



NATO and China: Addressing new challenges

By Meia Nouwens | 9 March 2022

Key Issues

- While NATO allies have agreed that China presents a challenge to the alliance, allies have not yet agreed on how to address those challenges. Allies remain divided, for example, with regards to allowing Huawei 5G into their national networks.
- NATO might not have the resources to operate in a significant way in the Indo-Pacific, but can contribute practically with partners in the region through sharing best practices and collaborating on emerging and disruptive technology development.
- Having expressed concern about Chinese military modernisation and missile development programmes, NATO could play a role in discussing arms control issues with Beijing, though should keep expectations low.

Introduction

The illegal Russian attack on the Ukraine moved NATO into the centre of public attention as the freedom and security of its members is at stake. China's rise and its support for Russia, although not as straightforward as expected, presents the alliance with an additional new challenge. China seems to be no longer "out of area". Furthermore, Chinese investment into NATO allies' critical infrastructure, its growing global economic and political influence, the modernisation of its military, its cyberattacks and participation in disinformation campaigns paired with its ambition to build capabilities for global reach are all factors that force NATO to deal with China within the alliance, as well as in the Indo-Pacific. This policy brief posits that NATO's priorities should be, first, to forge consensus on key matters such

as investment screening and critical infrastructure resilience at home, and, second, to consider how it can play a role in the Indo-Pacific.

The challenges that China poses to NATO

At the Madrid Summit in 2022, the North Atlantic Treaty Organization will define its core tasks and priorities for the 21st century. While NATO is expected to increase its attention to the Pacific, the war in the Ukraine will have an impact. Nevertheless, there is a growing unease within the alliance about China's rise, economically and politically, impacting on NATO and on its partner countries in the Indo-Pacific region.

The greater focus on China in the Strategic Concept has been under discussion within NATO and with allies since the mid-

2000s. Military-to-military cooperation with the People's Liberation Army began in 2007. In 2011, then-secretary general [Anders Fogh Rasmussen](#) supported engagement with China: He saw China, as a permanent member of the UN Security Council, playing an increasingly important role on the global stage, also as a partner for the alliance to achieve peace and stability.

Ahead of the North Atlantic Council at the level of heads of state and/or government in 2019, NATO Secretary General Jens Stoltenberg had announced that the 2019 Summit Communiqué would mention China for the first time in an [official document](#) – the [1999 Strategic Concept](#) had not mentioned China – The [2021 NATO Brussels Summit Communiqué](#), in which the Alliance adopted its 2030 Agenda. Countering China's various challenges to the alliance were the focus of the document as NATO seeks to address "China [...] coming closer to [the alliance]".

In the non-binding [2030 Reflection Report](#), and in NATO's [2030 Agenda](#) adopted in 2021, NATO officially stated its intention to work more alongside partners in the Indo-Pacific and tackle the political, economic, and military challenges China poses. However, the vast majority of these challenges fall within areas that are not traditionally NATO's responsibility.

The 2030 Agenda highlights China's military modernisation and to the creation of new capabilities in the cyber, space, maritime, and air domains. NATO voiced particular apprehension about China's development of nuclear-capable systems, which are able to reach NATO countries, and about Xi Jinping's government expanding its arsenal with "more warheads and a more sophisticated delivery system in an unrestricted manner". This adds another nuclear threat to NATO beyond the traditional threat posed by Russia, which President Putin has recently raised when attacking Ukraine.

Though China has not used force against NATO, it "has proven its willingness to use force against its neighbours". Consequently, NATO has to factor in China's development of longer-range, more advanced, and larger arsenals when planning its own nuclear deterrence. The military cooperation between Russia and China poses additional

concerns, as evidenced in the Ukraine War as well as by earlier joint-military drills in Russia and in the Euro-Atlantic region.

The 2030 Agenda is not limited to military considerations but identifies a broad range of challenges that China poses to the rules-based international order through its approach to human rights and international law. It identifies China's use of economic coercion and intimidatory diplomacy, as well as disinformation efforts, as challenges to NATO's unity, its collective resilience, the security of critical infrastructure (such as 5G), supply chains, and its ability to maintain an innovative edge in new technologies.

NATO places increasing importance on the development and adoption of technologies such as artificial intelligence (AI), autonomous weapons systems, biotechnology, quantum computing. Therefore, the protection of intellectual property rights and innovation in the academic and private sector have gained importance.

