alliance for securing democracy

G|M|E

5G Security: The New Energy Security

Europe's Strategic Vulnerabilities in the 5G Era and Lessons Learned from Europe's Dependence on Russia's Natural Gas

Kristine Berzina

Please direct inquiries to
The Alliance for Securing Democracy at
The German Marshall Fund of the United States
1700 18th Street, NW Washington, DC 20009
T 1 202 683 2650
E info@securingdemocracy.org

This publication can be downloaded for free at https://securingdemocracy.gmfus.org/5g-energy-security/.

Cover image by NicoElNino on Shutterstock.

Alliance for Securing Democracy

The Alliance for Securing Democracy (ASD), a bipartisan initiative housed at the German Marshall Fund of the United States, develops comprehensive strategies to deter, defend against, and raise the costs on authoritarian efforts to undermine and interfere in democratic institutions. ASD brings together experts on disinformation, malign finance, emerging technologies, elections integrity, economic coercion, and cybersecurity, as well as regional experts, to collaborate across traditional stovepipes and develop cross-cutting frameworks.

About the Author

Kristine Berzina is a senior fellow at the Alliance for Securing Democracy in GMF's Brussels office. She focuses on U.S.–EU relations, NATO, and energy topics. Berzina, who lived in Moscow part-time from 2014 until 2016, also analyzes Russia's foreign policy and writes about Baltic foreign policy and security issues. Berzina appears frequently in international media, including NPR, Deutsche Welle, Euronews, The Wall Street Journal, and Agence France-Presse. Prior to joining GMF, Berzina worked on energy security, transatlantic cooperation, and climate change and security in Berlin, Germany and in Washington, D.C. A native of Latvia, Berzina grew up in the United States. She received her master's degree in international relations from the University of Cambridge and her bachelor's in political science and history from Yale University. Berzina is a native speaker of English and Latvian, is fluent in German, and has a basic knowledge of Russian and French. Follow her on Twitter @kristineberz.

Introduction

Europe is on the cusp of a crucial technological and political transformation. This year, most EU member states will need to finalize plans for building 5G networks, which will overhaul the way their economies function. Only a handful of companies around the globe can provide the equipment needed for a 5G system—China's Huawei and Europe's Ericsson and Nokia are leaders. Europe's telecommunications operators have focused on economic questions such as cost and timing in selecting suppliers, but strategic and geopolitical concerns are no less important, as are the concerns of Europe's allies. The United States has banned Huawei from much of its infrastructure over security concerns, and in July, the United Kingdom reversed course and banned the installation of new Huawei parts from its 5G networks starting in 2021 and requiring the removal of existing equipment by 2027. The EU's member states are in the process of making critical decisions of their own, and the stakes are high. Europe is at risk of locking itself into new technological and strategic dependencies with an authoritarian state: China.

Europe has deep and painful experience with dependence on an authoritarian superpower, just in a different sector and with a different power. The commodity in question is old-fashioned natural gas, and the country is Russia. Western European countries entered into long-term energy ties with Russia through the construction of natural gas pipelines in the 1970s over vehement objections by successive U.S. administrations.[1] To this day, Russia is the largest supplier of natural gas to Europe,[2] and the decision to power European industry on Russian gas continues to eat away at European and transatlantic solidarity. Germany's ongoing support for Russian natural gas projects, such as the Nord Stream pipelines, ignores the energy security worries of Germany's EU neighbors[3] and is subjecting European companies to U.S. sanctions.[4]

Over the past several decades, the natural gas relationship between Russia and Germany, in particular, has grown into a vector for Russia's influence in Europe's strongest economy. Former German Chancellor Gerhard Schroeder became the chairman of the board of the first Nord Stream pipeline, which was conceived of during his chancellorship, and then drew further financial benefits from the Russian energy sector in his roles as chairman of the Nord Stream 2 pipeline and of Rosneft, Russia's massive state-owned oil company.[5] Having a former head of government accept money from Russian state-owned companies, and then advocate in favor of government policies friendly to Russia, is an example of how the economic relationship with Russia can corrupt and coopt the political establishment.

It has taken the European Union nearly four decades and significant funds to put in place a regulatory framework and infrastructure that offset the energy security risks inherent in the reliance on Russia's natural gas. Critical capabilities now in place include the ability to pump gas from west to east, EU oversight of member states' bilateral natural gas supply contracts with Russia, and the unbundling of monolithic companies to allow for greater competition and third-party access to major infrastructure.[6] And the system is still imperfect. While it is unlikely that EU citizens will be left freezing in January because of a natural gas supply cut-off, the distrust that pipelines foment between EU member states continues to poison European ties.

Moreover, getting here required various worst-case scenarios to occur—supply disruptions and Russian military aggression on the European continent—before the EU took significant action. In 2006 and 2009, Russia cut off natural gas supplies because of disputes with Ukraine that literally left Europeans in the cold during the dead of winter.[7] These incidents launched real regulatory efforts to increase the security of energy flows.[8] But even then, it took Russia's invasion of Crimea in 2014 for the EU to delve into the bigger geopolitical questions of energy security and launch a European Energy Union.[9] The Energy Union has fixed critical vulnerabilities but still was not able to stop plans to build new pipelines to Russia.

The EU does not have forty years to steel itself against the risk of China's technology and economic coercion. The digital economy is faster-moving and will be more fundamental to the transformation of Europe's economy in the coming decades than energy trade with Russia has been so far. It may be more important for Europe to protect itself against the strategic vulnerabilities that can come from technological dependency on China than it was for Europe to get the gas question right, and Europe will have less time to do it.

This paper explains what 5G technology is, assesses where the EU stands on telecoms infrastructure and 5G policymaking, compares the risks of Europe's dependence on Russia for natural gas with the risks of dependence on China for 5G, and offers policy solutions and recommendations for Europe to reduce its vulnerability.

What is 5G?

5G is shorthand for the fifth generation of telecommunications technology. Approximately once every decade, a new generation of technology emerges and has the power to transform our societies—the 2000s was the decade of 3G technology, flip phones, and work done largely on big desktop computers. When LTE and even faster 4G networks became operational in 2009-2010, they enabled the era of the smart phone and economic patterns that would have been unimaginable a decade earlier.[10] Uber and Lyft, food delivery services, and the gig economy are underpinned by 4G and data sharing on smartphones.

The fifth generation of telecommunications technology will introduce "high capacity, high-speed and low-latency (quick network response) services"[11] that will transform many sectors. This change hinges on speed, which chip manufacturer Qualcomm estimates will be a ten to twenty-fold increase in real-world applications.[12] The effect of this transformation is not only about how quickly a film can download. As connection speeds increase, entirely new economic models become possible. 5G enables the Internet of Things, with increasingly autonomous and connected devices performing key functions or enabling remote connections that once seemed far-fetched.[13] Transformational applications span the full scope of our existing economies, from the rollout of autonomous vehicles to eHealth systems that include remote robotic surgery[14] and even the overhaul of our electrical grids to allow the smooth integration of renewable energy sources.[15] 5G will also be essential for new realms, including for the operation of artificial intelligence systems based on real-time data collection and analysis.[16]

The infrastructure required for 5G networks will look different than what is in place for 4G. With a greater level of communication taking place between devices at the edge of networks, for example, between moving vehicles, there will be a greater need for computing and storage capacity at the edges. An image associated with past telecommunications generations is that of a hub and spoke. In the 5G era, network models appear more as three-dimension grids in which "network and cloud infrastructure slides" are set "over physical infrastructure."[17]

Globally, there are a limited number of suppliers for 5G networks. Mobile telecommunications operators racing to or set up 5G networks have to choose mostly between three equipment manufacturers, China's Huawei and Europe's Ericsson (Sweden) and Nokia (Finland). Other companies involved in setting 5G standards include Qualcomm (U.S.) and Samsung (South Korea).[18]

Bans on Huawei's 5G Technology

Countries around the world are at a crucial decision point for selecting suppliers for 5G networks. These decisions partly hinge on the factors of cost, timing, and existing relationships between telecommunications operators and equipment manufacturers. But because of 5G's fundamentally transformative nature, security concerns have become a core consideration in government guidelines for setting up new networks.

