February 2022

NATO and Digital Cooperation With the Indo-Pacific

Meia Nouwens

NATO will adopt this year a new Strategic Concept that sets out how it will address collective security in the face of old and new challenges. For the first time, China is expected to be mentioned as a challenge to the alliance.

NATO has since 2019 stated that China's economic, political, and military power present challenges to it at home and abroad, but it has not yet confirmed how it will tackle these.

NATO seeks to work more closely with partners in the Indo-Pacific to uphold the rules-based international order rather than operating in the region itself. Similarly, it has identified objectives to strengthen its capabilities in emerging and disruptive technologies (EDTs).

To contribute to regional security in the Indo-Pacific and Euro-Atlantic regions, NATO should combine these two objectives to leverage and extend its network of partners in the Indo-Pacific, and combine efforts in standard setting and innovation in EDTs. To combine innovation with like-minded countries, NATO could also work with the EU to develop digital partnerships and adhere to common data-governance policies.

G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Washington, DC Ankara Belgrade Berlin Brussels Bucharest Paris Warsaw

Introduction

In 2022, NATO finds itself in new territory. It is in the process of writing a new Strategic Concept, which will completed prior to the Madrid summit in June.[1] While Russia remains a belligerent actor and threat to the alliance's collective security, other challenges have arisen that the allies have yet to counter collectively. In particular, the political, economic, and military rise of China as well as its authoritarian turn have caused NATO to look further east than it has in the past and to consider whether the alliance as it currently stands is up to the task of countering the multifaceted challenges that China presents.

While the allies have agreed and stated publicly that China does present challenges, there is less consensus as to how to address these. First, the nature of the challenges that China poses at times fall outside of NATO's traditional thematic remit or it impacts areas of national rather than NATO competence, such as the development and adoption of investment-screening regulations to restrict access to strategic sectors in national markets. Second, the allies each have a different bilateral relationship with China. Considerations about how to balance security and prosperity are weighed differently across NATO capitals, complicating efforts to speak with a unified voice.

While the allies have agreed and stated publicly that China does present challenges, there is less consensus as to how to address these.

While China does not pose a direct military threat to NATO, the increasing pace of its military modernization and its focus on becoming a global power in emerging and disruptive technologies (EDTs) should be of concern to the allies. It raises, in particular, questions about future competitiveness in areas like artificial intelligence (AI), quantum technologies, and outer space. While NATO considers how to address the China challenge at home through greater coordination in areas of technological development, it should also seek to leverage the strengths of its like-minded partners, and bring partner countries that are important actors in EDTs, such as Australia and Japan, into NATO's programing in this field. This brief recommends that, in addition to its efforts to create synergies in innovation around EDTs, NATO should leverage similar security-related agreements in the Indo-Pacific that also seek to develop emerging technologies. Furthermore, to align the innovation capacities of the alliance and its like-minded partners, greater cooperation should be sought between NATO and the EU as well as partner countries in the Indo-Pacific in areas such as data free flow with trust, with the EU taking the lead.

The Changing View of China

A decade ago, the view within NATO of the relationship with China was vastly different to what it is today. In the early 2000s, the alliance began engaging with China on a political level.[2] In 2011, NATO's leadership considered the country a potential partner for promoting global peace and stability.[3] In an example of cooperation on areas of joint concern and interest, China and NATO conducted several joint anti-piracy drills and exercises in the Horn of Africa on an ad hoc basis throughout the 2010s until 2018.

However, by 2019 the bilateral relationships between China and some NATO members, notably the United States, had worsened considerably within the wider context of strategic competition. While Washington had already "pivoted to Asia" (at least in rhetoric) in President Barack Obama's second term, the Trump administration lobbied heavily

1 NATO, Strategic Concepts, November 29, 2021.

2 Jonathan Marcus, "China seeks dialogue with NATO," BBC News, November 14, 2002.

3 NATO, NATO – delivering security in the 21st century, speech by NATO Secretary General Anders Fogh Rasmussen, July 7, 2012.

