NATO’s China Role: Defending Cyber and Outer Space

Liselotte Odgaard

To cite this article: Liselotte Odgaard (2022) NATO’s China Role: Defending Cyber and Outer Space, The Washington Quarterly, 45:1, 167-183, DOI: 10.1080/0163660X.2022.2059145

To link to this article: https://doi.org/10.1080/0163660X.2022.2059145

© 2022 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group

Published online: 25 Apr 2022.

Submit your article to this journal

View related articles

View Crossmark data
NATO’s vague recognition in 2021 that China constitutes a challenge to the transatlantic alliance reflects an institution that has failed to take on the security threats emanating from Beijing. Russia’s invasion of Ukraine on February 24, 2022 highlights the reasons why this omission is problematic. The war in Ukraine has reignited transatlantic unity of purpose in addressing threats from Moscow toward European security. The existential shock that Europe is facing now that a Russian regime has shown itself willing to go to war against European countries carries with it the risk that China will be forgotten when NATO discusses its future priorities. During the war, China is walking a tightrope between maintaining its commitment to sovereignty and territorial integrity and keeping up cooperation with Russia. The future strength of the Chinese-Russian partnership is likely to be determined by the continued usefulness of Moscow in China’s efforts to carve out more space for a Sinocentric international order based on authoritarian regimes. Meanwhile, China will continue to engender threats to the US and Europe in all domains and across geographical regions.

With the summit statement of the North Atlantic Council released June 14, 2021, NATO extended a commitment to “engage China with a view to..."
defending the security interests of the Alliance,” since “China’s stated ambitions and assertive behavior present systemic challenges to the rules-based international order and to areas relevant to Alliance security.” China's coercive policies, nuclear arsenal, military modernization, military cooperation with Russia, lack of transparency, and use of disinformation are listed as main areas of concern for the alliance. NATO takes the China challenge seriously but has yet to devise a strategy to address it.

Compared to the United States, Europe took a long time to acknowledge its stake in managing security challenges from China. As Beijing pushed beyond its traditional zones of interest in East and Southeast Asia toward the Indian Ocean in the 2000s, US security policies began to focus more on China as Washington sought a new geopolitical equilibrium in Asia. Since 2014, France and the UK have spearheaded Europe’s naval diplomacy to counter the displays of force and increasing tensions in maritime Asia to which China contributes. This engagement has focused on regular exercises with the US and its Asian allies, operations in support of freedom of navigation, and base-sharing agreements. In 2021, the EU recognized that these geopolitical dynamics directly impact its security and announced the establishment of supportive mechanisms in its Indo-Pacific strategy. However, NATO has been conspicuously absent in these transatlantic endeavors designed to counter challenges to US and European security. Reflecting NATO’s absence from the main arena of US-China strategic competition, the alliance is hardly ever mentioned in off-the-record conversations on Indo-Pacific security between diplomats and think tank personnel.

NATO’s reluctance to take on the China challenge is perhaps not surprising, given its inherent assumption that the European continent is the jewel in the crown of the US alliance system, which is thought to guarantee US assistance in the event of a military threat against Europe. This assumption was challenged during the Trump administration, which openly questioned the US commitment to Article Five’s collective defense obligation. The invasion of Ukraine has given NATO a new lease on life and put it at the frontlines of transatlantic cooperation on deterring Russia from further military action in future. However, NATO’s focus on its eastern frontline carries the risk that the alliance turns into a Russia-focused European institution and ignores that China is a global great power competitor which also constitutes a major challenge to the security of all NATO member states.
Washington increasingly looks to the EU rather than NATO for guidance on Europe’s future security policy. One reason is that NATO’s toolbox is lagging in domains such as cyber and outer space, although cyber and outer space operations are key enablers of actions in all domains including air, sea, and land. One indication of this is the US-EU negotiations surrounding a common response to cyber threats which took place during the first US-EU Trade and Technology Council (TTC) meeting in Pittsburgh in September 2021. In addition, during Trump’s presidency, longstanding US dissatisfaction with Europe’s modest defense spending threatened to put NATO on the backburner in transatlantic security debates. Since then, Russia’s invasion of Ukraine has elicited a sea change in German defense policy with the announcement in February 2022 that defense spending will increase to more than 2 percent of its gross domestic output annually. While this may be a convincing signal that Europe will finally devote the resources required for its own defense and revive NATO’s central role in transatlantic security, there is also a risk that China will be moved to the periphery of the alliance’s agenda.