Australia, the United States, and the United Kingdom have cited security concerns to ban Huawei from 5G networks. Australia led the way in 2018, announcing that

> "The government considers the involvement of vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law, may risk failure by the carrier to adequately protect a 5G network from unauthorized access or interference."[19]

In 2019, the United States followed suit. The U.S. Department of Commerce's Bureau of Industry and Security (BIS) put Huawei Technologies and 114 of its overseas-related affiliates on the Entity List, which

> "identifies entities for which there is reasonable cause to believe, based on specific and articulable facts, that have been involved, are involved, or pose a significant risk of being or becoming involved in activities contrary to the national security or foreign policy interests of the United States."[20]

The designation requires U.S. companies to obtain a government license to sell technology to Huawei.[21] Moreover, this designation works in conjunction with President Trump's May 2019 Executive Order,[22] now extended until May 2021,[23] prohibiting U.S. companies from using telecommunications technology from firms that pose a threat to U.S. national security. These restrictions are commonly thought to target Huawei and ZTE in particular. Notably, there are exceptions to the ban on Huawei. The Department of Commerce has granted licenses to allow U.S. companies to continue cooperating with Huawei, particularly those operating rural wireless networks.[24]

In May and August 2020, the United States issued sweeping sanctions against Huawei that the Eurasia Group deemed a "lethal blow"[25] to the company. Huawei is reliant on U.S. made semiconductors. The 2020 U.S. sanctions banned Huawei and affiliates from purchasing semiconductors that are the product of U.S. software and technology (in the May sanctions) or indirectly, "where U.S. software or technology is the basis for a foreign-produced item" (in the August sanctions).[26]

The recent U.S. sanctions forced European countries to reevaluate their reliance on Huawei. In June 2020, the United Kingdom reversed course on an earlier policy that would have allowed Huawei to build 35 percent of its 5G network, announcing instead that Huawei would be removed from 5G networks by 2027 and that no new Huawei 5G equipment can be installed after December 31, 2020.[27] The U.K.'s restrictions came after a decision by National Cyber Security Centre that Huawei's 5G equipment would no longer be secure following the implementation of the May 2020 U.S. sanctions on Huawei that would prevent the company from being able to use U.S. components.[28]

Despite the trend among Europe's allies of moving away from reliance on Huawei for 5G technology, it remains to be seen whether the EU and its member states follow suit.

Where the European Union and its Member States Stand on 5G Equipment: Existing Ties and Future Policies

The European Union is developing frameworks for building secure 5G networks. For the EU's efforts to work, careful guidelines need to be set early, because once a supplier is chosen and equipment is installed, it is difficult to remove and replace. And in some ways, the EU is already behind. The EU is pushing member states to consider 5G network security as 5G networks are already being launched. In May 2020, 12 EU member states had commercial 5G services deployed. Additional member states are planning to make spectrum assignments and launch commercial services by the end of the year.[29]

While the EU has been able to force a conversation about 5G security within member states, the EU institutions have limited powers to change member states' policies and suppliers. Member states themselves have a patchwork of policies in place, from critical stances on 5G security to an absence of policies due to foot-dragging and delays.

European countries are significantly reliant on Chinese equipment in existing mobile telecommunications networks. Recent analysis of Europe's 4G radio access network (RAN) market found that Chinese vendors Huawei and ZTE have a 48 percent share of European 4G RAN networks, based on number of customers.[30] These numbers include non-EU states, such as the U.K. and Switzerland. Three countries are fully dependent on Chinese 4G RAN: Belgium, the Republic of Cyprus and the Faroe Islands. Fifteen countries have more than a 50 percent share, including Germany, Italy, and Greece.[31]

The existing commercial relationships between European telecoms operators and Chinese equipment suppliers make the question of future network security especially fraught, and there has been limited information and analysis of strategic dependencies on the European level.

With a view to setting up resilient and secure 5G systems, EU institutions initiated a political process in 2019 (see Textbox 1). These efforts started with high-level political decisions in the March 2019 European Council Conclusions[32] and the European Commission Recommendations on the cybersecurity of 5G, which argued that "ensuring the cybersecurity of 5G networks is an issue of strategic importance for the Union."[33] The EU's political stance was given teeth through additional steps, including an October 2019 Coordinated Risk Assessment on the Cybersecurity of 5G, a 5G Toolbox of Risk Mitigating Measures, and a 5G Toolbox Implementation Report.[34]

Chronology of the EU's 5G Efforts

22 March 2019: European Council stresses importance of a concerted approach to the security of 5G.

26 March 2019: European Commission adopts its recommendation on the cyber security of 5G networks.

9 October 2019: NIS Cooperation group releases the EU coordinated risk assessment of the cybersecurity of 5G networks.

21 November 2019: ENISA releases its Threat Landscape for 5G Networks.

3 December 2019: Council issues conclusions on the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G.

January 2020: NIS Cooperation group releases the EU Toolbox of risk mitigating measures in the context of cybersecurity in 5G networks.

29 January 2020: European Commission releases a communication on the implementation of the toolbox.

30 April 2020: Member states to have taken concrete steps to implement the toolbox recommendations.

24 July 2020: Member states, with the support of the European Commission and the European Union Agency for Cybersecurity publish a report on the progress made in implementing the joint EU toolbox of mitigating measures for identified 5G risks.

By 1 October 2020, Member states, with the European Commission, should assess the effects of the European Commission Recommendation from May 2019 and determine whether there is a need for further action.

Textbox 1

The EU's 5G process has resulted in several achievements. Putting out a coordinated risk assessment that investigates the EU's vulnerability in an EU-wide manner is a significant step forward for a sector that has been very national in its regulation and strategic outlook. Furthermore, the EU's risk assessment and 5G toolbox go beyond technical questions to include politically motivated threats from state or state-backed actors. They place meaningful attention on the risk of state interference through the 5G supply chain,[35] and they suggest strategic measures in the EU Toolbox to avoid "systemic, long-term dependencies."[36] This holistic vision of the security of 5G networks, when paired with the Commission's very ambitious timeframe for implementing recommendations, forces even laggard member states to evaluate their progress on 5G security.

But critical gaps remain. EU member states have not done enough to ensure a diversity of suppliers and strengthen diversity at the national level. The EU's 5G toolbox implementation report finds that EU member states' progress on assessing the risk profile of suppliers and applying restrictions is middling.[37] This is a logical outgrowth of the diverse approaches EU member states have been taking to 5G suppliers.

EU member states have taken very different approaches to Huawei's role in 5G network development. Many countries have taken a critical stance against Huawei, and nine EU member states are participating in the U.S. Department of State's Clean Network Initiative allowing only "trusted vendors" in their 5G networks. These are smaller EU states or those with close security ties to the United States: the Czech Republic, Slovenia, Poland, Sweden, Estonia, Romania, Denmark, Latvia, and Greece.[38] It remains to be seen how these government commitments to the Clean Network will be operationalized, because operators in these countries have existing relationships with Huawei.

The major European powers vary in their decision-making and communications approaches. Germany was expected to decide on Huawei's role in 5G networks in February 2020, but that decision has been delayed. Bundestag members increasingly are critical of Huawei's role, but Chancellor Angela Merkel has not indicated her position.[39] Reports suggest that the government will propose legislation in October 2020 that would effectively eliminate Huawei from the 5G market through bureaucratic hurdles rather than an outright ban.[40] Meanwhile, Germany's major telecom operator Deutsche Telekom is taking advantage of the delay to move forward with rolling out 5G networks using Huawei equipment.[41]

In contrast, France put in place a de facto ban on Huawei in 5G networks after 2028. This policy closely resembles the U.K.'s ban, but the French government's public messaging has been very different. Authorities have told telecoms operators that they will not be able to renew licenses for Huawei 5G equipment after they expire, but there has been no public condemnation of Huawei or discussion of the implications of the decision for France's foreign policy toward China.[42]

Belgium, the seat of the EU and NATO, has adopted a policy similar to the U.K.'s initial stance. High risk vendors will be excluded from the "core" and will be restricted to a 35 percent share of the radio access portion of the network.[43] In practice, Belgium will not have Huawei in its 5G networks. Both Belgian operators, Orange and Proximus, chose Nokia as their 5G equipment supplier.[44] This is a move away from its current 100 percent reliance on Huawei for 4G radio access network equipment. It is notable that a country in which many sensitive communications take place is only now beginning to reevaluate its cybersecurity vulnerabilities vis-à-vis high-risk vendors.

The Political Challenge of Russia's Natural Gas

The provision of natural gas could on its face be considered a technical and commercial question, something relegated to commodity markets rather than cabinet meetings. But in Europe, natural gas security is a foreign policy question as much as an economic one.

