

N F S
A U E
T T M
O U I
S R N
E A
R

November 18-21, 2021



WELCOME TO NATO'S FUTURE (SEMINAR)!

2021 was full of challenges in the international affairs: continuous spread of the COVID-19 pandemic, economic problems in the post-pandemic era, Russia's aggressive actions in Eastern Europe, continued threat of terrorism, China flexing its economic and military muscles, sophisticated cyber-attacks, proliferation of nuclear weapons and growing security impact of climate change.

As all these transnational problems can be only be tackled when states work together, the international cooperation among the transatlantic allies has become even more important. For NATO, the chaotic end of its military presence in Afghanistan has highlighted the need for the assessment of its engagements. Now it is too early to draw final conclusions and lessons learned. However, one conclusion is clear: the crisis in Afghanistan has not changed the need for the USA and Europe to stand together in a more dangerous and competitive world.

The NATO's Future Seminar will also look at the current challenges for the Alliance. In this booklet, one can find the perspectives and policy recommendations of our seminar participants in the collection of their essays.

Since 2007, the Youth Atlantic Treaty Association Germany (YATA) has served as a leading platform for young professionals in security and defense, working alongside our ATA seniors and fellow youth organizations to ensure that young professionals have a voice in the policy-making world and personal access to national and international events. In 2020 the recommendations of the seminar participants were even presented to Ambassador Bettina Cadenbach, NATO Assistant Secretary General for Political Affairs and Security Policy at the large international conference NATO Talk 2020 with more than 800 online followers. For the participants of our seminar, it was the highlight of the whole weekend that their ideas were read and commented by such a high-level NATO official.

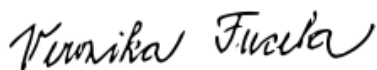
YATA Germany holds the NATO's Future Seminar for the eight time this year, encouraging and deepening the international as well as the cross-generational debate on current security issues. It provides a forum for an exchange of ideas and mutual understanding while bringing together more than 20 young professionals, scholars, senior experts, and NATO as well as government officials from some 10 countries (NATO member and partner states). More than 90 outstanding applications from more than 24 NATO and partner countries motivated us to continue our engagement for YATA Germany and to inform young leaders about the importance of NATO and the transatlantic partnership.

This year, the following three topics were selected by YATA members for the seminar. All of them share one essential feature: the necessity of NATO to broaden its scope, to prioritize threats, and to develop measures to attain collective security:

1. The Ability to Innovate: How the Alliance Integrates Operational Readiness, Innovation and Modernity
2. NATO's European Pillar: Shape, Size, Function?
3. New Era of Transatlantic Cooperation: A Common Position Towards China?

Our seminar would not be possible without the great and generous support of the German Atlantic Association (DAG), especially Kamala Jakubeit, as well as NATO's Public Diplomacy Division (PDD). I also would like to thank all our active YATA members who devote their time and energy for our work and our targets. We are thankful for their contributions as well as for our brilliant speakers and chairs who take the time to enrich our discussions with their expertise, insights, and curiosity. Thank you all for participating so actively in this endeavor and your commitment to making young voices an audible and visible part of "NATO's Future".

Sincerely,

A handwritten signature in black ink, reading "Veronika Fucela". The script is cursive and fluid, with the first name and last name clearly distinguishable.

Veronika Fucela
Chairwoman of Youth Atlantic Treaty Association Germany

LOGISTICAL INFORMATION

Travel

After the seminar you will receive a form with which the travel costs will be reimbursed. Travel within Germany can be reimbursed up to 100€, international travel up to 200€.

Entry regulations

Please familiarize yourself with the applicable entry regulations. Unfortunately, we cannot provide assistance in case of any difficulties.

Covid-19 Situation (as of Nov. 17, 11 a.m.)

Regulations can change every day. Please keep yourself updated; we cannot accept responsibility should last-minute changes make participation in the program no longer possible. Please note that most establishments (restaurants etc.) in Berlin apply the so-called 2G+ rule. This means that the stay is only possible for vaccinated or recovered persons with a current (no older than 24 hours) Corona test (no PCR!).

Please note:

- In the Hotel, the 2G rule applies (vaccinated or recovered persons)
- The NATO TALK on Friday will take place under application of the 2G+ rule.
- The NATO's Future Seminar will take place under the application of the 2G rule.

Please make also sure to always have a FFP2 masks with you.

Corona testing is possible throughout the city. Tests are free of charge.

NATO TALK & Alternative Programm

We are delighted to invite you to take part at the NATO Talk 2021. Due to the situation, YATA guests will be able to participate at the session on "Crisis Management "Out of Area" - Strategic Lessons taken from the Afghan Mission".