On February 11, 2022, during the runup to the Russian-Ukrainian war, the Biden administration published its Indo-Pacific strategy as US Secretary of State Anthony Blinken was in the midst of a Pacific trip to Australia, Fiji, and Hawaii. This US prioritization signaled that despite Moscow’s war in Europe, Washington remains committed to strengthening its presence in the Indo-Pacific and competing with China. If the US drops the ball on the Indo-Pacific, Washington is concerned that China might use force against Taiwan. Consequently, the key question for the US is how many resources can be tied up in Europe without losing sight of the long-term goal: deterrence of China. As US strategic competition with China increases while NATO is sitting on the fence, failure to develop a transatlantic defense policy that addresses China will leave Europe vulnerable to China’s ability to exploit the weak links in European defense arrangements, which are newly fragmented by the Russian invasion of Ukraine.

EU efforts to build an independent regional defense profile and nurture cooperation between Europe’s defense industry and national defense communities reflect a growing recognition that the region needs to become a self-reliant defense actor. However, Europe still needs to demonstrate that self-reliance does not imply merely focusing on Europe’s periphery. Otherwise, the industrial challenges from China may outcompete Europe’s defense industry. Shipbuilding is a case in point. By 2021, China built 50 percent of all existing ships in the world. Through design collaboration agreements, cyber espionage, and acquisitions, China has copied advanced innovative ship designs. Enormous financial resources from the state allow Chinese companies to enjoy economies of scale by building dual-use factories which not only outcompete Western
companies in the commercial shipbuilding industry, but also threaten the production of navy vessels. If not taken seriously, Europe and the US may soon have no choice but to buy frigates from China. This example demonstrates the centrality of China for global economic and security developments and should encourage Europe to manifest a position of unified strength in defending NATO member states against Chinese security challenges. This realization will help convince the US and its adversaries that Europe continues to be a credible partner in countering common threats against transatlantic security, whether they appear in or beyond the European region.

China’s challenges to US and European security constitute such common threats across a broad range of sectors. These include gradual reinterpretations of principles of international law, the subversion of universal liberal market economic practices, and cyber insurgencies targeting a wide range of civilian and military entities. These Chinese policies all have major military implications because they are related to developments in the operating principles, capabilities, and priorities of China’s armed forces. Only NATO can offer an integrated transatlantic response to the military aspects of Chinese policies that threaten those sectors across the globe, including European actors. NATO’s involvement is essential if the credibility of the alliance’s security guarantees is to be preserved and an effective response to China’s encroachments on a liberal rules-based order is to be established.

The omnipresent character of the China threat demonstrates that it is long overdue for NATO to position itself as a significant player in addressing Beijing’s challenges to transatlantic security. NATO is key to keeping US and European security policies coordinated when applying mechanisms of deterrence and defense against Chinese challenges. If transatlantic unity of purpose is lost, both the US and Europe are far less likely to succeed in addressing China sufficiently.

Why Europe Should Care about China

Unsurprisingly, the Biden administration has continued the efforts of the Trump administration to neutralize Chinese threats to US primacy. The administration’s interim national security strategy states that China “is the only competitor potentially capable of combining its economic, diplomatic, military, and technological power to mount a sustained challenge to a stable and open international system.”
To address the China challenge, the US vows to promote “a favorable distribution of power to deter and prevent adversaries from directly threatening the United States and our allies, inhibiting access to the global commons, or dominating key regions.” Chinese efforts to replace the United States as the principal global great power induce Washington to engage in total competition with China, taking into account Chinese policies and strategies in all major economic, technological, industrial, environmental, diplomatic, and defense policy decisions.

Europe does not face any such structural challenge to its position. However, it does face a challenge to its way of life. Europe is the US ally most concerned about the liberal principles of world order that form the basis of post-World War II institutions, including NATO: representative democracy, the rule of law based on the separation of powers, and individual human rights. The United States also expresses uneasiness about China’s challenges to these values. However, Washington considers the preservation of its primacy a precondition of preserving a liberal rules-based order. Hence, it prioritizes its Asian allies. The geographic location of US Indo-Pacific allies puts them at the center of military-strategic competition between Washington and Beijing and makes them equally concerned about Chinese assertiveness and hegemonic aspirations.