Europe is increasingly dependent on foreign suppliers for natural gas. In 2018, 83 percent of the EU's natural gas supplies were imported, and domestic production is continuing to decline.[45] Russia is Europe's main external supplier, providing over 38 percent of the EU's natural gas imports in 2018 and 2019.[46] This is a significant share EU-wide, but individual states have much higher dependency rates. Eleven EU member states are between 75 and 100 percent dependent on Russian natural gas imports.[47]

The decision to buy Russian natural gas has been a political question from the beginning. West Germany launched efforts to build pipelines and start purchasing natural gas from the Soviet Union as a part of its broader Cold War foreign policy. When Chancellor Willy Brandt was elected in 1969, he saw economic cooperation with the USSR as the main element of his Ostpolitik policy, which aimed at "'change through rapprochement' (Wandel durch Annäherung)."[48] In 1970, West Germany signed a deal with the USSR to provide steel pipes in exchange for gas, a deal designed to circumvent U.S. restrictions on West German steel pipe sales to the USSR.[49]

Still today, the future of pipelines and gas transit between European states and Russia depends on the foreign policy considerations of national leaders and senior EU officials. The completion of the Nord Stream 2 pipeline from Russia to Germany is subject to Chancellor Angela Merkel's blessing and has recently been questioned because of foreign policy questions unrelated to the energy sector—the Russian government's role in the poisoning of Russian opposition leader Alexey Navalny.[50] At the EU-level, the future of gas flows receives senior political attention because it is a crucial element of the EU's external affairs. European Commission Vice President Maroš Sefčovič played a crucial diplomatic role brokering agreements between the Energy Ministers of Ukraine and Russia for the continuation of Russian natural gas transit through Ukraine, despite the ongoing Russian military occupation of eastern Ukraine and annexation of Crimea.[51]

Willy Brandt oversaw an agreement to receive Soviet gas five decades ago. Only in the last 11 years has the European Union been able to counter many of its energy supply security vulnerabilities. Doing so has required both market reforms and high-level political initiatives. Market reforms, starting under the Third Energy Package,[52] broke apart vertically integrated natural gas companies and laid the groundwork for new suppliers to access pipeline and sales networks. The creation of reverse-flow capacity allowed natural gas to flow from west to east across the EU. As a result, Europe is able to receive and better distribute pipeline gas and new liquefied natural gas sources around the world (Qatar, Nigeria, and the United States.)[53] These technical measures, when paired with political initiatives encouraging dialogue, solidarity, and trust between the member states under the EU's Energy Union,[54] have gone a long way towards neutralizing Europe's energy security challenge.

The Energy Analogy: Similarities Between Dependence on Russia for Gas and on China for 5G Telecommunications

The policy problems of Europe's natural gas dependence on Russia and potential dependence on China for 5G technology may appear unrelated. But there are several structural similarities between the threats posed by dependence on Russian natural gas and dependence on telecommunications technology from Chinese companies with close ties to the Chinese state apparatus. Understanding these similarities can help policymakers prevent the emergence of the same vulnerabilities in telecommunications that developed in the energy sector. Today's European leaders are in the same position as Willy Brandt was in 1970, setting the foundation for a new economic relationship that would define Europe's economic and foreign policies for decades to come.

The five common characteristics described below begin to illustrate how policymakers in Europe may consider the problem of 5G dependence through the lens of their experience improving Europe's energy security.

Dependence on Russia for natural gas and on China for 5G are similar in five overarching ways:

1. Both 5G networks and natural gas have wide economic and societal reach and create security vulnerabilities for states and citizens alike.
2. Building 5G networks with Chinese companies or buying natural gas from Gazprom are situations in which commercial entities in democracies contract with entities taking directives from authoritarian governments.
3. Both 5G networks and natural gas pipelines are long-term infrastructure investments in which dependence can beget dependence.
4. Both 5G networks and natural gas pipelines create dependencies that run contrary to strategic alliances, pitting EU member states against each other and fracturing the transatlantic alliance.
5. Both 5G networks and natural gas pipelines put political and business elites at risk of being coopted by hostile states.

These common factors make both energy and telecommunications ripe for malign influence by authoritarian governments. Investments by authoritarian countries in both energy and telecommunications can put a country at risk of economic coercion. The Alliance for Securing Democracy defines economic coercion as the use of commercial, financial, or other economic tools and resources for foreign political purposes, including to establish dependencies that influence foreign governments, entities, or individuals. In addition, the reliance on authoritarian governments for technology can put countries at risk of cyber operations, which are the probing or penetration of computer networks or connected systems and devices to surreptitiously steal, alter, or collect data and/or to disrupt, manipulate, damage, or erode confidence in organizations, institutions, and processes.[55]

1. Wide Economic Reach and Security Implications

Both natural gas and 5G networks have wide economic reach and huge impact across the European Union. Natural gas has a variety of uses, from residential and district heating to industrial processes such as petrochemical and fertilizer production. Accordingly, a price spike or interruption in natural gas supply would have far-reaching effects. Even small increases in gas prices could leave households and employers unable to make ends meet. At worst, if natural gas supplies are cut off, households and manufacturers would be left cold and unable to continue production. When Russia cut off gas transit to Europe during a dispute with Ukraine in January 2009, households in the Balkans were left without heat, and Hungary and Slovakia suffered economic consequences.[56]

In practice, this means that without effective competition or a diversity of suppliers, the single supplier of natural gas wields significant influence over the business and political establishment of a dependent country. The European Commission charged Gazprom with using its dominant market position to impose unfair pricing, conditions, and territorial restrictions on its gas flows in an anti-trust investigation.[57] In addition, dependency in the

energy sector can lead elites to fear the economic consequences of offending the gas supplier. In Lithuania, for example, officials suspect that an alleged accident in a Russian crude oil pipeline supplying a Lithuanian refinery may have been purposely created to punish the country for selling the refinery to Polish rather than Russian buyers.[58]

5G technology will be more fundamental to European economies than natural gas has been in the past. 5G will transform not only personal communications and industrial manufacturing systems, but the newest generation of telecommunications technology will also affect sectors from health to transportation. And as in the case of natural gas, citizens' day-to-day lives can be disrupted by insecurity in the system. In the case of gas, price fluctuations could leave individuals unable to pay bills, but in the case of 5G, individual citizens' data privacy could be compromised by insecure 5G networks. Two data privacy risks that may be worsened by 5G networks are the risk of the exploitation of better geolocation data and the risk of poor data privacy management from an increased number of connected devices, including possibly insecure Internet of Things devices, and, generally, larger flows of data.[59] Large scale attacks are also possible. An interruption in 5G network coverage has the potential to fully paralyze society, halting traffic, stopping financial markets, and because of 5G-enable health care services, even putting lives at risk.

In the case of 5G networks, significant dependence on a single supplier, especially if that supplier acts in the interest of a hostile state rather than in a commercial manner, could have wide-reaching consequences. Among economic concerns, non-transparent pricing contracts in the telecommunications sector could result in an equipment supplier providing preferential rates for equipment in countries that are pursuing generally friendly policies towards the supplying state, or alternatively, punishing economic partners for unpopular decisions.

China's diplomats have already threatened European states with economic consequences in response to possible bans on Huawei. China's ambassador to Germany threatened consequences against Volkswagen and Daimler AG if Huawei were banned from Germany's 5G networks.[60] The same occurred in the United Kingdom after it banned Huawei in July 2020. China's ambassador to the United Kingdom threatened that investment from other Chinese companies in the United Kingdom could be compromised.[61]

As in the case of energy, which Russia uses as part of its hybrid toolkit to wield malign influence against its neighbors,[62] Europe could also face significant security consequences from dependence on China's 5G technology. NATO considers economic pressure and cyber-attacks, both of which can be executed through 5G networks, to be hybrid threats.[63] Although malicious 5G network cut-offs seem unlikely, such an eventuality cannot be ruled out. The EU's Coordinated Risk Assessment of 5G Network Security found that "hostile third countries may exercise pressure on 5G suppliers in order to facilitate cyberattacks serving their national interests. The degree of exposure to this risk is strongly influenced by the extent to which the supplier has access to the network."[64]

Because of the risks entailed in energy supply and information and communications technology disruptions, the EU considers these sectors as critical infrastructure.[65] But the situation is mixed on the national level and there is no consensus across the EU on this matter. Approximately half of the EU member states are considering adding future 5G infrastructure to critical infrastructure lists.[66]

2. Commercial Entities in Democracies Contract with Entities Beholden to Authoritarian Regimes

In both the cases of Gazprom and Huawei, European commercial entities contract with an authoritarian state's national champion. Nominally, both Gazprom and Huawei are also commercial actors. But the lines between the state and these companies is blurred.

Gazprom is majority owned by the Russian government and has a monopoly over pipeline natural gas exports. Other Russian energy companies are permitted to pursue only liquefied natural gas exports, with Novatek taking the lead.[67] This means that European countries have in the past, and will likely continue, to be able to buy pipeline gas only from Gazprom.