in Europe and within NATO for a greater focus on countering the security challenges that China poses. This included a China-focused discussion at the April 2019 NATO foreign ministers' meeting where Secretary of State Mike Pompeo called for the alliance to adapt to new threats from China as well as Russia.[4] While the United States continued to engage with its European and NATO partners on China throughout 2019 and early 2020, European countries also became more critical of China in 2020 as a result of the coronavirus pandemic.[5]

NATO's language on China has changed significantly from earlier discussions around cooperation and common interests. Instead, in the language it uses in official documents like the NATO 2030 Reflection Group Report and summit communiqués as well as in press conferences paints a picture of a China that has already risen, presenting new and unique challenges to the alliance that it may not be equipped yet to counter. Despite this, however, NATO leaders still stop short of labelling China a threat or an adversary.

NATO's language on China has changed significantly from earlier discussions around cooperation and common interests.

China, at present, does not pose a direct military threat to NATO. Instead, the main nature of the challenge lies in Beijing's growing international strength as an economic and political actor. China's GDP grew from $1.211 trillion in 2000 to $16 trillion in 2021.[6] This growth has been based on the country's increasing role as a global manufacturer and exporter since its reforms and opening up in the 1980s. The importance of trade in China's GDP growth is clear: in 2019, trade represented 34.5 percent of GDP.[7] Undoubtedly, other factors have contributed to China's economic strength, such as the important role played by its real-estate sector in buffering the country from the shocks of the global financial crisis in 2009.[8] Nevertheless, China is an important hub in global supply chains and an important (though not necessarily always the most important) trading partner for NATO allies.

China's Power Projection

The China challenge goes beyond trade and economics, however. Under President Xi Jinping, Beijing is on a path to achieving "the great rejuvenation of the Chinese nation" and the "China Dream" by bringing the country back to center stage of global politics. This idea is not entirely new. Though Xi has brought back personality leadership to Chinese politics, leaders before him have talked about China's rise. Deng Xiaoping spoke of the invigoration of China in the 1980s. In the 1990s, Jiang Zemin promulgated the idea of the "great rejuvenation of the Chinese nation." Xi's predecessor, Hu Jintao, followed lines similar to Jiang's. China's rise has thus long been a project of Chinese leaders. Under Xi, wielding the country's economic, military, and political heft for the survival of the Chinese Communist Party (CCP) and to project influence globally is stated more overtly than it has in the past. At the 19th Party Congress in 2017, Xi proclaimed that China's international influence had risen to the point that it had "the ability to inspire and power to shape" the international arena.[9] China, he stated, had "stood up, grown rich, and is becoming strong," and in doing so it was "blazing a new trail for other developing countries to achieve modernization."

4 Lesley Wroughton and David Brunnstrom, "Pompeo calls on NATO to adapt to new threats from Russia," China, Reuters, April 4, 2019.

5 PEW Research Center, Large majorities in most places have negative opinions of China, June 29, 2021.

6 Stella Qiu and Ryan Woo, "Factbox: Has China's $16 trillion economy fully recovered?," Reuters, April 16, 2021.

7 World Bank, "Trade (% of GDP) – China", 2022.

8 Alexandra Stevenson and Cao Li, "What to know about China Evergrande, the troubled property giant," The New York Times, December 9, 2021.

9 Xinhua, Full text of Xi Jinping's report at 19th CPC National Congress, November 4, 2017.

China's global power projection is not just economic and political but military too. Xi has set the goal to build the People's Liberation Army (PLA) into a global top-tier force that obeys the CCP's command and can fight and win wars. According to the 2019 Defense White Paper, the PLA's role is not limited to defending China's territory but also to safeguard Chinese interests in cyberspace, outer space, and the electromagnetic space as well as overseas and development interests.[10] At home, China has taken a greater authoritarian turn with the CCP's power ever-more central in every aspect of life, from reining in the private sector to establishing of party committees in civil society organizations and even an app to promote Xi Jinping Thought.[11]