We will meet at Schiffbauerdamm 12, Berlin at 12:45 pm. Entrance based on 2G+ Please be on time, the event will take place on the river cruise ship "Pioneer One". Being on time here is absolutely crucial since the ship will not be able to wait for us.

During the NATO Talk conference on friday morning, you can follow the NATO Talk (featuring NATO SG Stoltenberg via live stream (Registration at: ata-dag.de/natotalk2021/) or you can join us for a walking tour through Berlin, led by a Berlin - based YATA Alumna (or explore the capital on your own).

Social Media

Please note, that we will also cover the seminar on Twitter (@yata_ger) and facebook. So, make sure to follow us and feel free to share impressions. Hashtag will be: #NATOsFuture. Chatham House rules applies during workshop time. Panel discussions are open.

Hotel

Select Hotel Checkpoint Charlie Berlin (Hedemannstraße 11/12, 10969 Berlin). Single rooms are booked for all requesting accommodation. Check In is possible from 3 p .m. onwards.

Event Location

Forum Factory Berlin (Besselstraße 13-14, 10969 Berlin)

AGENDA

Thursday, 18.11.2021

Select Hotel Berlin Checkpoint Charlie, Hedemannstraße 11/12, 10969 Berlin
06:15 p.m. *Meeting at Hotel and Walk to Dinner*

Barcelona Tapas Bar, Friedrichstraße 211, 10969 Berlin
06:30 p.m. *Informal Dinner and Networking*

Friday, 19.11.2021

Select Hotel Berlin Checkpoint Charlie, Hedemannstraße 11/12, 10969 Berlin
09:00 a.m. *City Walk*

09:15 a.m. *NATO TALK online participation*

Schiffbauerdamm 12, 10117 Berlin
12:45 p.m. *NATO TALK Live participation*

07:00 p.m. *Informal Dinner and Networking - Informal debriefing conference*

Saturday, 20.11.2021

Forum Factory, Besselstraße 13-14, 10969 Berlin
09:00 a.m. *Welcome*

09:15 a.m. **Group Working Session I**

10:45 a.m. *Break*

11:15 a.m. **Group Working Session II**

12:45 p.m. *Lunch*

02:15 p.m. **Panel discussion I**
The Ability to Innovate: How the Allianz Integrates Operational Readiness, Innovation and Modernity

03:45 p.m. *Break*

04:15 p.m. **Panel discussion II**
NATO's European Pillar: Shape, Size, Function?

06:15 p.m. *Dinner*

07:30 p.m. **Fireside Chat**

Sunday, 21.11.2021

Forum Factory, Besselstraße 13-14, 10969 Berlin

09:00 a.m.

Panel discussion III

**New Era of Transatlantic Cooperation: A Common Position
Towards China?**

10:30 a.m.

Break

11:00 a.m.

Group Working Session III

12:30 p.m.

Break

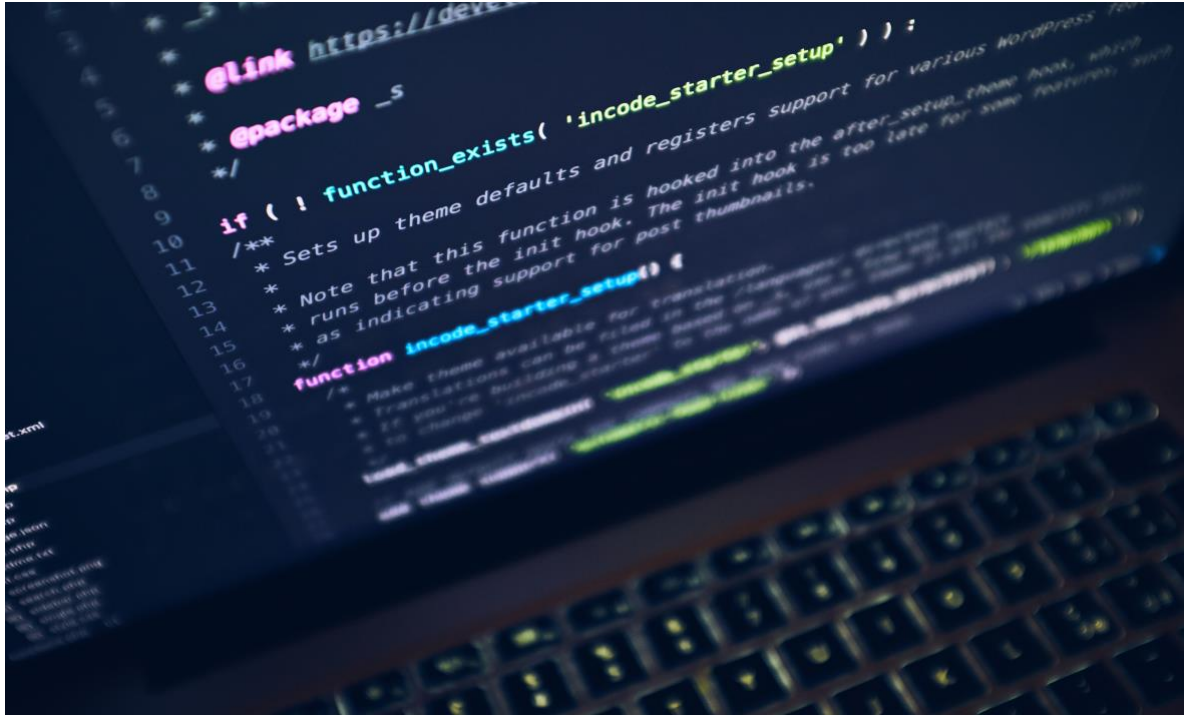
12:45 p.m.