Huawei is nominally different but also is beholden to the state. According to the company, Huawei was founded in 1987 by its CEO Ren Zhengfei, and, according to the company's website, it is a "a private company wholly owned by its employees. […] No government agency or outside organization holds shares in Huawei."[68] But the true ownership of the company is unclear.[69]

In the case of Huawei, European policymakers should pay careful attention to the matter of control more than to questions of ownership. The government of China and the Chinese Communist Party are exerting ever greater control over private companies, especially in the tech and communications sectors. The size of Huawei gives it even greater significance. Private companies are required to have Chinese Communist Party branches within them.[70] And the government has passed laws that require private companies to cooperate on sensitive issues. The 2015 National Security Law requires cooperation "to maintain national security" and a cybersecurity law requires that network operators like Huawei provide "technical support and assistance" to the government on matters of national security.[71] Because of this legislation, it is increasingly difficult to view Huawei as a company independent from the Chinese government.

The similarities between Gazprom and Huawei also extend to the high importance both Russia and China place on these national champions. Gazprom and Huawei are crucial to the economic development of Russia and China, respectively.

In Russia, natural gas exports play an essential role in the federal budget. In 2018, oil and gas exports generated 46 percent of Russia's federal budget revenues. A drop in natural gas exports would directly affect the Russian economy.[72] In addition, the income from gas sales abroad subsidizes domestic natural gas prices.[73] An increase in the price of gas and heating could easily become an important domestic policy issue in Russia. These factors have led researchers in Europe and Russia to argue that "national sovereignty over energy resources is a political paradigm"[74] and that the "importance of natural gas exports for Russia is hard to overestimate."[75]

For China, its success in the telecommunications and tech sector is no less important for the future vision of China's economy than energy is in Russia. In 2015, the Chinese government launched an ambitious ten-year plan called "Made in China 2025" that seeks to make China self-sufficient and a global leader in high-tech manufacturing. Information and communications technology are core elements of the plan.[76] An add-on strategy referred to as "China Standards 2035" is in the works—and here Huawei is already leading the way.

Huawei has been very active in the standard-setting bodies that shape the development of 5G technology. Standard-setting bodies, including 3GPP and ETSI, are organizations that bring together all relevant stakeholders in the telecommunications sector and ensure the products and technologies they develop remain inter-operable and that, for instance, a smartphone manufactured in China using U.S. and Korean components will work properly in Europe. Through this process, one technology becomes the standard that all stakeholders adopt in their products and networks. In the standard setting process for 5G, Huawei submitted more proposals to the 3GPP standards body than any other company.[77]

Standard setting has historically been a technical process carried out by engineers from all major telecommunications companies, who assess competing technologies as objectively as possible before choosing one based solely on its effectiveness. There is reason to believe that Chinese companies' contributions to standard-setting bodies can serve to advance China's national interest rather than simply solve common technological challenges.

In 2016, at a standard-setting meeting, Chinese company Lenovo voted for a Qualcomm-sponsored technology, LDPC, against a Huawei alternative, polar coding. Yet Lenovo changed its vote months later in a vote on the second part of the standard, in which the same choice of polar coding technologies came up, after accusations of "treason" from angry Chinese netizens. Lenovo's 74-year old founder wrote an online apology letter in which he explained that: "We all agree that Chinese companies should be united and cannot be played off one another by outsiders."[78] This statement and principle run contrary to the principles that have governed these scientific bodies and show the transformative effect Chinese companies can have on industry.

Both Gazprom and Huawei are the international faces of their countries' economic strength, and as such, they play outsize roles in the existing and future economies of Russia and China. Both companies have significant importance for, and connections to, their home authoritarian governments. This makes these companies fundamentally different from the commercial actors they contract within Europe—whether that be a multinational energy company like Shell or a telecoms operator like Vodafone.

European private companies, whether telecommunications or energy, do not play the same economic and geopolitical roles in their home countries that Gazprom and Huawei do. And because European companies assume that their partners also fit their own profit-driven and independent model, it can be difficult for European commercial companies to decipher the geopolitical versus commercial actions of their contracting partners. Given the disparity between the partly state-driven approach to trade in Russia and China versus in democratic countries, it would be beneficial for democratic governments to assist commercial actors in navigating and countering the high-politics present in these transactions. Some capacity already exists in the U.S. Foreign Commercial Service and the European Commission's delegations, but greater understanding of the political risks involved need to be shared in boardrooms and not only at the operational level.

3. Long-Term Infrastructure Investments: Dependence Begets Dependence

The large scale and high costs of both energy and telecommunications infrastructure lead both to be long-term investments for private companies and governments alike. A pipeline or telecommunications network, once set up, will continue to function for decades to come. Today, the pipelines built under Willy Brandt's Ostpolitik continue to transport natural gas, and 3G and earlier generations of network technology run in parallel to newer 4G networks. Once a piece of infrastructure is built and set up, it is difficult to remove.

Apart from the ongoing physical presence of infrastructure, the commercial relationships also continue to grow and yield new cooperation on projects in both the energy sector and in telecommunications. Germany's initial agreement with the USSR on overland natural gas pipelines led to the further development of the Nord Stream and later the Nord Stream 2 undersea pipelines with Russia. These pipelines have created path dependency for Germany on natural gas—even though new sources of natural gas were available on the global market, its existing pipeline infrastructure made continuing cooperation with Russia simpler than developing alternative infrastructure. Only in 2018, under pressure from the Trump administration, did Germany begin plans to construct its first liquefied natural gas import terminal.[79]

The same perception of path dependency exists in telecommunications. Currently, Huawei and ZTE provide the radio access network equipment for 48 percent of European customers.[80] Telecoms operators argue that these existing relationships make switching between equipment manufacturers prohibitively costly, and that Europeans are essentially grandfathered into their relationship with Huawei. Vodafone executive Joakim Reiter argued that "European carriers long ago installed Huawei products throughout 3G and 4G networks … Removing Huawei from 5G means removing it from 4G and so forth. This would cost huge sums and take many years to accomplish."[81]

In the United Kingdom, where Chinese companies have a 40 percent share of the 4G radio access network (RAN) market,[82] a senior telecommunication executive with BT argued that removing Huawei equipment would be "impossible to do in under 10 years."[83] Because initial roll-outs of 5G infrastructure build on earlier 4G infrastructure, the costs for keeping Huawei equipment to a 35 percent share of the 5G markets would have nearly 500 million GBP.[84]

Some external experts dispute these claims. Analysis from Strand Consult argues that telecommunications operators will need to upgrade much of their equipment anyway, and "in general, European operators are facing the swap of 4G networks built between 2012 and 2016."[85] Because of this, "restricting access to Huawei and ZTE will not necessarily raise equipment prices, reduce rollout time, or reduce competition in the market." [86]

Infrastructure replacement is possible. Recently, operators in Netherlands and Denmark have fully switched out their 4G RAN equipment. TDC in Denmark replaced a 100 percent Huawei system with a 100 percent Ericsson system, and KPN in the Netherlands is making the reverse move.[87] European policymakers should understand that moving forward with Huawei on 5G networks can lead to ongoing dependence on Huawei infrastructure in 6G and future network generations, especially because 6G is thought to be very dependent on 5G networks. Even if switching infrastructure is technically possible, the exclusivity and extent of that infrastructure relationship could make the ability to switch to other suppliers in future generations more difficult.

4. Dependencies That Run Counter to Strategic Alliances and Interests

European unity and alliances are among the EU's greatest strategic strengths. Membership in the EU has given European states enormous power in trade and external matters. As a bloc, the EU is the largest economy in the world, and its single voice on trade allows member states to wield greater influence than they would individually. As a market with a population of over 500 million, the EU outranks most others including the United States.[88]

Most European countries are also part of NATO, and the six that are not have either partner status or are able to cooperate with the military alliance through formal NATO-EU cooperation. This cooperation is especially meaningful on hybrid threats and cyber security, for which the EU and NATO have established a significant number of common proposals under a joint declaration.[89]

Natural gas and 5G dependence on Russia and China undermine the bonds between European countries and their transatlantic allies. Both the questions of natural gas and 5G cooperation arose in the context of geopolitical conflict between the Western democracies and authoritarian states. Furthermore, both the questions of natural gas and 5G pit the EU and United States against each other and sow discord between European capitals.