There has also been increasing concern about—among other things—the increasing levels of CCP control over segments of Chinese society, including the detention of and human-rights abuses against millions of Uyghurs; about Beijing's quelling of protests and heightened control over Hong Kong through the National Security Law for the special administrative region; and about the leveraging of China's high-tech industrial strengths in order to strengthen its surveillance state.[12] The changes that China has undergone extend beyond their domestic context, the country' littoral, or the Indo-Pacific. Xi's concept of "comprehensive national security" and a framework of laws on cyber and national security and national intelligence aim to allow the CCP to control the domestic and foreign environment to suit Chinese interests and national objectives.[13]

The Implications for NATO

For NATO, China's rise means expanding the alliance's relevance beyond countering Russia to the east and peace missions in its region. As its military activity, political influence, trade, and investments become more global, the challenges that China poses will be encountered around the world. As NATO Secretary General Jens Stoltenberg has stated, "China is coming closer to us."[14] However, the alliance has been behind the curve and is attempting to catch up on an already unfolded reality.

China is increasingly able to deploy its military further from afield, including in the Euro-Atlantic area. In 2017, a PLA Navy task group conducted exercises in the Baltic Sea and the Black Sea.[15] En route to the Baltic, the PLA Navy conducted live-fire exercises in the Mediterranean as well.[16] China has also become an important provider of military equipment and arms to its strategic partners and countries that are unable or ineligible to acquire such capabilities from Western defense prime contractors. So far in Europe, only Serbia has received orders of Chinese advanced military equipment, in the form of strike-capable uninhabited aerial vehicles. But China has found demand in the Middle East, Central Asia, and Africa, such as in Algeria, Egypt, Iraq, Kazakhstan, Nigeria, Pakistan,

10 The State Council of the People's Republic of China, Full Text: China's National Defense in the New Era, July 24, 2019.

11 Lily Kuo and Kate Lyons, "China's most popular app brings Xi Jinping to your pocket," The Guardian, February 15, 2019.

12 Patrick Wintour, "Leaked papers link Xinjiang crackdown with China leadership," The Guardian, November 29, 2021; Kari Soo Lindberg, Natalie Lunch and Pablo Robles, "How Hong Kong's National Security Law is changing everything," Bloomberg, October 5, 2021; and Paul Mozur, "Inside China's dystopian dreams: AI, shame and lots of cameras," New York Times, July 8, 2018.

13 China National People's Congress, National Security Law of the People's Republic of China, July 10, 2015; China National People's Congress, National Intelligence Law of the People's Republic of China, June 27, 2017; and Cyberspace Administration of China, Cybersecurity Law of the People's Republic of China, November 7, 2016.

14 Roula Khalaf, "Transcript: 'China is coming closer to us' – Jens Stoltenberg, NATO's secretary-general," Financial Times, October 18, 2021.

15 Sebastian Bruns and Sarah Kirchberger, "The PLA Navy in the Baltic: A view from Kiel," The Maritime Executive, July 19, 2017.

16 Zhao Lei, "Navy conducts live-fire drill en route to Baltic," China Daily, July 12, 2017.

Saudi Arabia, and the United Arab Emirates.[17] Its growing role as a supplier of advanced military technology risks changing the balance of power in regions close to the Euro-Atlantic area. China and Russia have in recent years grown closer in political and defense terms as a show of strength against the liberal democratic West. Though their relationship falls short of a formal alliance, Beijing has offered quiet support for Moscow's military aggression toward Ukraine as well as cooperation in areas of defense technology such as missile defense systems.[18] China's interests in playing a security and defense role in the global commons should also be of note to NATO as the PLA's space and cyber capabilities grow. The PLA's growing conventional and nuclear missile arsenal should be of particular concern to NATO, given China's lack of participation in existing arms-control regimes. While the focus on China's nuclear-capable missiles has been related to the role they play in the PLA's Indo-Pacific theatre missions, the increasing range and sophistication of its missile arsenal should be of concern to European security and defense too.

While not directed at NATO per se, China is also developing dual-use technologies for military and civilian purposes.

China is also already present in Europe through investments in national critical infrastructure. Chinese companies have acquired ownership stakes in 13 ports in Europe, from Belgium to Greece, and beyond to Turkey. Though NATO has not declared China an adversary yet, questions remain about how the country could leverage ownership of such infrastructure in the event of worsening ties with the alliance or its individual members.