5G, where China made important inroads in the European critical infrastructure and digital ecosystems, is a particularly grave concern for NATO. The United States, supported by some allies, regards the integration of Chinese-built 5G networks across the alliance as a significant intelligence and operational risk. This could also endanger European innovation in strategic industries. Companies like Huawei have close links with the Chinese Communist Party and according to Chinese laws could be pressured to reveal information about their overseas engagements. US officials contend that any information flowing through Chinese 5G networks could be compromised through Beijing's use of backdoors built into the code of the technology.

In the economic sphere, the Reflection Report contends, NATO Allies will continue to diverge as governments attempt to strike a balance between the need for security and the desire for economic benefits through access to the Chinese market. While the 2030 Agenda underscores the need for unity within the alliance, the Reflection Report highlighted that political unity across the alliance is at present still a 'work in progress' on how to address future challenges, including national economic interests.

As the report warns, China will continue to exploit this division among allies in its own interests.

What should NATO do about its “China challenge”?

Will NATO allies be united to have an impact? The 2030 Reflection Report and 2030 Agenda are clear: Allies should form mechanisms to share information and monitor their bilateral relationships with China, and the ongoing cooperation between China and Russia in military, technological, and political domains. In taking these actions NATO should be

mechanism, requiring its member states to establish their own investment screening mechanisms. However, by 2021, neither all EU Member States nor all NATO members have implemented such investment screening mechanisms.

5G is a striking example. While the United States has entered into [strategic competition](#) with Beijing, and the European Union has identified China as a [systemic rival](#) (as well as a partner and competitor), the US and some EU Member States still differ about whether to allow or restrict Chinese investment in national critical infrastructure. NATO’s 2021

“

How big a role NATO will play in the Indo-Pacific is yet unclear. NATO will have to continue taking on tasks to guarantee European security in the face of an aggressive Russia, and the persisting instability in North Africa and the Middle East.

”

clear that “any action taken is defensive in nature and in response to the stated intentions or actions of the current Chinese government”.

Addressing internal challenges

NATO allies need to forge a common position on China. This homework is necessary to narrow the differences identified in the Reflection Report and to work towards a common approach to China, as outlined in the NATO 2030 Agenda. If the allies fail in this, NATO will not be able to communicate to partner countries in the Indo-Pacific a coherent policy, which would undermine its credibility and complicate effective cooperation.

While the United States has strengthened its investment-screening mechanism (the Committee on Foreign Investment in the United States, CFIUS) in order to restrict potentially predatory investment in key areas of technology, the European Union passed a mechanism in 2020 [implementing regulations](#) of its 2019 foreign direct investment screening

Strengthened Resilience Commitment was a positive step, as well as the EU-NATO cooperation on resilience. However, despite the heightened concerns about supply chain resilience across the alliance and EU following the COVID-19 pandemic, there remains an uneven patchwork of regulation on the use of 5G with varying levels of restrictions.

Contrary to the EU, the US has banned the integration of Chinese telecommunications equipment into its national 5G network and has added additional Chinese companies and institutes to its [Entity List](#), restricting US companies from exporting components to China where they may be used in defence equipment or to suppress human rights in China.

The EU uses a different approach, namely generic legislation that restricts any technology which member states have to implement from potentially high-risk vendors. Germany passed its IT-Security Law in 2021, which allows the German government to veto procurement by untrustworthy telecommunications vendors. This is in line with

France, Italy, and Finland (an EU member but not a NATO member). In other countries like the Netherlands and Portugal, telecommunications firms, rather than central governments, have decided whether to use Huawei equipment in their 5G network rollouts. The Dutch government has opted for stricter vetting of telecoms suppliers, without outright banning Huawei. KPN – the Netherlands’ leading telecommunications provider – was one of the first European providers to opt out of using Huawei in the core of its 5G network, preferring Ericsson. The same approach was taken by Portugal’s three leading telecommunications others, which, like Hungary, Turkey, and Austria (an EU member but not a NATO member), still make use of Huawei’s 5G technology. Thus, there is still a way to ensure the security and resilience of critical infrastructure in the EU and NATO to meet the Chinese challenge together.

