Margrethe Vestager, "Statement by Executive Vice-President Vestager on the Commission Proposal on New Rules for Digital Platforms," Brussels: European Commission, December 15, 2020, https://perma.cc/NVV6-XQ3B.

30 Chase Foster and Jeffrey Frieden, "Crisis of Trust: Socio-economic Determinants of Europeans' Confidence in Government," European Union Politics 18:4 (2017), 511–535, doi:10.1177/1465116517723499.

31 Christopher Ingraham, "Coronavirus Will Undermine Trust in Government, 'Scarring Body and Mind' for Decades, Research Finds," *The Washington Post*, July 5, 2020, https://perma.cc/62SU-YW98.

32 Zora Siebert, "Digital Sovereignty – The EU in a Contest for Influence and Leadership," Berlin: Heinrich Böll Foundation, February 10, 2021, https://perma.cc/Q2J7-4MVV.

33 Ann C. Riedel, "Datenschutz: Den ritualisierten Debatten entkommen," Potsdam: Friedrich Naumann Foundation, January 28, 2021, https://perma.cc/HJ43-F8FL.

34 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.

35 Richard Wike, Janell Fetterolf, and Mara Mordecai, "U.S. Image Plummets Internationally as Most Say Country Has Handled Coronavirus Badly," Washington, DC: Pew Research Center, September 15, 2020, https://perma.cc/2ZLD-MS6V.

36 Initiative D21 e.V. and Institute for Public Information Management, "eGovernment Monitor 2013," 17.

37 Ingo Dachwitz, "Nein, der Cambridge-Analytica-Skandal fällt nicht in sich zusammen," *Netzpolitik.org*, October 23, 2020, https://perma.cc/ZGQ8-EZ2Y.

38 Bitkom, "Digitale Souveränität – Wie abhängig ist unsere Wirtschaft?" Berlin: Bitkom, February 18, 2021, https://perma.cc/G37F-7HHQ.

39 Carl Bildt, "China Is a Rising Digital Superpower. Europe and the U.S. Must Catch Up – Together." *The Washington Post*, February 1, 2021, https://perma.cc/F3NF-NREU.

40 Gramer, "Trump Turning More Countries in Europe Against Huawei."

41 Freedom House, "Freedom on the Net 2020: China," Freedom House, 2020, https://perma.cc/2YJE-W75C.

42 Melissa Heikkilä and Elisa Braun, "Digital Tax: A Cautionary Tale," *Politico Europe*, July 23, 2020, https://perma.cc/NHJ2-ZGUG.

43 Heiko Maas, "Speech by Foreign

Minister Heiko Maas on European Digital Sovereignty on the Occasion of the Opening of the Smart Country Convention of the German Association for Information Technology, Telecommunications and New Media (Bitkom)," Berlin: Bitkom, October 27, 2020, https://perma.cc/78Y4-WV9C.
44 European Commission, "The EU Cybersecurity Certification Framework," Brussels: European Commission, June 24, 2020, https://perma.cc/ZG2J-X334.
45 Simon Shooter and Stephanie Lopes, "European Union's New Cybersecurity Act: What Do You Need to Know?" London: Bird & Bird, April 2019, https://perma.cc/8A5Y-74T3.
46 Charter of Trust, "Driving Security in an Insecure World," Munich: Charter of Trust, March 2021, https://perma.cc/4V82-PX6Y; Siemens AG, "Charter of Trust Partners Decide on Further Measures for More Cybersecurity," Press Release, February 14, 2020, https://perma.cc/FDZ5-RZQF.
47 Mark Lerner et al., "Building and Reusing Open Source Tools for Government: Software for Public Benefit Should be Open Source by Default," Washington, DC: New America, July 10, 2020, https://perma.cc/57FE-WE7X.
48 European Commission, "Security Union: A Europe that Protects," Brussels: European Commission, October 2019, https://perma.cc/9HJN-42MM.
49 Margrethe Vestager, "Speech by Executive Vice-President Margrethe Vestager: Building Trust in Technology," Brussels: European Policy Centre, October 29, 2020, https://perma.cc/SNM3-DSF3.
50 Munich Security Conference, "MSC Security Innovation Board," Munich: Munich Security Conference, November 2021, https://perma.cc/33PH-M5W9.
51 Vestager, "Speech by Executive Vice-President Margrethe Vestager: Building Trust in Technology," October 29, 2020.
52 Ian Bremmer, "What Happens Next with Europe's New Regulation of Big Tech," *Time*, February 22, 2020, https://perma.cc/R3TP-LZUU.
53 European Commission, "A New EU-US Agenda for Global Change," 5.
54 Von der Leyen, "Speech by President von der Leyen at the Special Edition 2021 of the Munich Security Conference," February 19, 2021.

Image Sources

MSC/Koch
P. 5

MSC/Koerner
P. 22

MSC/Niedermüller
P. 15

Unión Europeaen Perú
P. 13

All other images:
MSC/Kuhlmann

Acknowledgments

The Munich Security Conference would like to thank the Landesamt für Sicherheit in der Informationstechnik for supporting this project.

Landesamt für Sicherheit in der Informationstechnik

The authors would like to thank the entire team at Kekst CNC, as well as Marcel Lewicki and Melissa Hanlon, for their indispensable support in putting together this Munich Security Brief.

Imprint

Authors
Simon Pfeiffer, Randolf Carr

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/REFQ1817

Please cite as: Simon Pfeiffer and Randolf Carr, Error 404 – Trust Not Found: A European Survey on Digital (Dis)trust (Munich Security Brief 2/2021, March 2021), Munich: Munich Security Conference, https://doi.org/10.47342/REFQ1817.

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.

The Munich Security Briefs

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.