The Chinese presence in Europe's telecommunications networks present a similar concern. During the Trump administration, the United States pushed forward a "clean networks" initiative to try and sway European partners and allies to restrict Huawei technology from their national 5G telecommunications networks. Though some have joined, European countries and NATO allies remain divided with some opting to restrict Huawei from their networks outright, some taking a legal approach to "high risk vendors" without naming Huawei directly, some leaving the decision to their national telecommunications companies, and some having either not yet taken any decision or already welcomed Huawei in their networks.

While not directed at NATO per se, China is also developing dual-use technologies for military and civilian purposes as part of its aim to become a world leader in high-tech manufacturing and in particular in emerging technologies such as AI by 2030.[19] China's toolbox for achieving this includes heavy investment in sectors such as AI and quantum technologies through state support and incentivization mechanisms as well as collaboration with and technology transfer from innovative industries and researchers in other countries.[20] China's military technological ambitions thus also present a competition challenge to the strategic innovative industrial strengths of NATO members.[21]

NATO's public acknowledgement of these challenges at leadership level is an important first step toward countering them. Statements by NATO leaders in 2019 and a communiqué in 2021 in which NATO announced it considered China a "systemic challenge"

17 US Office of the Secretary of Defense, Annual Report to Congress: Military and Security Developments involving the People's Republic of China 2021, November 2021; and Bruce Einhorn, "Combat drones made in China are coming to a conflict near you," Bloomberg Businessweek, March 17, 2021.

18 Xinhua News, "Wang Yi holds telephone talks with US Secretary of State Blinken," January 27, 2022; and The Guardian, Russia is helping China build a missile defence system, Putin says, October 4, 2019.

19 State Council of the People's Republic of China, The State Council on printing and distributing circular of the new generation of artificial intelligence development plan, July 20, 2017.

20 Helena Legarda and Meia Nouwens, China's pursuit of advanced dual-use technologies, International Institute for Strategic Studies, December 18, 2018.

21 Bruce Shen, "Europe faces the tricky ask of policing Chinese investments", The Diplomat, August 6, 2021.

were followed by the NATO 2030 Reflection Group Report in 2020 that reflected this language.[22]

While the report discussed the whole range of challenges and threats to the alliance, China featured heavily as a main one. It recommended strengthening the alliance's political unity and decision-making to deal with the China challenge. Second, having acknowledged that areas like investment screening, countering economic coercion tactics and disinformation may not lie within NATO's traditional areas of competence, the report recommended the alliance should work with partners such as the European Union and like-minded countries in the Indo-Pacific. This was echoed by the Brussels summit communiqué in June 2021, which stated that NATO will continue to work as an alliance with like-minded partners, in particular the EU, with regard to the protection of critical infrastructure, resilience, securing technological innovation, and addressing challenges to the rules-based international system.[23] Last, the report called on NATO to help allies "maintain their technological edge or respond to critical weaknesses that could affect the security of the alliance as a whole."[24] It stated that constructive dialogue with China is still possible and recommended identifying opportunities to jointly address global challenges. The report also recommended pursuing NATO's implementation strategy that would lead to a net assessment of allies' national efforts in developing and adopting EDTs. To this end, the NATO Brussels summit communiqué announced the establishment of a NATO Innovation Fund and a Defense Innovation Accelerator for the North Atlantic (DIANA).

Some steps have been taken. NATO already works closely with the EU on addressing the political and economic challenges posed by China, and it has launched initiatives to maintain its technological edge. However, finding agreement between allies that have differing bilateral relationships with China will be a significant obstacle to implementing further policies aimed at countering its assertive presence in the Euro-Atlantic area and toward partners in the Indo-Pacific.