Transatlantic conflict over Europe's natural gas supplies started during the Cold War, escalated during the Ukraine crisis, and continues today. While Western European nations supported the building of pipelines to the USSR, the Carter and Reagan administrations embargoed U.S. products and technology from use in the USSR's oil and gas transit infrastructure.[90] The Nord Stream 2 pipeline was born during the biggest crisis between transatlantic democracies and Russia since the Cold War and undermines EU and U.S. policies supporting Ukraine.[91] Gazprom and its Western partners Royal Dutch Shell, E.ON, and OMV signed the Memorandum of Understanding for Nord Stream 2 in 2015,[92] shortly after Russia's invasion of Crimea and the downing of flight MH17 in Ukraine. Russia chose this moment of political tension to pitch new energy ties to Europe, undermining existing transit routes through Ukraine. Germany's government lobbied in favor of the pipeline while U.S. officials spoke critically against it. The U.S. State Department's Special Envoy for International Energy Affairs Amos Hochstein argued to Europeans that the pipeline "compromised the concept" of the EU Energy Union.[93]

In 2020, transatlantic tensions over Nord Stream 2 have continued to rise. The United States levied sanctions on companies, including European companies, that would help Russia complete the Nord Stream 2 pipeline to Germany.[94] The sanctions heightened tensions between Germany and the United States at a time of already frayed transatlantic ties. U.S. Senators Ted Cruz, Tom Cotton, and Ron Johnson sent a letter to the German port

of Sassnitz threatening sanctions, leading German Foreign Minister Heiko Maas to criticize those who should be Germany's closest transatlantic partners.[95]

Tension over the construction of the Nord Stream 2 pipeline is rife within the EU as well. EU member states in Central and Eastern Europe are opposed to the Nord Stream pipelines fearing an increase in Europe's dependence on Russian natural gas and criticizing Europe's ongoing financial support to a hostile government. The Prime Minister of Poland Mateusz Morawiecki argued that the Nord Stream 2 pipeline "explodes the EU's energy policy from the inside."[96]

Just as natural gas pipelines to the USSR grew out of the Cold War, questions over China's 5G technology is emerging during rising tensions between the Western democracies and China. These tensions are most explicit between the United States and China. The United States sees China as a rising power with global ambitions that threatens the principles and interests of the U.S. and its allies. U.S. Secretary of State Mike Pompeo has drawn attention to the "fundamental political and ideological differences between" the United States and China and President Xi Jinping's "decades-long desire for global hegemony of Chinese communism."[97] The Trump administration is concerned about an unbalanced trade relationship, the stealing of intellectual property, China's strong and "more menacing" military, its human rights violations, especially in Hong Kong and Xinjiang, and what Secretary Pompeo deemed the Chinse Communist Party's insistence "on silence over its human rights abuses as the price of admission for Western companies entering China."[98]

The EU is focusing on many of the same things but has not taken as critical of a stance toward China. European Commission President Ursula von der Leyen has said that "the relationship between the European Union and China is simultaneously one of the most strategically important and one of the most challenging we have" and labeled China "a negotiating partner, an economic competitor and a systemic rival."[99] Like the United States, the EU is concerned about its unbalanced trade and investment relationship with China and China's human rights abuses in Xinjiang and Hong Kong.[100]

NATO for the first time is tracking threats China poses to the alliance. [101] In line with its traditional mission, NATO is concerned about China's military build-up. But increasingly, NATO sees China "coming closer" to the alliance, including through investments in infrastructure in NATO countries and in cyberspace, as NATO Secretary General Jens Stoltenberg has said. [102] In 2019, NATO Defense Ministers agreed to baseline security requirement for 5G and other telecommunications networks. These requirements fit into NATO's broader work to protect cyber infrastructure.[103]

The common transatlantic and European concerns over threats posed by China should be a point of cooperation. But instead, intra-EU and intra-NATO tensions are simmering over the question of 5G technology and China. The United States has pressed its European allies to reject Chinese 5G technology in a manner so forceful that it can be perceived as disrespectful. In an op-ed in Politico, U.S. Secretary of State Mike Pompeo argued that "it's critical that European countries not give control of their critical infrastructure to Chinese tech giants like Huawei, or ZTE."[104] Europe's choice of 5G technology is increasingly perceived, both by President Trump and Chinese officials, as a question of choosing sides between the United States and China in their trade war.[105]

The conflicts over natural gas and 5G serve hostile powers' aims to weaken the EU and NATO alliance. The Kremlin pursues policies that explicitly aim to weaken European ties and divide EU member states.[106] Sijbren de Jong argues that "Moscow, where possible, employs a tactic of 'divide and rule' whereby it either aims at weakening the centre (Brussels) by playing off Member States against one another, or undermine EU cohesion and coherence as a whole."[107] This is especially true in its use of natural gas policy, as illustrated through the Nord Stream 2 pipeline conflict and Russian offers to Italy and Greece to serve as gas hubs in Europe. [108]

China's policies also seek to downplay the role of the EU. Rather than engaging with powerful EU structures, China has launched bilateral and multilateral cooperation with individual EU member states or a group of member. China solicited the participation of individual EU member states in its Belt and Road Initiative (BRI), and Italy joined in 2019. This project, nominally an infrastructure network, is a vehicle for Beijing's geopolitical

influence around the world. Both EU and U.S. officials have expressed concern that Italy's involvement in BRI would jeopardize Europe's security.[109]

Similarly, China minimizes the significance of the EU through its 17+1 initiative, which brings together seventeen Central and Eastern European countries both from within and outside the EU. The European Court of Auditors has found that because China engages bilaterally with each of the seventeen smaller states in the framework, it "creates a risk to cohesion of EU action. In addition, the 17+1 framework may also affect the implementation of the EU policies in the Western Balkans as five countries in the 17+1 framework are Western Balkan states with candidate or potential candidate status."[110]

European policymakers should assess how the economic relationships they build with Russia and China fit into the countries' larger foreign policy aims. Europe's experience with Russia on energy provides many examples of efforts to divide the EU and NATO allies. The emerging economic relationship with China is beginning to follow the same paradigm.

5. Risk of Coopting Business and Political Elites

Commercial ties between Europeans on one side and Russia or China on the other not only build high-level strategic dependencies and vulnerabilities but also create countless personal and commercial relationships. These relationships can put European business and political elites at risk of being coopted by their authoritarian country counterparts.

The prime example of this is the cooption of former German Chancellor Gerhard Schroeder by the Russian energy sector. As chancellor from 1998 until 2005, Schroeder supported the development of natural gas ties between Germany and Russia and oversaw initial planning for the Nord Stream pipeline. Once Schroeder left office, he became chairman of the Nord Stream shareholders' committee and serves the same role for Nord Stream 2. In 2017, Schroeder became the chairman of Rosneft, Russia's largest oil company. While holding these roles, Schroeder continues to express political opinions over Germany's Russia policy. In particular, he has opposed sanctions against Russia for its invasion of Crimea.[111]

Schroeder's example shows that through expanding natural gas ties with Germany, Russia was able not only to establish a lucrative economic partnership but also gain a political ally at the top of one of Germany's most prominent political parties. Given Gerhard Schroeder's personal financial and career interest in the success of Russia's energy exports, his motivations for expressing views on Germany's foreign policy are suspect. But for many German voters, his opinions still carry the weight of a trusted head of state.

China uses similar tools. The Chinese Communist Party's approach to governing domestically focuses on "cultivating, co-opting, and coercing non-party elites" in a manner that ties "economic opportunity to political compliance," argues Matthew Schrader; the CCP is increasingly applying this approach abroad to foreign "countries, companies, organizations, and individuals."[112] This should be a worry for European countries in which China is seeking to invest. Some European states are already seeing the political fallout that comes from seeking closer economic ties to China. In September 2020, Chinese Foreign Minister Wang Yi threatened Czech Senate President Milos Vystrcil, saying the political should pay "a high prices" for visiting Taiwan.[113]

There also is growing evidence that Huawei can serve as an intermediary for the CCP and should therefore be viewed with greater scrutiny. Reports suggest that Huawei helped the governments of Uganda and Zambia interfere with political opponents encrypted communications.[114] In October 2020, the U.K. Parliament's defense committee announced that Huawei had colluded with the Chinese state.[115] European officials should be aware if companies working in their telecommunications networks are at risk of undermining democratic processes.

Recommendations to Prevent Undesirable Scenarios in Future 5G Networks: Lessons from the Energy Sector

European political leaders can apply lessons from EU energy policy to counter three undesirable scenarios in 5G rollout.

Undesirable Scenario 1: PRC Black Boxes in Future 5G Networks and Smart Infrastructure

In future telecommunications systems, European policymakers should seek to avoid Chinese vendor supplied and operated "black box" systems. A black box system is "a system for which we can only observe the inputs and outputs, but not the internal workings."[116]

A company will be able to set up smart infrastructure systems, including smart cities or other multi-sector services, through 5G networks.[117] And such systems could become "black boxes" in which local or national officials, and even the telecoms operators purchasing the systems, would lose oversight of the technology and standards used, and the manner, location, and terms under which data is managed. Because such systems could span multiple critical industries, from telecommunications and transportation to energy, the risk of breaches or malicious outages is especially high.