Asian allies share the European dilemma of how far to travel down the route of joining forces with Washington in countering Chinese threats. Cooperation with Washington today triggers the classical alliance concern of abandonment versus entrapment. A good example is US-China space and naval competition, sectors in which modern Chinese weapons are eroding US deterrence. Australia is central to the evolving US space and naval security agenda. Canberra has expanded its capacity for communications and intelligence in outer space to play a key role, integrating its space activity with US space systems so it will be difficult for an enemy to target the US military alone. But on the flip side, Australia is now exposed to threats such as advanced cyberattacks against jointly operated satellites. Similarly, Canberra has decided to build long-range nuclear-powered submarines, which take Australia into the heart of naval warfare in East and Southeast Asia. In the event of war, Australian attack submarines may therefore become a prime target for China to defend its nuclear missile-launching submarines, and hence a nuclear deterrent and a carrier-strike option against the United States. Australia faces entrapment concerns since it risks being drawn into great power conflicts due to risky or offensive behavior which it would prefer not to get involved in.

Canberra’s fear of abandonment appears to have trumped fears of entrapment and a loss of strategic autonomy. Australia does not have the capabilities to defend its territory and is relying on the United States to do so. Europe, by
virtue of its geography, may be less inclined to make the same cost-benefit analysis. The region is less exposed to China’s hegemonic aspirations in the Indo-Pacific and more concerned about entrapment. Under Biden, sanctions designed to defend liberal norms such as freedom of speech, democratic representation, and minority rights will remain in place as a demonstration of US support for liberal values. Washington has also formally reengaged in the multilateral institutional frameworks of the United Nations (UN), the World Trade Organization (WTO), and the World Health Organization (WHO), just as it has recommitted to NATO. However, at the same time, Washington’s attention and resources are directed at new fora and ways of working together through an intermeshing network of partnerships—such as the Quadrilateral Security Dialogue (QUAD) with Japan, India, and Australia—and new intensified affiliations between countries such as Japan and India, Australia and Japan, and Taiwan and India. As US-Chinese competition becomes increasingly militarized, the US may gradually shift its focus towards these fora where China threats are front and center of decision-making. This speaks volumes about the US prioritization of neutralizing China’s threat against its primacy.

European defense postures, however, are primarily directed towards Russia, the Middle East, and North Africa rather than China. Divergent US and European defense postures have caused decisionmakers and commentators to argue that NATO is primarily responsible for threats emanating from the European neighborhood. France and Germany have emphasized that NATO should focus on addressing threats in Europe’s periphery to avoid entrapment in US-Chinese strategic competition. It seems Paris and Berlin prefer to develop a military-strategic presence vis-à-vis China based on the more flexible format provided by EU mechanisms and nationally-based agreements between European capitals, staying clear of stifling formal collective defense obligations in their contributions to countering threats from Beijing.

Abandonment is downplayed as an unlikely scenario in Europe. Analysts point out that if contributions to bilateral NATO projects are taken into account, US contributions to NATO actually grew during Trump’s presidency, despite his overt skepticism of the value of alliance commitments for US security. Moreover, allied cooperation with the United States in Europe’s geographical periphery has never been stronger. The implications of the swift US withdrawal from Afghanistan without NATO consultation is brushed off as an action of no consequence for US security commitments elsewhere because Washington had little interest in continuing a losing battle in Afghanistan that prevented it from directing resources toward more pressing threats emanating from China and Russia.