Presentation of the Recommendations & Wrap-up

02:00 p.m.

Farewell Lunch

PAN | The Ability to Innovate: How the Alliance EL 1 | Integrates Operational Readiness, Innovation and Modernity



© Photo by Luca Bravo on Unsplash

To maintain their strategic edge in an increasingly contested world, the United States, Europe and NATO must understand how to leverage emerging and disruptive technologies (EDT) to enhance shared security and better prepare for future crises. A critical factor in their success will be NATO's ability to communicate and operate across militaries, domains, and a wide range of EDT-enabled capabilities. This requires enhancing standardisation and interoperability across the Alliance's concepts, doctrine, capability targets, and technical requirements related to EDT. The purpose of the workshop is to understand transatlantic perspectives, discuss the pros and cons of public-private cooperation, and identify ways in which policy could be coordinated on defense technology issues.

PANELISTS



Gabi Dreo
Director, Research Institute
CODE (Cyber Defence),
Universität der Bundeswehr
München

Gabi Dreo heads the Chair of Communication Systems and Network Security at the Bundeswehr University in Munich. She is director of the research institute CODE (Cyber Defence), member of the advisory board and supervisory board of Giesecke+Devrient GmbH, member of the supervisory board of BWI IT GmbH and BWI Systeme GmbH and member of the administrative board of the German Research Network. Prof. Dreo studied computer science at the University of Maribor, Slovenia and received her PhD and habilitation from Ludwig-Maximilians-University Munich. In 2016, she received the Europe Medal from the Minister of State Dr. Merk. Her research focuses on IT security of networked systems, network technologies such as Software Defined Networking and NVF, IoT as well as Smart Data.



Denis Mujkanovic
Vice President Corporate
Procurement for New
Technologies, DHL

Denis Mujkanovic has been the Vice President of Corporate Procurement for Digital Services and New Technologies at Deutsche Post DHL Group since November 2017.

In this role, he has the global responsibility to procure and contract the most innovative solutions in areas such as robotics, data analytics, process mining and cloud computing. Further, he led the team which created the supplier innovation program (TRAILBLAZER) of Deutsche Post DHL, bringing market experts and logistic teams together to innovate in logistics and scale solutions. Prior to this role he held several positions in IT consulting and outsourcing procurement. Denis Mujkanovic is also a regular speaker and panelist at global procurement conferences in the areas of digitalization and automation of Procurement. Mr. Mujkanovic is trained in business management and information systems management.



Moritz Zimmermann
Staff Officer, Innovation Unit,
Emerging Security Challenges
Division, NATO

Moritz Zimmermann is a staff officer in NATO's Innovation Unit within the NATO International Staff's Emerging Security Challenges Division. He previously worked for NATO's Science for Peace and Security Programme, the Operations Division of the NATO International Military Staff and the European Commission. The views expressed are his and do not necessarily reflect those of the North Atlantic Treaty Organization.



André Loesekrug-Pietri
Chairman, Joint European
Disruptive Initiative

André Loesekrug-Pietri, held leadership positions in private equity, government, industry and as an entrepreneur. Starting as assistant to the CEO of Aerospatiale-Airbus, he then spent 15 years in private equity and venture capital. In 2017, he became Special Advisor to the French Minister of Defence, responsible in particular for technology and innovation. He is the Director of the Joint European Disruptive Initiative (JEDI), the European Darpa. Graduate from HEC and from Harvard Kennedy School, he attended Sup-Aero aerospace engineering school.

CHAIRS



Rafael Gehring
Program Leader Digital
Transformation, DHL

Rafael has over 10 years of international supply chain and logistics experiences across Europe, Asia Pacific and the US for the Private sectors. He has led large scale negotiations in Software related sourcing initiatives, successfully worked strategies for country organisations across Europe and currently leads a Digital Transformation program for a national operation. He has a strong background in negotiations, sourcing and supply chain sales strategy having worked in a variety of roles in this context. Besides his industry experience he also lectures supply chain & logistics management at DHBW Stuttgart University.