Similarly, European authorities should scrutinize not only 5G equipment vendors but apply the same criteria for network management and service provision. EU and national authorities should evaluate the full supply-chain role of high-risk vendors across not only 5G networks and the telecommunications sectors but across smart infrastructure broadly. A scenario in which a high-risk vendor provides network equipment and network management services approaches a "black box" paradigm under which no party in the system has an incentive to report security gaps and back doors.

Energy security examples show that transparency within the system is significant for ensuring security. European countries formerly had vertically integrated energy companies that generated (or produced/imported), transported, stored, and distributed natural gas. Consumers did not have much visibility into the system, nor were other actors able to enter the system to ensure competition. In a way, these twoo were black boxes. In this closed, non-transparent system European countries did not have the option of buying gas from suppliers other than Gazprom, they were subject to natural gas price spikes and supply interruptions. Once the EU unbundled the vertically integrated companies, a different reality became possible. Alternative natural gas suppliers, new supply routes, and other energy sources became accessible, and the natural gas sector became less susceptible to political manipulation.

In the natural gas sector, other technical solutions beyond unbunding helped achieve positive political outcomes. These included requiring third party access to infrastructure and the provision of EU funding for key infrastructure projects through the Projects of Common Interest mechanism. Policy and financial tools were key in order to develop infrastructure where market forces alone did not allow security-minded solutions to be built.[118]

Applicable Solutions:

- **Solution 1: The EU should recommend, and member states should set, nuanced limits on Chinese companies' and other high-risk vendors' roles in the full supply chain for 5G networks and future smart infrastructure.** These can either be blanket or partial bans in response to nuanced security assessments.

  These policies should be paired with efforts to build better public awareness of who owns, operates, and provides services to manage telecommunications and new technological infrastructure. These lessons could be included in cybersecurity and media literacy educational curricula already in place across the EU.

- **Solution 2: Where there is no blanket ban, the EU should set guidelines to unbundle the 5G and smart infrastructure value chain and networks to create competition, greater transparency, and incentives for reporting security breaches.**
- **Solution 3: The European telecommunications sector, like the energy sector, is fragmented into many small markets. This, and the generally poor financial position of many telecommunications operators, means that EU funding to subsidize the purchase of more secure equipment and facilitate regional cooperation on digital security could make a difference.**

Undesirable Scenario 2: Continued EU Fragmentation and Disunity on China Policy

The lack of EU leadership on China policy and the EU institutions' lack of insight into the terms of bilateral agreements between member states and China can lead to further fragmentation of European political unity. The Chinese government and private sector prefer to cultivate bilateral relationships with EU member states. Disparate policies on 5G security can lead to greater foreign policy fragmentation on larger geopolitical issues, from stances on Hong Kong to possible efforts to draw Europeans away from their transatlantic partners.

Russia has used divide-and-rule strategies against European countries for decades. The EU's Energy Union structures and policies provided the first meaningful counterweight to Russia's attacks. Under the previous European Commission, Vice President Maroš Šefčovič served as a single point of contact for all politically significant energy issues. He was given the power to broker very sensitive gas transit negotiations between Ukraine and Russia.[119] Because Europe had someone in change of energy security, it was easier for the EU to speak with a single voice.

The EU's 2014 Energy Security Strategy[120] and the Energy Union[121] prioritized the principle of solidarity between member states. This is especially significant given the nation-centric culture dominant in the sector. The EU made the principle more tangible through practical tools for improving cross-border, and especially, regional cooperation. Common EU stress tests in the natural gas supply security[122] and the provision of financial[123] and political support to cross-border projects showed member states how cooperation should work in practice. Finally, the EU made solidarity mandatory in the case of gas supply interruptions through new regulation on gas supply security. The new regulation put member states in "risk groups" tasked with coming up with solidarity measures for the group.[124]

Finally, the European Commission gained the ability to review intergovernmental agreements between EU member states and third countries on oil and gas deliveries. This allows the EU to catch issues around anti-competitive practices and supply security before deals are signed.[125] Importantly, this also established the EU as an important power in energy agreements, obstructing Russia's strategy of sidelining Brussels and pursuing asymmetric deals with individual states.

Applicable Solutions:

- **Solution 1: The European Commission should designate clearer leadership on the political dimensions of 5G and digital technology security, creating a single point-of-contact for challenging tech and telecommunications related to China rather than a division of labor between many commissioners.**

  At the moment, there is insufficient clarity about where responsibility lies between Executive Vice Presidents Vestager (responsible for A Europe Fit for a Digital Age) and Dombrovskis (An Economy that Works for People—Trade), and HR/VP Borrell (A Stronger Europe in the World).
- **Solution 2: The European Commission should improve mechanisms, and provide financial support, to promote cooperation on 5G security and smart technology at the EU, regional, and global levels.**

  The energy security model of regional risk groups and greater funding for regional and cross-border projects would bolster a common risk perception and security approach across EU member states.

Furthermore, the EU already funds standards-setting bodies. As these bodies gain greater geopolitical significance, they would benefit from greater political attention and security-minded guidance. This is an area where the EU has influence through its existing funding but does not yet use it.

- **Solution 3: There should be greater EU oversight of member state bilateral memorandums of understanding (MOUs) with China.** The European Commission has very little oversight or awareness of the content of bilateral MOUs signed between member states and China.[126] Attaining a formal right of review in such agreements would limit China's ability to sideline the EU and wield disproportionate power in negotiations.
- **Solution 4: Europeans should not go it alone.** The European Union should move together strategically, as it aimed to do in the Energy Union, rather than adopt a piecemeal approach to 5G policy. Fragmentation is exploited by authoritarian states in their economic policies, as shown by the 17+1 and Belt and Road Initiative.

  Europe should also build coalitions of democracies for smart technology with global partners, including the United States, United Kingdom, Australia, New Zealand, India, South Korea and others who support democratic norms.

Undesirable Scenario 3: Loss of European Champions in Future Technology, Leading to Full Technological Dependence

Having a choice of 5G suppliers depends on European telecommunications technology companies continuing to survive in a market in which Chinese companies benefit from state assistance. European policymakers should fight to avoid a scenario is which Huawei and other Chinese manufacturers push Ericsson and Nokia out of business, leaving Europe dependent on China for future generations of technology.

This is not an outlandish possibility. In 2000, the two biggest telecommunications equipment firms were North American:Lucent and Nortel. Less than a decade later Nortel went bankrupt and Lucent was diminished and sold off. What led to their downfall, according to Robert Atkinson, the President of the Information Technology and Innovation Foundation, was that the U.S. government did not view the sector as strategic and did not protect and promote these companies. Instead, free market policies pushed for greater competition and weakened these former champions.[127]

Huawei has thrived because of government support. The government has helped Huawei through low-cost financing through government banks, tax reductions for the tech sector, the designation of being a National Key Laboratory, and other benefits.[128] The Wall Street Journal estimated the support to be worth over $75 Billion over the past 25 years.[129]

The energy sector has been through a similar catastrophe in Europe and can provide lessons for keeping European companies in business. In the 2000s, Germany had a 20 percent share of the global solar energy market.[130] In 2017, SolarWorld, the last solar cell manufacturer in Germany, once a global leader, succumbed to Chinese competition.[131] Years earlier, SolarWorld's officials warned that because "The Chinese offer their customers a price that's below cost […] the Chinese government forces the good, technologically advanced companies into a dire financial straits so they can ultimately monopolize the market."[132]

The European Commission aimed to help the solar industry against China's competition through an anti-dumping investigation[133] and the imposition of anti-dumping tariffs against Chinese solar panels.[134] But these measures came too late for many solar panel manufacturers. European industry now needs to play catch-up against American and Asian manufacturers.[135]

Applicable Solutions:

- **Solution 1: The European Union and member states should address European companies' concerns over unfair competition.** Telecommunications should be considered a high-priority industry for the EU and for member states. The EU and member states should support European industry by investigating anti-competitive practices from authoritarian countries in a timely manner. The EU's help for the solar industry came too late and put the EU at a disadvantage against foreign competitors. The security implications of failing to be a strong player in the telecommunications technology sector would be much greater than those of losing the lead in solar panel manufacturing.
- **Solution 2: The European Union and member states should cooperate with like-minded countries to ensure a diversity of democratic country technology suppliers.** Consultation and open dialogue on the risks of authoritarian-country technology with Australia, New Zealand, the United States, Canada, South Korea and other democracies can help move forward the debate on 5G from a conversation about costs to a conversation about the hidden risks of interference. Such open, global conversations can shape consumer behavior as well.
- **Solution 3: The European public and private sector should watch out for hidden costs in setting up new technology.** As in the case of solar panels, the public and government can become excited about new technology and fall for the promise of obtaining that technology at very low prices from Chinese companies. But both the public and private sectors should watch out for the hidden costs, including the costs of replacing the infrastructure early if security flaws are found and potentially higher costs for security management in systems built on high-risk vendor equipment.