Meeting the Challenge: Digital Technologies

Due to the nature of the challenges that China poses to it, NATO's priority should be to meet them at home. However, in countering the economic, technological, and security challenges that China poses, collaboration with partner countries in the Indo-Pacific that are like-minded and have valuable experience in countering Beijing's assertiveness is equally important. Nevertheless, as Secretary General Stoltenberg has stated, NATO is unlikely to face the China challenge by being physically present in the South China Sea or elsewhere in the Indo-Pacific region.[25] Due to resource constraints and other concerns, this remains unlikely in the near future. NATO can best meet the technological challenge that China poses through greater collaboration and coordination with regard to the digital space and emerging and disruptive technologies. While current NATO activity in EDTs, as well as in data management and governance, is a step in the right direction to protect domestic resilience and to enhance innovation capacities, there are further options to strengthen the alliance's technological edge at home and with partners in the Indo-Pacific.

Expand NATO collaboration on EDTs to partners in the Indo-Pacific

NATO is in the process of developing the mechanisms, funding, and strategy behind DIANA and the NATO Innovation fund, the former aimed at launching in 2023 and the latter potentially totaling to $1 billion. DIANA aims to be NATO's version of the United States' Defense Advanced Research Projects Agency and to bring together transatlantic efforts on critical technologies, working with industry and academia on

22 NATO, NATO 2030: United for a New Era, November 25, 2020.

23 NATO, Brussels Summit Communiqué, June 14, 2021.

24 NATO, NATO 2030: United for a New Era.

25 NATO, NATO 2030 – safeguarding peace in an unpredictable world: Keynote speech by NATO Secretary General Jens Stoltenberg at the Sciences PO Youth & Leaders Summit, January 25, 2021.

AI, big-data processing, quantum-enabled technologies, autonomy, biotechnology, hypersonic weapons, and space. Subsequently, the Innovation Fund will seek initially to invest $81.2 million per year in transatlantic startups. Importantly, it will work with pre-vetted investors to ensure that "the technology will be protected from illicit transfers."[26]

While much is still left to be decided on both these efforts, there are clear areas for practical cooperation with partners in the Indo-Pacific; for example, with regard to the Australia-United Kingdom-United States (AUKUS) security pact and the Quadrilateral Security Dialogue joining Australia, India, Japan, and the United States.

First, AUKUS aims to promote cooperation beyond the initially agreed nuclear-powered-submarine program. The agreement seeks to foster "deeper integration of security and defense-related science, technology, industrial bases and supply chains."[27] Trilateral collaboration will focus on cyber capabilities, AI, quantum technologies, and additional undersea capabilities.

Following the first in-person leaders' summit of the Quad in September 2021, leaders of the four countries put forth an initiative to partner on emerging technologies, space, and cybersecurity, and to cultivate next-generation talent.[28] Exact timelines for these initiatives are still unclear. With regard to the latter, the Quad Fellowship will provide 100 scholarships per year for students in science, technology engineering, and mathematics from the four countries to study in the United States. Ultimately, the program will seek to develop a network of science and technology experts among the Quad countries. On critical and emerging technologies, the countries will work together to publish a statement of principles that touches on the design, development, governance, and use of technology; to establish a technical standards contact group; to launch a semiconductor supply-chain initiative; to support 5G deployment and diversification; and to monitor advances in biotechnologies.[29] The Quad countries will also collaborate on cybersecurity issues and establish a space-related working group that shares climate change-related satellite data, enables capacity-building in space-related domains in other Indo-Pacific countries, and consults on norms and guidelines.

While the overlap is not exact, there are significant areas for cooperation between NATO, AUKUS, and Quad countries.

While the overlap is not exact, there are significant areas for cooperation between NATO, AUKUS, and Quad countries. Australia and Japan are already NATO partner countries and cooperate politically with the alliance on a variety of levels from parliaments to heads of state, ministries of foreign affairs and defense.[30] Bringing partner countries into NATO's programing on EDTs would not only increase the alliance's innovative capacities but also allow it to align itself with the priorities of partners in the Indo-Pacific to a greater extent.