Mirco Giannini
Medical Officer,
German Federal Army

Mirco is a prospective medical officer at the German Federal Army and currently in the final semester of his studies at Charité Berlin. He served as an intern to the Bundeswehr Command and Staff College and as Assistant to the Senior Medical Officer of the 10th Armoured Division. Currently he is preparing for his deployment to the Bundeswehrkrankenhaus Berlin.



Leonhard Simon
Communications Manager,
Munich Security Conference

Leonhard Simon works as Communications Manager at the Munich Security Conference (MSC). In this position he coordinates the production of all digital communication content including conducting interviews with high-level participants. He received his Master's degree studying International Security in Barcelona and his Bachelor degree in international politics studying in Munich and Cork, Ireland. Leo works also as freelance photographer. In July 2019, he was elected as a member of YATA Germany's executive board.

INNOVATION FOR A STRONGER NATO COOPERATION

by Arzu Abbasova

NATO's ability to adapt to the changes in the world has made it a successful alliance, said Secretary- General Jens Stoltenberg in his 2020 speech. Yet, it is undeniable that the security environment has been changing in the last decade with the rising threats from cyber and hybrid attacks, necessitating military, the political and institutional adaptation from the NATO ensuring Alliance's adaptability, efficiency and solidarity. On one hand, Russia and China investing in new technologies has highlighted the return of power competition with a technological edge, while on the other hand enhancements in AI, quantum technologies, machine learning has given the signs of emerging ways that the wars can be fought. In fact, today the security threats do not necessarily come from land or sea but can be generated by humans from remote sources, from space, cyberspace or from unmanned systems. This is to say, the defence does not only encompass using military equipment but is also about a fight against algorithms and bots.

NATO has indeed recognized the need for advancing its technological capability and integrating innovation and modernity. Thus, particularly in the last few years different initiatives including Innovation Board, Advisory Group on Emerging and Disruptive Technologies, Innovation Unit within the Emerging Security Challenges Division were created. The allies have also pledged to launch a Defense Innovation Accelerator for the North Atlantic (DIANA) and the NATO Innovation Fund to encourage interoperability and adoption of new technologies. Although these already demonstrate Alliance's attention and efforts, still there is more that NATO can do to maintain its strategic edge. Below the currently existing challenges are described with certain policy recommendations on how NATO can tackle them.

Challenges and recommendations:

1. Bridging the technological gap: There is a technological gap between the allies which hinders the interoperability while also diminishing the alliance cohesion. Some of the leading allies already have identified a focused approach on the incorporation of new technologies, while smaller states like Central or Eastern European countries lag behind in this regard. To deal with this problem,

NATO shall encourage more targeted defence investments and focus on supporting industrial specialization across its members. Indeed, similar to the cybersecurity field small allies can concentrate on developing very specific technological capabilities through which they can contribute to both Alliance's defence and bridge the technology gap. Yet, it is important to prevent duplicity and use targeted efforts. For ensuring organizational clarity NATO can adopt a system of allocation or allies can agree on sharing arrangements.

2. Public-Private Sector Collaboration- Research and Development and integration of new technologies and innovation to NATO have high importance for ensuring the Alliance's technological edge. Nevertheless, many of the technological advancements particularly in the case of EDTs take place in the private sector which quickly responds to the emerging needs and incorporates the updates. This also means that NATO is not the main innovator of these technologies, and its adaptability depends on how strongly it builds civilian-military relations. Thus, NATO shall introduce a new alliance wide framework allowing to detect relevant technologies and to acquire and integrate innovation from the private sector in high speed.
3. Benefits of cooperation- It is worth noting that, the challenges that NATO faces are also experienced by the European Union which on its own develops mechanisms against the emerging technological threats. As an example, the European Defense Fund supports R&D and encourages an innovative and competitive defence base. Knowing that the same efforts are undertaken via these two organizations, overlapping capabilities, talent, budgets for defence investment can be easily identified. To turn this duplication into an advantage, NATO and the EU need to work out a mechanism of collaboration where their work and spending can be wisely coordinated and jointly regulated.
4. Competing with Brainpower- Both Russia and China have been substantially investing and accelerating their technologies. To win this competition, talent acquisition and benefitting from human capital is essential for NATO. As such, there shall be a triangular alliance between academia, governments and the industry bringing together the universities, startups and governments to innovate more and ensure adaptability.