This lack of a common standard of protection also applies to the alliance’s academic and private sectors, particularly concerning emerging and disruptive technologies (EDTs) despite NATO’s actions in the form of an Emerging and Disruptive Technologies agenda and roadmap; its Artificial Intelligence Strategy; and its decision to create a Defence Innovation Accelerator for the North Atlantic (DIANA) and an Innovation Fund.

The Coherent Implementation Strategy on Emerging and Disruptive Technologies innovation covers seven technological areas: AI, data and computing, autonomy, quantum-enabled technologies, biotechnology and human enhancements, hypersonic technologies, and space.

These areas overlap with the first AUKUS project on technological cooperation, Australia’s plan to invest US\$81 million in quantum technology and a new innovation hub forging strategic partnerships with like-minded countries. Collaboration between AUKUS member states and NATO on dual-use technology research and development would not only benefit participating countries by pooling research and development resources and talent, but also by contributing to setting standards together for key areas of new technology. Common standards are important should NATO and partner countries in the Indo-Pacific seek to enhance future interoperability in areas like cyber, AI, space, and quantum.

Future cooperation between AUKUS and NATO may, however, be complicated by France’s recent downgrading of relations with Australia. [France’s Indo-Pacific Strategy](#) now states that France will continue cooperation with Australia on a case-by-case basis based on French and regional interests and on cooperation with the US on areas mentioned in the AUKUS agreement.

As the strategy highlights, the Indo-Pacific region is essential to France’s cooperation on research and innovation, and tech cooperation between the two groupings should not be entirely discounted yet. Beyond AUKUS, NATO could also consider collaborating further with its own current partner countries in the Indo-Pacific, such as Japan. Japan already [cooperates intensively with the EU](#) in this area, and cooperation with NATO could bring a needed defence angle to common standard-setting.

In sum, as EU member states are responsible for the implementation, the level of investment screening and protection varies with the EU and NATO, allowing some inroads in critical industries as well as innovative research.

Addressing challenges in and with the Indo Pacific

As we have shown that NATO has recognised the challenges and threats posed by China, there remains the need to define not only modalities but also whether the Indo-Pacific shall be included in the competition. The United States has committed to adjusting its posture towards its foremost strategic challenge and made the Indo-Pacific its priority theatre. Although precise details on the implementation of the recent [US Indo-Pacific Action Plan](#) are still lacking, how big a role NATO will play in the Indo-Pacific is yet unclear. NATO will have to continue taking on tasks to guarantee European security in the face of an aggressive Russia, and the persisting instability in North Africa and the Middle East.

While only a few NATO Allies can realistically contribute to a physical presence in the Indo-Pacific, a coordinated presence is foreseen in the 2021 EU Indo-Pacific Strategy. France as an Indo-Pacific country is already present. The United Kingdom, with its Indo-Pacific tilt, is also a possibility. The [Carrier](#)

[Strike Group 2021](#) that involved the UK, US, and the Netherlands has shown that through collaboration and cross-decking, countries with fewer assets can also contribute. The intensity of a NATO presence will ultimately depend on whether there are sufficient capabilities to be spared for the Indo-Pacific. Current [tensions with Russia](#) and the war in Ukraine exemplify the need for a realistic assessment of how NATO can combine providing security in the Euro-Atlantic region with a meaningful role in the Indo-Pacific.

More and better information and assessment sharing with NATO's so called "Partners across the globe" in the region (Japan, Australia, South Korea, New Zealand) would increase its regional role and relevance. Expanding the network to include those facing up to a more assertive China, India, or countries in Southeast Asia would help too. NATO's [centres of excellence](#) in the Indo-Pacific could also be leveraged in sharing knowledge and contribute to capacity and skill-building of partners on topics ranging from cooperative cyber defence to maritime security.

Joint cooperation on high-tech initiatives and emerging disruptive technologies as part of security agreements could be pursued. The technological scope of AUKUS could present an opportunity for NATO to jointly achieve its goals with regards to defence innovation and adoption of EDTs.

Involving China in discussions about arms control could increase NATO's standing in the Indo-Pacific. The Reflection Report points to China's increased conventional and nuclear missile buildup, and states that the alliance must continue to advocate arms control regimes. Secretary General Stoltenberg echoed these points at a pre-NATO leaders summit news conference in 2021: Allies should leverage NATO "even more as a unique platform for dialogue on arms control, disarmament, and non-proliferation". China, he [stated](#), "as a global power, has a responsibility to engage in arms control efforts". Stoltenberg has called for a greater role for NATO in arms control over the past few years, as NATO also has experience in negotiating arms control proposals.