Endnotes

1 For example, the Reagan administration: Richard Nephew, Transatlantic Sanctions Policy : From the 1982 Soviet Gas Pipeline Episode to Today, Center on Global Energy Policy, Columbia University, 22 March 2019.
2 Eurostat, "EU imports of energy products - recent developments," June 2020.
3 Andrius Sytas, "EU leaders sign letter objecting to Nord Stream-2 gas link," Reuters, 16 March 2016.
4 Euractiv and AFP, "Challenging Germany, US opens way for sanctions on Russia pipeline," Euractiv, 16 July 2020.
5 BBC News, "Anger as German ex-chancellor Schroeder heads up Rosneft board," 19 September 2017.
6 Rem Koreweg, Energy as a tool of foreign policy of authoritarian states, in particular Russia, Study Requested by the European Parliament's Committee on Foreign Affairs., European Parliament, 27 April 2018.
7 Reuters, "Timeline: Gas crises between Russia and Ukraine," 11 January 2009.
8 European Commission, Third Energy Package, 16 March 2020.
9 European Commission, Energy Union, 31 July 2020.
10 Elsa Kania, "Securing Our 5G Future: The Competitive Challenge and Considerations for U.S. Policy," Center for New American Security, November 2019.
11 European Commission, "The Commission adopts Implementing Regulation to pave the way for high capacity 5G network infrastructure," Digibyte, 30 June 2020.
12 BBC News, "What is 5G and what will it mean for you?," 28 January 2020.
13 European Commission and 5GPPP, 5G Empowering Vertical Industries, February 2016, available from European Commission, "More than smartphones: White paper shows how 5G will transform EU manufacturing, health, energy, automotive, media & entertainment sectors," 22 February 2016.
14 Ryan Madder, "Robot surgery could be the future of health care in remote areas," Fortune, 11 February 2020.
15 European Commission and 5GPPP, 5G Empowering Vertical Industries.
16 European Commission, Towards 5G, 23 June 2020.
17 European Commission and 5GPPP, 5G Empowering Vertical Industries. p. 12-13.
18 Elsa Kania, "Securing Our 5G Future," p.7.
19 Australian Ministry of Home Affairs and Ministry for Communications and the Arts, "Government Provides 5G Security Guidance to Australian Carriers," Press release, August 23, 2018.
20 Federal Register, "Addition of Certain Entities to the Entity List and Revision of Entries on the Entity List," 21 August 2019.
21 David Shepardson and Karen Freifeld, "China's Huawei, 70 affiliates placed on U.S. trade blacklist," Reuters, 16 May 2019.
22 The White House, Executive Order on Securing the Information and Communications Technology and Services Supply Chain, 15 May 2019.
23 Chaim Gartenberg, "Donald Trump extends Huawei ban through May 2021," The Verge, 13 May 2020.
24 David Shepardson and Karen Freifeld, "Trump extends U.S. telecom supply chain order aimed at Huawei, ZTE," Reuters, 13 May 2020.
25 Sherisse Pham, "New sanctions deal 'lethal blow' to Huawei. China decries US bullying," CNN Business, 18 August 2020.
26 U.S. Department of Commerce, "Commerce Department Further Restricts Huawei Access to U.S. Technology and Adds Another 38 Affiliates to the Entity List," 17 August 2020.
27 Dan Sabbagh and Lily Kuo, "Huawei to be stripped of role in UK's 5G network by 2027, Dowden confirms," The Guardian, 14 July 2020.
28 Gov.UK, "Huawei to be removed from UK 5G networks by 2027," 14 July 2020.
29 NIS Cooperation Group, Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity, European Commission, July 2020.
30 Strand Consult, Understanding the Market for 4G RAN in Europe: Share of Chinese and Non-Chinese Vendors in 102 Mobile Networks: Version 1.2, p. 16.
31 Strand Consult, Understanding the Market for 4G RAN in Europe, p. 40.

32 European Council, European Council Meeting (21 and 22 March 2019) Conclusions, EUCO 1/19, 22 March 2019.
33 European Commission, Commission Recommendation of 26 March 2019 on Cybersecurity of 5G networks C(2019) 2335 final, 26 March 2019.
34 European Union Agency for Cybersecurity (ENISA), "Report on the EU 5G Toolbox Implementation by Member States Published," 24 July 2020.
35 European Commission, EU-wide coordinated risk assessment of 5G networks security, 9 October 2019.
36 NIS Cooperation Group, Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity, European Commission, July 2020, p. 4.
37 NIS Cooperation Group, Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity, July 2020. p. 6.
38 U.S. Department of State, The Clean Network, Accessed 05 October 2020; Matthew Lee, "Pompeo, in Slovenia, pushes 5G security, warns about China," ABC News, 13 August 2020.
39 The Economist, "America's war on Huawei nears its endgame," 16 July 2020.
40 Guy Chazan and Nic Fildes, "Germany crackdown set to exclude Huawei from 5G rollout," The Financial Ties, 30 September 2020.
41 Reuters, "Huawei asks Germany not to shut it out of building 5G networks - Der Spiegel," 31 July 2020.
42 Mathieu Rosemain and Gwénaëlle Barzic, "Exclusive: French limits on Huawei 5G equipment amount to de facto ban by 2028," Reuters, 22 July 2020.
43 Laurens Cerulus, "Belgium to cut down on Huawei gear," Politico, 25 June 2020.
44 Supantha Mukherjee and Mathieu Rosemain,"Huawei ousted from heart of EU as Nokia wins Belgian 5G contracts," Reuters, 9 October 2020.
45 European Commission Market Observatory for Energy, Quarterly Report on European Gas Markets, Volume 13 Issue 1, First Quarter 2020.
46 Eurostat, Extra EU-27 imports of natural gas from main trading partners, 2018 and 2019 v2, 08 July 2020.
47 Eurostat, EU Imports of Energy Products – Recent Developments, June 2020, p. 11.
48 Aurélie Bros, Tatiana Mitrova, and Kirsten Westphal, German-Russian Gas Relations: A Special Relationship in Troubled Waters, Stiftung Wissenschaft und Politik, December 2017, p.5.
49 Ibid.
50 Damien McGuinness, "Nord Stream 2: Why Germany may pull plug on Russian pipeline," BBC News, 9 September 2020.
51 European Commission, Statement of Vice-President Maroš Šefčovič on the positive outcome of trilateral gas talks, 20 December 2019.
52 European Commission, Third Energy Package, 19 March 2020.
53 Eurostat, "Main suppliers of natural gas and petroleum oils to the EU," EU Imports of Energy Products – Recent Developments, June 2020.
54 European Commission, Energy Union, 31 July 2020.
55 Alliance for Securing Democracy Team, A Note on Coming Updates to the Authoritarian Interference Tracker, 17 June 2020.
56 Simon Pirani, Jonathan Stern and Katja Yafimava, The Russo-Ukrainian gas dispute of January 2009: a comprehensive assessment, NG 27, Oxford Institute for Energy Studies, February 2009. f
57 European Commission, Antitrust: Commission sends Statement of Objections to Gazprom for alleged abuse of dominance on Central and Eastern European gas supply markets, Press Release, 22 April 2015.
58 Judy Dempsey, "Lithuanians suspect Russia of dirty tricks - Europe - International Herald Tribune," The New York Times, 7 August 2006.
59 GSMA, GSMA, 5G and Data Privacy: An Overview for Policymakers, July 2020.
60 Tony Czuczka and Steven Arons, "China Threatens Retaliation Should Germany Ban Huawei 5G," Bloomberg, 15 December 2019; Matt Schrader, Friends and Enemies: A Framework for Understanding Chinese Political Interference in Democratic Countries, Alliance for Securing Democracy, 22 April 2020, p. 6
61 Guy Faulconbridge and Martin Quin Pollard, "China warns UK: 'Dumping' Huawei will cost you," Reuters, 15