Arzu Abbasova
Research Assistant, Cyber, Space
and Future Conflicts Programme,
International Institute for
Strategic Studies (IISS)

Arzu Abbasova is a Research Assistant at Cyber, Space and Future Conflicts Programme at International Institute for Strategic Studies (IISS). She is also currently a graduate student in a dual master's degree program in International Security and International Relations at Sciences Po, Paris and London School of Economics. Prior to her graduate studies, she obtained a first-class degree in International Relations from SOAS, University of London. Previously, Arzu worked as a research assistant at Sciences Po, Paris. Her academic interests include cyber security, conflict resolution and foreign policy analysis.

THE ABILITY TO INNOVATE: HOW THE ALLIANCE INTEGRATES OPERATIONAL READINESS, INNOVATION AND MODERNITY

by Maria Bertomeu Pardo

Since its founding, NATO holds the ability to adapt and innovate thanks to the tools, the structures and the people in place to foster creativity and innovation, which have guaranteed NATO's military superiority and assured its technological edge against rivals for seven decades. Today, we are embarking on a new stage of adaptation and survival in which NATO's competition is global and has a strong technological dimension.

Since the end of the Cold War, the security environment has become more complex. Recent years have seen the rise of multipolar great power competition, where new technologies as instruments of state power are changing the nature of warfare and enabling new forms of attacks. From Artificial Intelligence, to quantum technologies and autonomous capabilities, EDTs are progressively playing a critical role in the security environment, both in systemic competition and in aggravating trans-boundary security threats. China, and to a lesser extent Russia, is increasingly dedicating considerable resources to the disruptive technology domain, intensifying the efforts on illicit technology transfer and intellectual property theft. While the West has been at the forefront of R&D in innovations critical to stability and security since NATO was founded, future uncertainties demand that NATO continues to adapt so, for policymakers, the question immediately arises: "Is the NATO Alliance ahead or behind?".

Innovation in the defence industry has changed, once dominated by national defence cultures, it seems it is now ruled by non-traditional players. If adversaries gain competitive advantage in this area, states and non-state actors will have the potential to threaten our societies and the opportunity to overthrow NATO's political and military cohesion, weakening its interoperability and leading to dependencies on adversarial states. To prevent this, ambitious innovation should be reflected in the capabilities NATO asks its Allies to deliver, starting with a common understanding and approach of the major challenges the Alliance faces in this domain. The Emerging and Disruptive Technologies Roadmap endorsed by Allies in 2019, the NATO 2030 process, the NATO Innovation Board established in 2020, the

Innovation Unit within the Emerging Security Challenges Division established in 2020, and the new 'defence innovator accelerator' have all been major drivers for change in the Alliance initiative for modernisation, yet, the pace and scale of NATO's political focus on innovation must increase.

Allies do not concur on the ethical and legal considerations of the military use of EDTs and are bounded by their national-industrial preferences and national innovation initiatives. Other limitations include challenges in the pace of adoption, in engaging with NATO EDTs development initiatives, contrasts in the spending levels and technological compartmentalization, fragmented and incomplete information and skills, lack of NATO-EU cooperation, allied technology and digitalization gaps, and detachment from innovation ecosystems.

Maintaining a technological edge is the underpinning of NATO's ability to deter and defend against potential threats and it is an essential component of NATO's geopolitical signalling and consistent with its policy of competing from a position of strength. The leveraging of emerging and disruptive technologies has become crucial and NATO must re-evaluate the tools it needs to support its overarching goal of ensuring collective defence, including a new framework in which innovation drives greater adaptability, efficiency, and solidarity. Key steps to transform NATO into an innovator in its strategic environment include communication, training of its workforce, enhancing standardisation and interoperability across domains, prioritising systemic innovation targets, intensifying collaborative innovation so that no ally gets left behind and broadening and regularising NATO-EU Cooperation.

Some recommendations to successfully accomplish these goals include:

- Foster the interoperability of military capabilities that are enabled by emerging technologies and incentivise transatlantic defence cooperation on EDTs to avoid technology gaps between allies. This is one of the main challenges the Alliance faces internally. The absence of interoperability prevents the organization from engaging efficiently in EDTs projects and undertakings, and efficient information sharing.
- NATO's mission is to lead in EDTs governance and normative globally. Following a values-based

innovation strategy requires embedding democratic values into the development, adoption, and use of EDTs by the allies. Hence, innovation efforts need to be closer linked to, and based on, NATO's democracy-centred tech diplomacy with like-minded global partners, some of whom could be invited to join the Defence Innovation Accelerator.

- Develop a knowledge acceleration programme for leadership and professional staff across HQ to train and recruit talent and improve the technological proficiency of its leadership and technical workforce. Innovation acceleration is composed of different layers, which must be lined up successfully to meet the objective. Training and education cannot be overlooked since the professional staff must be

involved and confident to support innovation programs. To do this, NATO can include a mentoring or training partnership with selected tech firms with the objective of importing deeper technological know-how into the organisation.