A potential stumbling block for such cooperation might be the recent tensions between the EU (and therefore some NATO members) and the AUKUS countries. Transatlantic relations soured following the announcement of the establishment of the secu-

26 Vivienne Machi, "NATO hopes to launch new defense tech accelerator by 2023," Defense News, June 22, 2021.

27 Prime Minister's Office, UK, US and Australia launch new security partnership, September 15, 2021.

28 White House, Fact Sheet: Quad Leaders' Summit, September 24, 2021.

29 Ibid.

30 NATO's "global partners," such as Australia and Japan, are countries with whom the alliance engages politically and have access to the same activities that NATO Individual Partnership Cooperation Programme countries receive. They work with NATO on areas of common interest, such as cyber defence, counterterrorism, non-proliferation, and resilience. In some cases, NATO and its global partners cooperate through NATO military operations or through defence capacity, training, and educational programmes. See NATO, Relations with partners across the globe, August 25, 2021.

rity pact and the related cancellation of the submarine deal worth $90 billion between Australia and France. The announcement of AUKUS also coincided with the publication of the EU's Indo-Pacific strategy, which highlights the ambition to work with the Quad in the region.[31] There is thus a potential risk that EU members that are also NATO members, in particular France, may prioritize technological development within an EU rather than NATO context.

This risk may be overstated, however. The EU's Indo-Pacific strategy focuses primarily on digital governance and partnerships: the development of shared technological standards, alone and together in coordination with like-minded partners, for areas such enhancing governance around AI based on democratic principles and fundamental rights. The EU's practical engagement with its Indo-Pacific partners on the development of EDTs is still limited. It only has agreements on areas of practical cooperation and development with a select few countries in the Indo-Pacific, such as India and Japan with which it has agreed to deepen cooperation on 6G, standardization, AI, blockchain, and quantum and other technologies.

The security and defense section of the EU's Indo-Pacific strategy does not make any mention of cooperation with like-minded countries in the Indo-Pacific on EDTs.

Second, the security and defense section of the EU's Indo-Pacific strategy does not make any mention of cooperation with like-minded countries in the Indo-Pacific on EDTs. The strategy's main focus here is on cooperation on disinformation, maritime security, outer space, cybersecurity, peacekeeping, counterterrorism, and arms control. As the EU's focus on EDTs is primarily on standard setting, governance, ethics, and civilian applications, there may be an opportunity to collaborate and share the burden with NATO. NATO could work alongside the EU to ensure standards are set for EDTs in the defense and civilian realms while taking the lead on the development and adoption of defense-related EDTs.

Establish NATO standards on data governance together with partners in the Indo-Pacific

In 2017, the commander of NATO's Allied Command for Transformation, General Denis Mercier, stated that "data is now a main strategic resource. Processes for collecting, sharing, exploiting and distributing data are the main drivers to adapting organizations."[32] This remains true with regard to the military and civilian, public and private sectors. If shared policies on data governance promote interoperability, help to establish rules and norms, and secure data, then divergent policies could have the opposite effect. If NATO aims to remain competitive and to increase its innovation strengths in EDTs and digital technologies, digital policy coordination should be an area of discussion within the alliance.

In October 2021, NATO defense ministers agreed to the alliance's first-ever strategy for AI, which includes an ambition to agree on standards of data collection and use for AI. NATO also has standards and processes related to big data produced by the alliance.[33] However, if NATO members and partner countries seek to cooperate and collaborate on the development and adoption of emerging technologies and data-driven innovation, then addressing data governance and trusted cross-border data flows between allies and across partners is of importance. To date, some NATO members are aligned through membership of the EU and its General Data Protection Regulation (GDPR) and through the European Data

31 European Commission, Joint Communication to the European Parliament and the Council: The EU strategy for cooperation in the Indo-Pacific, September 16, 2021.

32 Editorial Team, Data Management is Key to NATO Success, Gov Data Download, June 1, 2017.

33 NATO Science and Technology Organization, NATO guide to data collection and management (DC&M) for analysis support to operations, August 27, 2020.

Governance Act (subject to final approval by the European Parliament and Council of the EU this year).[34] However, other allies, such as the United States, have taken different approaches to data governance and it remains to be seen whether the new EU-US Trade and Technology Council can find solutions for transatlantic cooperation in this area.[35]

Last, if collaboration between the innovative economies of NATO allies and their partners in the Indo-Pacific is a goal, then greater like-mindedness and alignment of data-governance norms should be an area of consideration in the future within the alliance and with countries like Australia, India, and Japan.

