China, 5G, and Alliance Security Beyond the 2021/22 NATO Summits

This summary presents the key points drawn from a roundtable organized by GMF and held under the Chatham House rule, which brought together experts from Europe and the United States to explore how broad questions around China, 5G, resilience, and critical infrastructure were being addressed in the context of NATO. The roundtable was held in 2021 but the conclusions and analysis were updated following the invasion of Ukraine and NATO's 2022 Madrid summit.

- The Russian invasion of Ukraine underlines NATO's indispensable role for the security of European allies, while China's announcement of a "no limits" partnership with Russia has demonstrated the wider spectrum of threats that NATO now has to take into account. It reinforces the imperative to ensure that NATO is well adapted to all dimensions of the new security environment that it confronts.
- From the major trifecta of summits around President Joe Biden's visit to Europe during the summer 2021 and the 2022 Madrid summit, it has become clear that China will occupy a central role in the transatlantic relationship in the years ahead. China now intersects with NATO's agenda in several ways, occupying a far more entrenched part of the discussion there than ever before. While NATO is not in a military conflict with China, China remains a key geopolitical competitor to the West as a whole. Moreover, the United States sees China as a direct national security threat and there are several plausible contingencies that would draw the two sides into military confrontation. Even if there is division in Europe on the matter, European allies in NATO have traditionally assumed part of the US security and defense agenda in exchange for security guarantees. However, China also poses a set of distinctly European security risks. A particular question relates to resilience and critical infrastructure, given the considerable dependency of Europe's digital infrastructure on Chinese technology. The current debate lies in whether NATO is the optimal platform to address those issues, if the EU should take a more active role instead, or if there is an appropriate division of responsibilities between them.
- Telecommunications have been identified by NATO as a new focus area. In order to deliver on its key mission of collective defense, NATO needs stronger infrastructure to withstand hybrid interference. Yet, infrastructure is typically privately owned in most European countries. This makes it susceptible to external interference and drives economic decisions that can neglect national security aspects if not clearly regulated by law. Russia is one state actor that resorts to various types of hybrid tactics on NATO territory. However, China has also begun to use various sophisticated political and non-military tactics vis-à-vis NATO as a whole and individual countries to spread its political and economic influence.
- For resilience to be the catalyst of closer NATO-EU cooperation, a balance must be found where the roles of both organizations are explicitly defined. Nowadays, NATO is adopting a more robust framework, including in the non-military dimension. NATO is mostly about political coordination and consultation, crisis management and collective defense, as well as interoperability. On the other hand, the EU has a range of regulatory instruments at its disposal, from the 5G Toolbox to the European Democracy Action Plan, which address some of the wider resilience issues. As such, common ground and shared responsibilities between the EU and NATO should be determined, and closer linkages between traditional military capability planning and resilience requirements must be established as this will be one of the key pillars for the future of NATO-EU cooperation.
- Uncertainty remains as to whether protecting civilian infrastructure in Europe would fall under the scope of NATO. In other words, would a cyberattack on civilian infrastructure in Europe trigger Article Five? If not, is it the EU's competence instead? Further, the lines between civil and military infrastructure are blurred, especially when

it comes to telecommunications.

- Telecommunications are assuming greater importance for the functioning of our societies and economies, as well as providing the basis and future of innovation. These two dimensions are subsequently linked in the race for technological supremacy. Technology has been and will be the key to deterrence and defense. Technological dominance ensures not only battlefield supremacy but also supremacy beyond it. Such dominance is contingent on a robust and constantly advancing industrial base that integrates civilian and military innovation, research, and development. Joint innovation initiatives across the Atlantic to maintain and heighten critical capabilities on and off the battlefield are needed. This requires better and more efficient linkages between military and civilian industries. NATO needs to find smart ways of integrating the economic dimensions that underpin elements of its security policies, particularly as industrial strategy comes to the fore of thinking again in Europe and the United States. New political channels must be built to facilitate such integration in order to strengthen the alliance's resilience and maintain its competitive edge.

- For now, it does seem like NATO is struggling with this role. Hence, precision is needed in identifying and categorizing issues falling under its scope. A first step for politicians is to set up clear parameters in areas where business with China would not compromise national security. NATO is also a natural platform to hold security exchanges with various institutions, non-state entities, and NATO partners that are experienced with dealing with China, such as Japan and South Korea. Thereby NATO should continue to prioritize digital infrastructure (5G/advanced, undersea cable, etc) and China, keeping both high on its agenda.