- Expand cooperation with the private sector and academia because the future innovative mechanisms and equipment will not be home-based (NATO-based) but will be shaped and constructed by industry. This cooperation will lead in the implementation of new technologies with the objective of allowing for horizontal steering and the participation of all Allies.



Maria Bertomeu Pardo
*Joint Intelligence and Security
Division, NATO*

Maria Bertomeu Pardo is a Spanish national and graduate of a Joint degree in Economics and International Relations from the University of Aberdeen and a Master's in Development Economics and Public Policy from Universidad Autónoma de Madrid. She has always been fascinated by the research on disruptive innovation, Artificial Intelligence, outer space strategy, and hybrid and cyber warfare, which is why she focused her Bachelor's thesis on the Geopolitics of ICTs and her Master's thesis on Artificial Intelligence for Food Security in Africa, which will be presented at the end of October on the 4th Conference of AMENET, a Jean Monnet Network, co-founded by Erasmus+ Programme of the EU. Currently, she is pursuing her interest in cyber warfare interning at NATO HQ, in Brussels, in the Joint Intelligence and Security Division where she works on CIS Security and cybersecurity policy oversight

TACKLING EMERGING AND DISRUPTIVE TECHNOLOGIES THROUGH EXPANDED PUBLIC-PRIVATE ENGAGEMENT

by Christopher Coppock

NATO's transatlantic position grants it the unique opportunity to serve as a conduit for enhanced collaboration, research, and problem-solving on defense related issues. Today, this position is no more vital than in the race to understand, manage the risk, and take advantage of the opportunities posed by Emerging and Disruptive Technologies (EDTs).

EDTs represent the present and future of technologies capable of creating insecurity for the alliance. For NATO, this represents a stark shift from the strictly military threats that the alliance is accustomed to facing and creates a challenge for its typically bureaucratic and thoughtful nature. Further, the EDTs of today – the areas of focus NATO has identified are highlighted below – may not continue to be the salient EDTs of tomorrow. Taken together, the evolution of current EDTs and the potential for new technologies to arise that threaten the security of NATO members will require the alliance to increase its adaptability and flexibility to keep up with the pace of change. NATO must begin by accepting that rapid iteration and repeated failure are necessary evils, both within the alliance itself and by private partners, to stay abreast of technology developments. Beyond accepting unaccustomed levels of innovation related risk, NATO must prove its value as a multi-national coordinator of and leader in EDT solutions for the largest member states to view the alliance as a worthwhile vehicle for EDT research.

Drawing from the NATO Advisory Group on Emerging and Disruptive Technologies 2020 report, the seven EDTs that NATO intends to focus on are AI, big-data processing, quantum technologies, autonomous systems, biotechnology, hypersonic technology, and space. For an alliance whose core functionality has remained the deployment of military force to deter or counter aggression, it is not realistic to expect NATO's traditional internal resources to be able to adapt the alliance to the risks and opportunities presented by even one of these EDTs in a timely fashion, let alone all seven of them. Thankfully, NATO has recognized the need to take steps to establish new entities focused on the

exploitation of EDTs, and to expand public-private partnership.

Following the June 2021 Brussels Summit, NATO made two major EDT-related announcements. The first was the creation of the Defense Innovation Accelerator for the North Atlantic (DIANA); a body designed to coordinate cross-alliance collaboration on EDTs by member state governments, academia, and the private sector. The second is the NATO Innovation Fund, intended to identify and invest in emerging companies that are developing technologies relevant to the security of member states. At present, the Innovation Fund's initial design calls for funding on an opt-in basis from NATO members, with a target of €70 million per year. While far from the only actions the alliance is taking to position itself to manage the threats and opportunities posed by EDTs, for NATO to maintain its relevance and value for member states, the alliance must take these actions further.

Beginning with DIANA, the accelerator's most significant initial challenge will be carving out a meaningful space alongside the United States' DARPA, or Defense Advanced Research Projects Agency, particularly given that the United States has a history of jealously guarding its most advanced research findings from even its closest allies. While this attitude may be unlikely to change soon, for DIANA to provide real value to the alliance, the United States must be able to identify EDTs upon which it is willing to support transatlantic research.

The NATO innovation fund itself faces two immediate challenges: first, the willingness of member states to optionally contribute to the €70 million annual target must be closely watched. Further, states may not be incentivized to fund the program if research and product outcomes will be available to all member states, whether they have contributed or not. This uneven relationship between input and output may encourage member states to retain the money for domestic research. Accordingly, it may increase the long-term value of the fund if contributions are required – rather than optional – and are proportional to member states GDP or a similar metric. The second challenge facing the innovation fund is that €70 million is simply a small amount of money that will severely limit both the number of possible investments and the size of individual investments that the fund can make into promising startups.

There are three potential policies that the alliance can consider to build upon its already significant work related to EDTs.