And yet, in the event of US involvement in using force in a conflict with China, it is likely that Washington would redeploy forces stationed in and near Europe to the Indo-Pacific. In the absence of a European commitment to
participate in countering China challenges, and if forced to choose, the Indo-Pacific is likely to trump Europe on the US list of security priorities. This scenario has given rise to the argument that to restore the credibility of NATO’s collective defense commitment, a division of labor between the United States and Europe would be desirable. Such an arrangement would allow the US and its Asian allies to focus on countering China threats in the Indo-Pacific, while Europe concentrates on countering Russian threats, providing more effective defenses collaboratively against threats from China and Russia.17

Rather than highlighting the need for a division of labor within NATO, the 2022 invasion has highlighted that Russia’s appetite for threatening Europe with military action is closely entwined with its long-standing strategic cooperation with China. Intelligence reports that China told Russia in February 2022 not to invade Ukraine before the end of the Winter Olympics in Beijing testify to the closely orchestrated Chinese-Russian approach to the West.18 Moscow and Beijing are both strategic opponents of the US, a shared status that has spurred them to coordinate their separate geostrategic priorities in Europe and the Indo-Pacific, forging unison pushback against what they consider Western encroachments on their spheres of interest.19 The poorer than expected performance of the Russian armed forces in its 2022 war with Ukraine has pushed China to try to appear neutral. Nevertheless, China has joined Russia in opposing further enlargement of NATO, and in the Indo-Pacific, Russia has joined China in opposing Taiwanese independence.20 It would be wise for Europe and the US to plan for Sino-Russian geostrategic coordination to continue unless more clear evidence that China will abandon Russia is presented. One thing is certain: China will work with the partners that help it advance a Sinocentric international order based on authoritarian regimes. And to counter this development, Europe and the United States need to devise effective mechanisms for joint responses to Beijing as well as to Moscow.

A US-European division of labor is not likely to help NATO develop tools to defend itself against threats from China and Russia. The lack of electronic warfare in Russia’s war with Ukraine has revealed gaps between its concept of operations and the tactics of the Ukrainian military. As demonstrated in prior operations in Syria and the Donbas, Russia will adapt and learn in the short and long term. For example, Russia can be expected to improve its electromagnetic spectrum management in order to enhance its planning and management of forces on the battlefield. Meanwhile, China is watching the performance of the parties involved in the war with a view to update its cyber and space capabilities as well as strategic concepts. As a consequence, both Russian and Chinese threats will continue to increasingly emerge in the cyber and space domains. This calls for global and functional defenses rather than an exclusive geographical focus. It is more important than ever to
design NATO for a future where threats toward transatlantic security are global and requires a unified response.

Even if the balance of forces between the United States and Europe is asymmetrical, the response to Chinese and Russian threats should be joint. In a perfect world, NATO would respond as it did in 1966 when France filed for divorce: redefine the purpose of the alliance by expanding it. In 1967, the Harmel report added to the original purpose of defending member states with the management of European security writ large. Ideally, in 2022 a similar exercise would globalize NATO’s purpose to encompass defending the transatlantic member states against threats from China in all domains and across geographic regions. However, since 1967, US security interests have moved away from Europe and the post-Soviet sphere and put China and the Indo-Pacific region at the top of the US list of priorities. Washington is not likely to volunteer to spend time and resources renegotiating the fundamental political and military transatlantic relationship. If NATO took on a similar effort, it is likely to produce institutional disintegration and paralysis. Instead, NATO must put existing resources and mechanisms to good use to demonstrate its relevance for addressing the China threat in all domains and in the Indo-Pacific. The strategic question for NATO should not be whether, but how?

NATO cannot continue to stand by idly while its member states are redirecting their foreign and defense policies to take into account Chinese encroachments on European security without losing credibility as an adequate guarantor of transatlantic security. It is not only the US that has turned its attention toward the Indo-Pacific; NATO member states such as the UK and France, as well as the EU, are recognized as significant contributors to Indo-Pacific security efforts in the US Indo-Pacific strategy. The US encourages NATO to continue to focus on committing more attention to the Indo-Pacific, an indication that so far the alliance has been largely absent from security initiatives in the region. NATO invariably goes unmentioned when deterrence of China is on the security agenda of major powers. Engaging NATO in US and European naval diplomacy would allow NATO visibility on China issues, but it would also meet with insurmountable resistance from significant US partners in the Indo-Pacific, such as France and Germany. If European or US vessels and aircraft were to fly the NATO flag when participating in freedom of navigation operations in the South China Sea to counter China’s claims to historic waters and demands for
prior notification of military vessels, Beijing is likely to respond in line with its current position of issuing warnings and pursuing such military vessels. The fact that relaxed prospective responses from Beijing seem highly plausible diagnoses the problem: NATO is no longer a cause for concern for China, who does not believe the alliance can agree on a collective transatlantic response to Beijing’s security challenges.