- Given that cyber threats have been a long-standing concern area for NATO, 5G networks have naturally become a focus for NATO discussions—even if its defense dimensions have slowly been put on the agenda. In addition, how data is processed and stored is a key security area that must not become a blind spot. Protecting our public sector and our industries, along with ensuring that companies, citizens, and government institutions have the possibility of sending their traffic end-to-end to a non-Chinese network is at the heart of the matter. In 5G for instance, cloud infrastructure will play a significant role. Under Chinese law, the Chinese government can request and be granted access to the data of any private company in China, putting at risk all data on a Chinese 5G cloud. To take the example of Belgium, all of its telecom infrastructure was previously reliant on Chinese equipment, including mobile communications used by the EU and NATO administrations. Similarly, Chinese equipment today permeates Germany's networks—meaning that the mobile traffic of basically all NATO troops based in Germany goes, at some point, through network reliant on Chinese technology. The new German IT Security law rightly refers to the security needs of NATO when it comes to assessing the trustworthiness of vendors. It also shows that ambitions and implementation could diverge greatly: since the law last year entered into force, Huawei's share in Deutsch Telekom's (DT) 5G network has risen to well above 60 percent. In 2020, DT's cloud, built and run by Huawei, has the Nuclear Research Center (CERN) in Switzerland as a key reference customer upon its launch. In other words, the top nuclear research center stores data on a Chinese cloud. It is thereby a minimum requirement that networks fulfilling functions for government networks, defense industry, and internal security must not rely on Chinese equipment. Beyond that, networks that fulfil critical functions for society, such as utility and pharmaceutical industries, healthcare, banking, or transportation and communication, must likewise not be compromised.

- East European NATO allies have so far been wary of increasing NATO's attention to China, concerned about an undue distraction from the threat from Russia. The past few months have shown that NATO must do both: deal with threats from Russia and from China—in fact , the two are intertwined. The war against Ukraine has drastically proven the imminent danger of aggression by the Russian regime. On the other hand, China's ever-closer ties with Russia, its explicit support for Russia's stance on NATO, the full deployment of its propaganda outlets in favor of Moscow's positions, and the latent prospect that Beijing may swing in with economic support – or even arms transfers – underscore that Sino-Russian cooperation “without limits” centrally means cooperation against the West. NATO must take into account that Sino-Russian joint capabilities can be directed both towards Russian goals in Europe, Chinese goals in Asia, and joint interests elsewhere.

- This leads to a drastically increased security risk from Chinese telecom equipment in the networks of, for example, Central and Eastern European allies. As NATO ramps up its military defense capabilities on its eastern border in the face of Russian threat, telecommunication networks in Poland, Romania, and other countries still rely heavily on Chinese gear. In fact, none of these countries ensures the removal of untrusted vendors in the coming years. The strictest rules yet limit roll out of further Chinese equipment, but accept the risk of untrusted legacy equipment until mid at the decade and longer—a hardly acceptable approach. The possibility that, in the event of a conflict, China could give Russia access to, for example, Polish telecom networks via Huawei or ZTE is real and dramatic in its consequences.

- The cost of replacing Chinese telecoms infrastructure in Europe will not be prohibitive: as operators upgrade from 4G to 5G, all their aging equipment will be replaced regardless. As such, a total ban on new Huawei equipment in Europe could “naturally” take about six years before the installed untrusted base is simply phased out. The question is rather one of ensuring a faster transition towards trusted technology on national security grounds, where short-term commercial considerations regarding phase-out times should not determine the pace. Another recurrent myth is that Chinese vendors are technologically more advanced than European vendors. The United States and South Korea are considered leaders in 5G networks rollout – their infrastructure has been deployed without using any Chinese equipment, relying instead mostly on European technology. When it comes to pricing, the European vendors are also able to compete with their Chinese competitors—but they are not able to compete with the Chinese state. China’s subsidies for homegrown companies operating on global markets, as well as the preference for Chinese companies in its domestic market, continues to distort the playing field. The issue is most acute for the smaller operators across Europe, Latin America, and Asia, which have weaker credit scores and thus must resort to Chinese loans unless alternative financing mechanisms are offered. One approach being suggested as an alternative is Open-RAN. Yet in practice, Chinese presence and influence in its development structures must raise questions and requires a comprehensive risk assessment.

- The EU Toolbox for 5G security is a good starting point for forward steps. However, its non-compulsory nature allows for different interpretation and implementation across EU members, therefore creating vulnerabilities. One concrete next step could be to ensure stricter implementation of the toolbox across the EU. However, the EU Toolbox for 5G can only be the starting point. Networks connecting critical assets via fiber optics, transport, and undersea cables require the same scrutiny and strict implementation of safeguards as the radio access and core network. The joint development of toolboxes for these network perimeters could be envisioned.

- While nuanced language was adopted at the NATO 2021/02 summits, allies have concurred that China’s behavior interferes with our democratic principles and national security. Hence, the systemic challenge that China poses has become a key NATO agenda item and it is amplified by the Russian-Chinese intensified collaboration. The alliance’s policy towards China has been solidified in the Strategic Concept, which was adopted at the NATO summit in Madrid. The challenging part for NATO will be to address the various and diverse current security threats at once—hybrid deterrence, disruptive and emerging technologies, and vulnerable critical infrastructure. Due to the fast-changing security landscape and the rapid development of technology, being able to excel at all fronts will be crucial to NATO’s continued success.