1. NATO leadership should encourage national leaders to issue a joint statement at the 2022 Summit in Spain that the alliance will be a centerpiece of member states' collective research into EDTs.
2. NATO should seek to first make contributions to the Innovation Fund mandatory for all members, later to be followed by regular increases in the size of those contributions.
3. NATO should consider ways to act as a public-private partnership conductor; identifying researchers and businesses across member states whose work can build upon that of others for the benefit of the entire alliance.



Christopher Coppock
*Post-Graduate Student,
London School of Economics*

Christopher Coppock is a post-graduate student at the London School of Economics studying International Relations. Previously, he performed post-graduate study in International Security at Sciences Po in Paris and worked for four years for the AI cybersecurity firm Darktrace. His research interests lay in the intersection of cybersecurity, foreign policy, and cyber norms.

***NATO AND EMERGING TECHNOLOGIES:
STRENGTHENING DIGITAL SOVEREIGNTY
THROUGH INDUSTRIAL AUTONOMY***
by Anna Hardage

In the geopolitics of cyber, geography is no longer the primary driver – in fact, one can argue that it never truly was. The so-called fourth industrial revolution has fundamentally altered the way we live, work, and relate to one another. How war and security are conceptualized has also become considerably more abstract as these technologies transcend the traditional concepts of states and borders. Modern conflicts can be described as hybrid; “the distinction between war and peace and combatant and noncombatant [...] is becoming increasingly blurry”. New technologies are undoubtedly providing opportunities for NATO militaries to become more effective, resilient, cost-efficient and sustainable; however, they are also being applied by NATO adversaries, both state and non-state actors, and pose threats to militaries and civilians in Allied nations.

On both sides of the Atlantic, militaries, societies, economies, and information systems require increasingly advanced technologies to remain competitive, retain their advantage, and address vulnerabilities. Since 2019, NATO has worked to adopt a strategy to ensure the alliance’s edge in seven key emerging and disruptive (EDT) technologies: artificial intelligence, data and computing, autonomy, quantum-enabled technologies, biotechnology, hypersonic technology, and space.¹ The implementation thereof will require the U.S., Europe and NATO to better understand how to harness and leverage EDT to enhance collective security to improve readiness for future conflicts.

I argue that NATO must drive its EDT work through the creation of a NATO-EU apparatus and investment in technology to strengthen digital sovereignty through investment in industrial autonomy. Supporting this, Günter Koinegg, Global Head of Defense, Space and Homeland Security at Atos summarized:

“Collaboration and interaction must be by design, not by process. To innovate, there has to be an ongoing

communication loop between private sector and public sector.”

Investment in dual-use technologies must be a focus for NATO countries to be able to fight digital battlefield and implement common solutions. My first suggestion is: A new innovation investment mechanism that brings national governments together with private sector experts and academia.

It would create opportunities for increased interoperability as well as shared knowledge and capabilities both between member states as well as the member states and the private sector. Through both private and public investment, companies would be enabled to develop new and enhanced capabilities in all aforementioned EDT areas for both government and civilian use. In the creation of these solutions, however, NATO must ensure the global interoperability. This of course means US and EU, but also other global partners and potential partners should be able to partake in it.

Concretely, for the EU, this entails strengthening (investing in) national defense and tech industries throughout all EU member states to create a common standard of digital sovereignty on the EU level. There needs to be one consolidated resolution and common framework to spread capabilities, regulate the accumulation and storage of information, encourage innovation and investment in those new technologies, and reduce redundancies between sectors. What’s more, the investment strategy must include investing in innovation from non-traditional players such as academia. Including academia would bring a unique perspective to the table and encourage innovative ideas on all levels of society at a faster rate. It also serves the purpose of investing in the next generation of students and educational opportunities in member countries. From there, strategies can be more easily conceptualized to enhance standardization, communication, and interoperability across the Alliance’s concepts, doctrine, capability targets, and technical requirements related to EDT, which is a critical factor in their success.

An issue in this process is that Europe differs from the U.S. on key defense tech issues such as regulation, data, and stakes in national champion companies. A EDT strategy will require cross-cultural exchange to account for different threat perceptions within the alliance. Furthermore, any AI initiative needs to account for tech standards and ethics between members. Izabela Albrycht, Executive Board Member at DIGITALEUROPE said that hard power standards are necessary to protect from adversaries while ethical standards are primarily for soft power projection, i.e. protecting democratic values in cyberspace – and a good strategy needs to incorporate both. The US and EU will

have to be able to find common ground on contentious issues to be able to move forward.

Great power competition has taken on a strong technological dimension. NATO needs to focus on designing a framework that fosters security across all domains and enables us to automate and master technology, and ultimately create preconditions for western values. This will happen by taking risks – the ability to employ emerging and disruptive technologies more effectively than competitors will shape the global role of the United States and the transatlantic alliance in the coming decades.