Although NATO visibility may be desirable, it may also not be the best place to start working on increasing the alliance’s role in getting into the game of deterrence of China. French and German resistance toward allowing NATO to play a role in the Indo-Pacific far from the European continent stems from entrapment concerns. Such resistance to the alliance’s involvement indicates that NATO has to prove capable of combining US and European views on how to deal with China threats without increasing the entrapment potential in the eyes of key European allies.

**NATO in Cyber and Outer Space**

Cyber and space is a promising arena for NATO to address China challenges by building member state resilience. Like the air and sea domains, as areas that belong to no one state and which provide access to much of the globe, they form part of the global commons. Command of the commons has been the key enabler of the US global position of power for many decades. However, China wields a sufficient range of sea, air, cyber, and space capabilities such that the global commons is now a contested zone. In contrast to the sea and air domains, cyber and space are sparsely regulated. This lack of international norms enhances the risk of conflict based on misperception, making NATO cooperation pertinent. Adversarial activities toward the US and Europe in the cyber and space domain threaten transatlantic security. These come not just from China, but also from other adversaries such as Russia and Iran. Mechanisms for addressing these challenges in the military sector are essentially generic and not, at least in their basic design, established with a particular country in mind. Thus, cyber and space provide an avenue for NATO to contribute without major internal resistance. NATO would also benefit from long-standing US-EU cooperation on cyber and space issues.

NATO has vowed to clarify Article Five’s collective defense commitment to encompass threats to satellites in space and coordinated cyberattacks. NATO can design this effort to include adversarial behavior from China. The alliance
already has an array of instruments to deal with cyber and space challenges from adversaries. These can be extended to encompass China without pronouncing it a threat.28 This approach allows the US and Europe time to adjust their cooperation to take into account the fact that China poses military threats to them both without explicitly using the language of threat at a time when NATO members do not agree if China should be defined as a challenge that can trigger Article Five responses.

Since the late 1990s, the vulnerability of shared space assets to cyberattacks has been a concern for both the US and Europe. For example, in 1998 a US-German satellite, used for peering into deep space, was rendered useless after it turned suddenly toward the sun, damaging its High Resolution Imager by exposure. NASA later determined that the accident was linked to a cyber-intrusion at the Goddard Space Flight Center. Coordinated cyberattacks have emerged as a major threat to both the US and Europe since the late 1990s. For example, for about eighteen minutes on April 8, 2010, China Telecom advertised erroneous network traffic routes that instructed US and other foreign internet traffic to travel through Chinese servers. Other servers around the world quickly adopted these paths, routing all traffic, including government and military traffic, to about 15 percent of the internet’s destinations through servers located in China.29

In the future, the need to enhance situational awareness in space is likely to lead to further integration of space assets between the US and its allies. Civilian entry points are likely to provide a growing opportunity for infiltration. The weak state of cybersecurity in civilian agencies should also be considered. Chinese military doctrine prioritizes weaponry that targets vulnerabilities in the deployment of US and allied power, such as the use of cyberattacks to disrupt surveillance assets, intelligence networks, and command-and-control systems.30 These threats are significant, since next generation systems, including fighter aircraft, destroyers, and special forces, will not function without access to space communication and space-derived data.

Although European and US allies have indigenous space programs outside the NATO framework, cyber security and outer space would be a useful field for joint explorations of how to divert and manage attacks and identify an agency which can coordinate transatlantic responses to attacks. Allies are embedded in a range of information networks which may be disrupted, giving rise to alliance management concerns emerging from attacks. The lack of red lines regarding behavior in cyber and outer space between the US and its allies on one hand, and adversaries such as China on the other, adds to the risk of misperception and escalation, and hence also highlights the need for allied coordination to avoid starting a war by mistake. An improved NATO dialogue on safeguards and alliance consultation could also assist communication with China on arms control and conflict prevention in cyber and outer space, which is not currently taking place.
Looking to the future, NATO’s success in establishing transatlantic mechanisms for cyber and outer space safeguards and consultation will be crucial to allow NATO a key role in taking on the China challenge in ways that help restore faith in NATO’s credibility as a provider of collective defense in all domains. It will also assist NATO in straddling the chasm between member states prioritizing threats from either China, Russia, the Middle East, or North Africa, since cyber and space threats potentially stem from all of them, and the effectiveness of cyber and space defense mechanisms do not necessarily depend on geographical origin.