While NATO currently is in the process of deciding its position on China in the updated NATO Strategic Concept, it could offer itself as a platform for arms control talks on a technical level as it includes three

of the five nuclear-armed permanent members of the UN Security Council. NATO has the technical expertise, and China might be more willing to discuss arms control matters outside of a bilateral setting.

Expectations, however, should be measured. China's perception of NATO as a US-led alliance could work either in favour or against arms control talks. While any perceived pressure on China would reaffirm Beijing's view that NATO is acting solely for the United States' interests, a multilateral platform could allow Beijing to indirectly discuss concerns with the US.

Conclusion

The challenges posed by China to the alliance are not new. Already in the last ten years, allies have been grappling with issues of foreign investment into strategic industries and critical infrastructure, imbalanced trade relationships with China, influence operations and disinformation, and the problem of technology transfer to China.

However, the increasing assertiveness by the PLA and China's increasingly forceful and at times aggressive diplomatic tactics in the Indo-Pacific, as well as its increasingly authoritarian turn at home, have heightened awareness in the alliance. The war in Ukraine made it clearer that the alliance will need to think carefully about how to balance its focus on maintaining security in the Euro-Atlantic region with any potential role in the Indo-Pacific. However, there is scope for the latter. Members should continue to improve information sharing and assessing Chinese investment in their economies, within the alliance as well as with partners in the Indo-Pacific region. Allies should build a stronger common approach to domestic Chinese challenges, such as in national critical infrastructure, keeping an innovative edge, and resilience needs to be addressed first to enable the alliance to ensure both political and military security. Doing so is not just in NATO's internal interest but of benefit to its engagement with the Indo-Pacific region and to setting common standards with partners outside of the alliance, particularly in areas of defence-relevant disruptive technologies. There is scope for NATO to be a platform to engage with China, too, on areas of key interest, such as arms control. However, on this last point, expectations should be measured.



ABOUT THE AUTHOR

Meia Nouwens

Meia Nouwens is a Senior Fellow for Chinese Defence Policy and Military Modernisation at the International Institute for Strategic Studies. Her expertise lies in China's international relations, regional strategic affairs, and cross-service defence analysis. Previously, Ms. Nouwens worked for the European Union's representative offices in New Zealand and Taiwan, and she has worked in the public and private sector focusing on security analysis. She holds a BA with Honors in International Relations and Political Science from Macquarie University, a Masters of International Relations and Diplomacy from Leiden University in conjunction with the Clingendael Institute, and an MPhil in Modern Chinese Studies from the University of Oxford and Peking University.

Meia.Nouwens@iiss.org

 @MeiaNouwens

The **Centre for Security, Diplomacy and Strategy (CSDS)** seeks to contribute to a better understanding of the key contemporary security and diplomatic challenges of the 21st century – and their impact on Europe – while reaching out to the policy community that will ultimately need to handle such challenges. Our expertise in security studies will seek to establish comprehensive theoretical and policy coverage of strategic competition and its impact on Europe, whilst paying particular attention to the Transatlantic relationship and the wider Indo-Pacific region. Diplomacy as a field of study will be treated broadly and comparatively to encompass traditional statecraft and foreign policy analysis, as well as public, economic and cultural diplomacy.

The **CSDS Policy Brief** offers a peer-reviewed, interdisciplinary platform for critical analysis, information and interaction. In providing concise and to the point information, it serves as a reference point for policy makers in discussing geo-political, geo-economic and security issues of relevance for Europe. [Subscribe here](#). The CSDS Policy Brief is a discussion forum; authors express their own views. If you consider contributing, contact the editor Prof. Michael Reiterer: michael.reiterer@vub.be.

Follow us at:

Twitter [@CSDS_Brussels](#)

LinkedIn [CSDS Brussels](#)

Youtube [CSDS](#)

<http://csds.brussels-school.be>



BRUSSELS
SCHOOL OF
GOVERNANCE

Visitor's address:

Pleinlaan 5, 1050 Brussels, Belgium

Mailing address:

Pleinlaan 2, 1050 Brussels, Belgium

The Brussels School of Governance is an alliance between the Institute for European Studies (Vrije Universiteit Brussel) and Vesalius College.

info_bsog@vub.be

www.brussels-school.be