Summary
Beyond 5G: The Need for Trusted and Secure Digital Infrastructure

On 9 October 2023, a group of officials, academics and industry experts from different European countries gathered in Berlin to discuss the security of European critical digital infrastructure. The event titled "Beyond 5G: The Need for Trusted and Secure Digital Infrastructure" was co-organized by the German Marshall Fund of the United States and the Digital Society Institute at ESMT Berlin and was hosted in the GMF Office. The discussion provided valuable new perspectives relevant to the current 5G debate in Germany and identified best practices.

In Europe, the focus on 5G security has shifted from technical aspects to a broader concern encompassing political and strategic considerations, with a particular emphasis on distinguishing between trusted and high-risk vendors. This change highlights the significance of factoring in the geopolitical implications of economic choices. Digital infrastructure has now become indispensable for society, the economy, and governmental operations, presenting security challenges, such as surveillance and espionage. At the same time, it can create valuable opportunities for enhanced protection; for example, the Ukrainian parliament's decision to migrate government data to the cloud at the beginning of the Russian Invasion has ensured continued operations of Ukrainian infrastructure and safeguarded critical information.

Europe is currently grappling with substantial security challenges rooted in geopolitical competition and instability, as authoritarian regimes openly challenge democratic systems, blurring the lines between peace, crisis, and conflict. China's global power ambitions extend to key areas like 5G, undersea cables, and cloud computing and thereby pose significant risks to European digital infrastructure security. To effectively counter these threats, a long-term security approach is needed, requiring continuous legislative efforts in accordance with a "strategic competition mindset" as well as investments in resilient digital ecosystems. In addition, measures like strengthening research and development, screening foreign direct investments, and limiting untrusted vendors are essential steps. Protecting privacy and ensuring the proper functioning of economies and governments are key objectives.

The UK's approach to 5G security is marked by a comprehensive strategy that prioritizes cybersecurity and seeks to reduce reliance on high-risk vendors through the Telecommunications (Security) Act of 2021 and the National Cyber Strategy 2022. This approach involves close collaboration with telecom operators, setting clear deadlines for limiting high-risk vendor involvement, and maintaining open communication across ministries. The ultimate aim is to ensure network security by having the capacity to restrict high-risk vendors. Sweden's response to 5G security was initiated by the Swedish national regulatory telecom authority's decision in October 2020 to effectively exclude high-risk vendors, phasing out their equipment by January 2025. The amendments to Sweden's Electronic Communication Act enable the exclusion of high-risk vendors for national security reasons, reducing dependence on high-risk vendors. The Swedish case also underscores China's ability to flexibly adjust European vendor's market share in China in response to actions in Europe and highlights the need for a European coordinated, evidence-based cybersecurity approach in telecommunications. In the meantime, European vendors' market share in China has slipped to lower single digit.

In the EU, the Digital Compass introduced ambitious goals to improve digital infrastructure by 2030. However, a significant connectivity gap persists, necessitating over 200 billion euros in

investments to bridge it, despite measures like the Gigabit Infrastructure Act. Additionally, misconceptions about 5G have complicated matters in Europe, including the belief in a limited number of vendors, concerns about infrastructure replacement costs, and the perceived delays caused by excluding high-risk vendors. Germany, a major EU player, holds a significant share of the 5G Radio Access Network (RAN) but faces challenges. Addressing these issues is vital to ensure the security and independence of Europe's digital infrastructure, particularly in the face of potential disruptions from China – potentially in coordination with an ever aggressive Russia.

The digital infrastructure challenges faced by Germany and Europe are complex and have resulted in extensive political debates. While concerns over 5G security and the presence of Chinese vendors are significant, policymakers often overlook the digital infrastructure of other critical sectors such as banking and renewable energy. Particularly worrying is Germany's reliance on high-risk vendors, especially within transportation and critical infrastructure sectors. Generating more than a quarter of the EU's GDP, Germany holds a substantial share of the 5G Radio Access Network (RAN). Despite committing itself to implementing the EU's 5G Toolbox, German telecom operators have made commercial decisions to rely on high-risk vendors, posing challenges to achieving the EU's digital infrastructure objectives. Concerns in Germany about potential Chinese retaliation have further caused delays in decision-making highlighting that existing dependencies on China may already have an unduly large influence even on decisions that directly impact the security of the country and of the EU and NATO. This underscores the need for more comprehensive security strategies.

The US is advocating for the introduction of "OpenRAN" to mitigate security challenges. While US support for Open RAN is notable, it may not fully align with the EU's interests. Also, the emergence of private companies controlling critical infrastructure such as Starlink highlight the increasing interdependence of civilian and military digital infrastructure, as well as creating new risks as Elon Musk's actions in Ukraine have demonstrated. To effectively address these challenges, there is a pressing need for more data and independent knowledge concerning the security of digital infrastructure in Europe. Additionally, governments must enhance their capacity to assess risks and make well-informed decisions.

Although the event was called "Beyond 5G," much of the discussion was spent on 5G networks, not least due to Germany's continued reluctance for decisive action, fearing retaliation from China. However, the workshop also showed that in dealing with high-risk vendors, it is smarter to act earlier and more decisively to avoid the costs of retroactive "de-risking" and to set the right expectations for vendors from the outset. European countries would do well to learn from one another. While fear of retaliation is understandable, it also underlines the expectation that China is willing to exploit dependencies and therefore further confirms the need for de-risking. A key lesson is that the EU needs to act together to deter possible countermeasures.