Improved communication between NATO and the EU will be essential for NATO to successfully address the military aspects of cyber and space threats. The framework for permanent EU-NATO relations, Berlin Plus, was concluded in March 2003. It allows for the exchange of classified information, the EU’s use of NATO assets and capabilities for EU-led crisis management operations, and the establishment of consultation arrangements. Due to disagreements over responsibilities and jurisdiction, however, meaningful coordination did not take place until July 2016. On this occasion, NATO and the EU issued a joint declaration stating their intention to work together on security and defense responses to unprecedented challenges emanating from the South and East of the Euro-Atlantic area. During Biden’s visit to Brussels in June 2021, NATO promised to strengthen cooperation with the EU on promoting peace and stability including protecting critical infrastructure, strengthening resilience, maintaining a technological edge, and addressing challenges to a rules-based order. The EU-US summit statement from the same visit merely reaffirms support for robust NATO-EU cooperation and promises to strengthen the partnership. At the level of policy implementation, it is clear when talking to NATO and EU officials that usually they do not coordinate their strategies and tactics for countering China challenges.

The EU-US summit statement’s negligible mention of cooperation with NATO indicates that the ball is in NATO’s court if strengthening NATO-EU coordination is to take place. French and German concerns about entrapment are a major barrier to meaningful NATO-EU cooperation. The area of cyber and space security may allow NATO to work around this roadblock. In line with the EU’s practice of supporting the efforts of groups of member states to take the lead on issues where EU institutions cannot trump sovereignty, in the area of cybersecurity the EU has decentralized implementation to work around national resistance. This has allowed the EU to respond...
collectively and effectively to cyberattacks in Europe, primarily through bolstering capacities and law enforcement cooperation. However, the EU is not yet a globally influential and effective cyber-power because differences among member states over issues such as whether to prioritize tech sovereignty or Europe’s global tech competitiveness prevent the EU from acting in unison on the global stage.

The first US-EU TTC meeting held in September 2021 was an important step in strengthening the EU’s global position in cooperation with the United States, and hence called into question whether NATO has a role to play in cyber security. The next couple of years will demonstrate whether the EU and the US are able to focus on becoming mutually supportive global cyber security guardians by cooperating on strengthening investment screening, export controls, and rebalance global supply chains in semiconductors. The successful implementation on both sides of the Atlantic of the recommendations of the TTC working groups will determine if transatlantic cooperation positions the US and the EU as global partners in guarding cyber space. In part, this will depend on the EU’s ability to forge common positions that meet the US halfway on issues such as tech sovereignty and data privacy, points of contention through which transatlantic relations have been marred by conflict.

The potential convergence of transatlantic views on cybersecurity leaves room for NATO to play a significant role because the EU is a civilian and economic, rather than military, set of institutions. The NATO summit in Brussels in 2018 carved out a role for NATO which the EU cannot fulfill, allowing NATO members to integrate their sovereign cyber capabilities into NATO operations and missions. However, compared to the EU’s major role in cyber, NATO’s role is negligible. As EU civil-military cooperation ramps up in enhancing Europe’s autonomous defense profile while allowing US companies a role in this effort, the union looks set to become an even more dominant actor in transatlantic cyber defense. Because NATO is a military organization, it has the procedures and instruments to position itself in a key role in coordinating and implementing the military aspects of cyber defense between the US and Europe. The multinational cybersecurity effort which is confronting the global threat posed by Chinese state-sponsored cyberattacks involves NATO, the EU, Australia, New Zealand, and Japan, and sets NATO off to a good start in enhancing its profile in countering Chinese challenges to transatlantic cybersecurity. However, it remains to be seen if it manages to deliver mechanisms that succeed in integrating allied responses in the military sector in a way that complements US and EU cyber defense initiatives.