July 2020.
62 Michael Ruehle and Julijus Grubliauskas, "Energy as a Tool of Hybrid Warfare," NATO Energy Security Center of Excellence, 19 May 2015.
63 NATO, "NATO's Response to Hybrid Threats," 8 August 2019.
64 European Commission, EU-wide coordinated risk assessment of 5G networks security, p. 27.
65 Official Journal of the European Union, COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, 23 December 2008; Commission of the European Communities, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" {SEC(2009) 399} {SEC(2009), 400}, COM(2009) 149 final, 30 March 2009.
66 Conversation with EU official.
67 James Henderson and Vitaly Yermakov, Russian LNG: Becoming a Global Force, NG 154, Oxford Institute for Energy Studies, November 2019.
68 Huawei, Our Company, 2020.
69 Raymond Zhong, "Why Owns Huawei? The Company Tried to Explain. It Got Complicated," The New York Times, 25 April 2019.
70 Lindsay Maizland and Andrew Chatzky, Huawei: China's Controversial Tech Giant, Council on Foreign Relations, 6 August 2020.
71 Ashley Feng, "We Can't Tell if Chinese Firms Work for the Party," Foreign Policy, 7 February 2019.
72 Vladimir Kutcherov, Maria Morgunova, Valery Bessel, and Alexey Lopatin, "Russian natural gas exports: An analysis of challenges and opportunities," Energy Strategy Reviews, Vol. 30, July 2020.
73Aurélie Bros, Tatiana Mitrova, and Kirsten Westphal, German-Russian Gas Relations: A Special Relationship in Troubled Waters.
74 Ibid.
75 Vladimir Kutcherov, Maria Morgunova, Valery Bessel, and Alexey Lopatin, "Russian natural gas exports: An analysis of challenges and opportunities."
76 James McBride and Andrew Chatzky, "Is 'Made in China 2025' a Threat to Global Trade?" Council on Foreign Relations, 13 May 2019.
77 Hideaki Ryugen and Hiroyuki Akiyama, "China leads the way on global standards for 5G and beyond," Financial Times, 5 August 2020.
78 Lindsay Gorman, "The U.S. Needs to Get in the Standards Game-With Like-Minded Democracies," Lawfare Blog, 2 April 2020.
79 Ariel Cohen, "Germany's First LNG Terminal is the Right Move for Europe's Energy Security," Forbes, 13 November 2018.
80 Strand Consult, Understanding the Market for 4G RAN in Europe: Share of Chinese and Non-Chinese Vendors in 102 Mobile Networks: Version 1.2, p. 16.
81 Joakim Reiter, "5G After Covid-19," *Lawfare Blog,* April 16, 2020.
82 Strand Consult, Understanding the Market for 4G RAN in Europe: Share of Chinese and Non-Chinese Vendors in 102 Mobile Networks: Version 1.2, p. 40.
83 Mark Sweney, "BT boss warns of outages and security risks if UK ditches Huawei," The Guardian, 13 July 2020.
84 Ibid.
85 Strand Consult, Understanding the Market for 4G RAN in Europe: Share of Chinese and Non-Chinese Vendors in 102 Mobile Networks: Version 1.2, p. 7
86 Ibid, p. 14.
87 Ibid, p. 4.
88 European Commission, EU Position in World Trade, 18 February 2019.
89 European External Action Service, EU-NATO Cooperation, June 2020.

90 Gary H. Perlow, "Taking Peacetime Trade Sanctions to the Limit: The Soviet Pipeline Embargo," Case Western Reserve Journal of International Law, Volume 15, Issue 2, 1983; George C. Wilson, "U.S. Clears Way for Soviet Buy of Pipeline Gear," The Washington Post, 18 November 1980.
91 Georg Zachmann, "Nord Stream 2: A Bad Deal for Germany and Eastern Europe," Energy Post, 11 July 2016; Radio Free Europe Radio Liberty, "EU Summit Turns Focus To Nord Stream 2," 18 December 2015.
92 Gazprom, "Gazprom, E.ON, Shell and OMV agree upon developing gas transmission capacities to deliver Russian gas to Europe," 18 June 2015.
93 Pavol Szalai, "US energy envoy: North Stream 2 could resurrect cold war divisions," Euractiv, 1 August 2016.
94 Radio Free Europe/Radio Liberty, "U.S. House Approves More Sanctions Related To Nord Stream 2," 21 July 2020.
95 Deutsche Welle, "Nord Stream 2: Germany 'displeased' at US sanctions threat," 10 August 2020.
96 Alexandra Brzozowski, "Polish PM: Nord Stream 2 blows up EU energy policy 'from inside'," Euractiv, 14 September 2020.
97 U.S. Department of State, "Communist China and the Free World's Future," Speech by Michael Pompeo, Secretary of State, 23 July 2020.
98 Ibid.
99 Ursula von der Leyen, State of the Union 2020, European Commission, 16 September 2020, p. 5.
100 Ursula von der Leyen, State of the Union 2020, p. 6.
101 NATO, London Declaration, 4 December 2019.
102 NATO, Press Conference by NATO Secretary General Jens Stoltenberg following the meetings of NATO Defence Ministers, 17 June 2020.
103 Mircea Geoană, Speech by NATO Deputy Secretary General Mircea Geoană at the CYBERSEC GLOBAL 2020 virtual conference, September 28, 2020.
104 Michael R. Pompeo, "Europe must put security first with 5G," Politico, 2 December 2019.
105 The Economist, "America's war on Huawei nears its endgame," 16 July 2020.
106 Geir Hågen Karlsen, "Divide and rule: ten lessons about Russian political influence activities in Europe," Palgrave Communications 5, 19, 2019.
107 Sijbren de Jong, Confuse, Divide and Rule - How Russia Drives Europe Apart, IES Policy Brief Issue 2016/2, March 2016. p. 1.
108 Ibid.
109 Andrew Chatzky, "China's Belt and Road Gets a Win in Italy," Council on Foreign Relations, 27 March 2019.
110 European Court of Auditors, The EU's response to China's state-driven investment strategy, Review no. 3, 2020, p. 42.
111 BBC News, "Anger as German ex-chancellor Schroeder heads up Rosneft board."
112 Matt Schrader, Friends and Enemies, p. 12.
113 Euronews, AP, AFP, "China threatens retaliation after Czech delegation visit to Taiwan," Euronews, 31 August 2020.
114 Matt Schrader, Friends and Enemies, p. 14.
115 Reuters, "UK parliament committee says Huawei colludes with the Chinese state," 8 October 2020.
116 Dallas Card, "The "black box" metaphor in machine learning," Towards Data Science, 5 July 2017.
117 Hideaki Ryugen and Hiroyuki Akiyama, "China leads the way on global standards for 5G and beyond," Financial Times, 5 August 2020.
118 European Commission, Commission publishes 4th list of Projects of Common Interest – making energy infrastructure fit for the energy union, 31 October 2019.
119 European Commission, "Statement of Vice-President Maroš Šefčovič on the positive outcome of trilateral gas talks," Press Release, 20 December 2019.
120 European Commission, Communication from the Commission to the European Parliament and the Council - European Energy Security Strategy, {SWD(2014) 330 final}, COM(2014), 28 May 2014.
121 European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment

Bank - A Framework Strategy for a Resilient Energy Union with a Forward-Looking Climate Change Policy, COM/2015/080 final, 25 February 2015.
122 European Commission, Stress tests: cooperation key for coping with potential gas disruption, 16 October 2014.
123 European Commission, Commission publishes 4th list of Projects of Common Interest – making energy infrastructure fit for the energy union.
124 Ruven Fleming, "A legal perspective on gas solidarity," Energy Policy, Volume 124, January 2019.
125 Voice of America, "EU Nations Agree to Let European Commission Review Oil, Gas Deals," 7 December 2016.
126 European Court of Auditors, The EU's response to China's state-driven investment strategy.
127 Robert Atkinson, "Who Lost Lucent?: The Decline of America's Telecom Equipment Industry," American Affairs, Volume IV, Number 3, Fall 2020.
128 Ibid.
129 Chuin-Wei Yap, "State Support Helped Fuel Huawei's Global Rise," The Wall Street Journal, 25 December 2019.
130 Insa Wrede, "Chinese exports crushing German solar industry," Deutsche Welle, 16 June 2012.
131 Julian Wettengel, "Last major German solar cell maker surrenders to Chinese competition," 11 May 2017.
132 Insa Wrede, "Chinese exports crushing German solar industry."
133 Yu Chen, EU-China Solar Panels Trade Dispute: Settlement and Challenges to the EU, European Institute for Asian Studies, June 2015.
134 European Commission, EU imposes provisional anti-dumping tariffs on Chinese solar panels, Press Release, 4 June 2013.
135 European Commission, Mass-produced European solar panels on the horizon, 19 June 2020.