NATO has agreed already to work with the EU in areas where the latter has experience and competence.

This undoubtedly falls outside of the realm of NATO's traditional area of competence and more clearly a suitable role for the European Commission. This is not an obstacle: NATO has agreed already to work with the EU in areas where the latter has experience and competence. Furthermore, the EU is an active player in bilateral discussions between member states and non-EU countries about data sharing and data governance. Its Indo-Pacific strategy already envisions a greater role for the EU in the region in areas of digital governance through Digital Partnership Agreements with Japan, Singapore, and South Korea. The EU has already deepened its digital partnership with India in 2021 which seeks to promote 5G in line with global strategies and develop joint visions for next generations of information and communications technology, to promote digital cooperation between private sectors in each country, and to ensure that data regulation in India and the EU align with each other. Similarly, the EU and Japan created the world's largest area of safe data flows in 2019 when the European Commission adopted an adequacy decision on Japan for a data-sharing agreement.[36]

Conclusion

While countering the challenges that China poses to NATO will not be easy, the greatest challenge will be to find agreement and unity between allies on how to address their shared concerns about China's rise. The limitations on NATO's resources, particularly due to the requirements of allies to focus on collective security and defense at home, will make it difficult for the alliance to counter the China challenge in the Indo-Pacific. Though a show of commitment by sending military assets to the region and NATO's partners there is important, addressing the challenges that China poses to the alliance and its partners alike should be done in more varied ways.

NATO should focus on expanding its current work in the digital sphere to cooperation and collaboration with partner countries in the Indo-Pacific in order to build a strong ecosystem of like-minded digital actors. By cooperating on EDTs and sharing data to ensure that the private and public sectors in allied and partner countries as well as institutions like the EU remain competitive, NATO and like-minded countries can take steps toward bolstering their defense and security capabilities and preparing for competition as well as for conflict.

34 European Union, Regulation (EU) 2016/679 on the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, May 4, 2016; and Luca Bertuzzi, "Data Governance: new EU law for data-sharing adopted," Euractiv, December 1, 2021.

35 Nigel Cory, How the EU-U.S. Trade and Technology Council Can Navigate Conflict and Find Meaningful Cooperation on Data Governance and Technology Platforms, Information Technology & Innovation Foundation, December 2, 2021.

36 European Commission, European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows, January 23, 2019; European Commission, Joint Communication to the European Parliament and the Council: The EU strategy for cooperation in the Indo-Pacific.

The views expressed in GMF publications and commentary are the views of the author(s) alone.

About the Author

Meia Nouwens is senior fellow for Chinese defense policy and military modernization at the International Institute for Strategic Studies in London. Her expertise lies in Chinese cross-service defense analysis, China's defense industry and innovation, and China's regional strategic affairs and international relations. She also analyzes responses to Chinese power projection. Previously, she worked for the European External Action Service in Taipei, Taiwan, and Wellington, New Zealand. She holds an MPhil in modern Chinese studies from the University of Oxford, an MA in international relations and diplomacy from the University of Leiden, and a BA with honors in international relations and political science from Macquarie University.

Acknowledgments

This brief is part of a project at the German Marshall Fund of the United States supported by the Norwegian Ministry of Foreign Affairs.

About GMF

The German Marshall Fund of the United States (GMF) strengthens transatlantic cooperation on regional, national, and global challenges and opportunities in the spirit of the Marshall Plan. GMF does this by supporting individuals and institutions working in the transatlantic sphere, by convening leaders and members of the policy and business communities, by contributing research and analysis on transatlantic topics, and by providing exchange opportunities to foster renewed commitment to the transatlantic relationship. In addition, GMF supports a number of initiatives to strengthen democracies. Founded in 1972 as a non-partisan, non-profit organization through a gift from Germany as a permanent memorial to Marshall Plan assistance, GMF maintains a strong presence on both sides of the Atlantic. In addition to its headquarters in Washington, DC, GMF has offices in Berlin, Paris, Brussels, Belgrade, Ankara, Bucharest, and Warsaw. GMF also has smaller representations in Bratislava, Turin, and Stockholm.