In outer space, the EU is also increasingly active, recognizing the need to deepen investments in areas such as satellite navigation, earth observation, space situational awareness, and secure communications, which are all central
to enhanced space security. The EU has established the EU Agency for the Space Programme, which has oversight over everything the EU does in orbit as a bloc. Moreover, the EU uses the European Space Agency (ESA) as technical advisor and industrial procurement agent. This setup allows the EU to become more agile, dynamic, and innovative in space as rapid industrialization is taking place with US entrepreneurs and well-funded Chinese space programs in leading roles. In the pipeline are a next generation of Europe's satellite-navigation system, Galileo, and an extension of the scope and capabilities of its Copernicus-Sentinel spacecraft, which monitors the state of the planet. The EU focuses on ensuring that Europe has independent space capabilities, but it does not develop instruments such as space weapons systems.

In the outer space realm, NATO has tremendous potential for playing a key role in developing instruments in the military sector that involve European and US space capabilities. NATO's decision to declare outer space an operational domain at the London summit in 2019 is a first step in allowing NATO an active role in addressing growing anti-satellite threats from China and Russia. With the US as the leading power in outer space and with the EU developing its space platforms to enhance situational awareness and security, NATO has the tools to work out a common transatlantic definition of the anti-satellite challenges that need to be addressed. The establishment of mechanisms that ensure coordination across military NATO commands regarding intelligence gathering and the interface between cyber and space defense, as well as civilian and military occurrences and initiatives, would potentially strengthen the ability of allies to counter anti-satellite threats considerably. As with cyber, NATO must first integrate the space issue into all its organizational and operational structures, and secondly, develop mechanisms that focus on coordination between US and European capacities on the basis of a common understanding of the challenges to be addressed.

NATO's Role in the Global Commons

NATO can only be as effective as its member states allow it to be. NATO reflects the state of transatlantic relations: are US and European security outlooks sufficiently compatible such that the alliance is able to address threats from China collectively? This question is reflected in how well they manage to define common challenges and establish mechanisms that allow them to address these
challenges together. NATO was a natural center of security focus for Washington when Europe was the main arena for US-Soviet deterrence. Today, the Indo-Pacific competes for US attention and resources as competition with China has moved to the center stage of US security and defense priorities.

The strategic shift in US priorities does not mean that Europe cannot continue to remain a significant influence on global security dynamics. The EU has demonstrated its continued relevance in the security realm, not merely by relying on its role as a major trade bloc, but also by reforming the interplay between member states and EU institutions to avoid being paralyzed by consensus requirements, which apply in most areas outside the trade sector. This is done by providing platforms for member states to start initiatives. If successful in attracting support within the union, the initiatives are consolidated by supportive mechanisms and programs.43

NATO is not the EU and hence should not duplicate its methods. The EU is driven by the urge to secure the continued influence of its member states on major global issues. NATO’s raison d’être is to facilitate transatlantic cooperation in the military sector to counter common threats and challenges. Coordination is complex at a time when US and European security outlooks are drifting apart in terms of threat perceptions and priorities. At the same time, fears of entrapment stifle NATO’s efforts to update its relevance, principally because key members such as France and Germany are not interested in NATO taking on China as a threat.

Nevertheless, NATO’s agreement to define China as a challenge promises opportunities for positioning the alliance in a key role in transatlantic relations. Because cyber and space encompass threats from other adversaries such as Russia and Iran, these domains are a good place to start taking on China as they do not require that China be singled out as a threat. By taking on the responsibility for coordinating US and European definitions of cyber and outer space threats in the military sector, integrating these domains in all organizational and operational NATO structures, devising mechanisms for the member states to address cyber and outer space threats, and by facilitating intelligence exchange and management of the vulnerabilities produced by civil-military interaction and overlapping interfaces between the cyber and space sectors, NATO can demonstrate its continued relevance for transatlantic security in an era where threats are increasingly global and transcend geographical boundaries. There’s no time like the present.

ORCID

Liselotte Odgaard http://orcid.org/0000-0002-3244-4920
Notes

25. Interviews with anonymous Chinese generals conducted by author, September 2021.
27. Interviews with EU officials conducted by author, November 2021.
28. Interviews with NATO officials conducted by author, November 2021.
35. Interviews with EU and NATO officials conducted by author, November 2021.


41. Interviews with NATO officials conducted by author, November 2021.