Anna Hardage
Research Assistant,
Foreign Policy and Defense in
the United States Senate

Anna Hardage currently works as a Research Assistant for Foreign Policy and Defense in the United States Senate. She is also a graduate student at the University of North Carolina at Chapel Hill and Humboldt University to Berlin in the Transatlantic Master's Program where she has specialized in transatlantic affairs, especially defense issues surrounding NATO as well as trade. She has experience working in both the United States government in Washington DC and Leipzig, Germany, as well as the EU Commission in Bonn. She completed her undergraduate studies at the University of Bonn, Germany, in Political Science, Sociology and Media with a focus on international affairs and political communications.

ON MILITARY AIs by Matthias Klaus

Recent years have seen articles and books published on the idea of AI changing the nature of warfare. And the Nagorno-Karabakh conflict with its usage of loitering ammunitions like the Israeli harpy drones illustrate just how far the development of autonomous weapons has already progressed.

While leading AI philosophers like Thomas Metzinger campaign for the ban of autonomous weapons systems in the European Union, their efforts were unsuccessful thus far. As no truly autonomous weapons have yet officially been deployed could they still be stopped?

If the alliance was to follow these warnings and employ the precautionary principle, it would join China among other nations advocating for a ban of fully autonomous weapon systems. But this raises another question: What are (fully) autonomous weapon systems? China's definitions leaves loopholes, like the qualifier of "impossibility of termination", turning them effectively into fire-and-forget weapons. This peculiar interpretation clashes with the general Western understanding, and underlines the need for sharper definitions as a first necessary step.

Other experts, like Kenneth Payne of KCL, argue it is already too late to prevent the introduction of autonomous weapon systems, as their allure is too strong for governments to ignore. Instead, they should be strictly regulated across the globe, to ensure certain standards will be followed. This would entail a common understanding of what AI should or could do, resulting in common goals and limitations to be negotiated.

Whereas the use of AI-controlled vehicles to extract wounded or clear minefields is relatively uncontroversial, the situation is different for AI in active warfighting roles such as autonomous vehicles. Indeed, it commands the attention of most discussions and articles on the topic. But on the sidelines, AI is considered to enhance the military decision-making process, requiring a closer look, too.

The frequently invoked digital battlefield results in ever-growing amounts of data which need to be analysed and interpreted by the respective headquarters. Simultaneously, the increasing automatization and speed of action on the battlefield necessitate fast decisions from

higher command. This situation calls for AI to aid staff in coping with battlefield information and enable commanders to make timely and adequate decisions. For this, AI needs to work reliably at high performance, while resisting outside attacks.

However, AI could do much more than just compile and translate data, it could also aid in developing strategies and courses of action. Ultimately, this could result in scenarios where AIs plan and order attacks on military targets. This discussion differs from the well-known ethical dilemma of autonomous weapon systems with regard to the time dimension and its causality. Whereas drones strike their targets directly and immediately, AI in decision-making may advise or determine attacks on targets, which will then be conducted by other assets at a later time. Thus, the issues could rather manifest in the form of automation bias and de-skilling. It boils down to the question of responsibility for attacks and possible collateral damages and how due diligence can be enforced. Ideally, military AI in NATO states can be turned into another example of a High Reliability Organisation.

Policy Recommendations:

- a) Shared definitions, binding standards, and common procurement
 - Banning or introducing AI requires a common understanding, NATO should strive for harmonized definitions and binding regulations.
 - Past and current defence acquisitions have proven the detrimental effects on costs, delivery time and performance when projects need to accommodate many different roles and preferences. NATO should strive for common and fixed procurement processes, enabling interoperability and preventing delays.
- b) Settle on common goals and limitations
 - Different military and political cultures need to be taken into account. AI is not a neutral and independent agent, human values, concerns, and biases influence its programming. NATO needs to negotiate what AI could – and should – be able to do in warfare and assign responsibilities, while striving for a "Brussels Effect" to spread these norms.
 - The development of AI should be coordinated and led by NATO, with all member nations participating

and agreeing on the goals of the program. This ideal will face serious hurdles in the form of concerns about IP and the respective defence industries, which need to be resolved in a swift manner.

c) Design Resilience

- Standardization can result in various vulnerabilities, especially in cyberspace. When all alliance members use the same kinds of AI, potential attackers can also tailor attack vectors to these

systems. Also, potential bugs and other errors would reverberate across the alliance.

- The benefits of better cooperation and interoperability outweigh the risks of standardization. Still, NATO should endeavour to include sufficient redundancies and safety measures during the design phases.



Matthias Klaus
Former German Army Officer

Matthias Klaus is a former German army officer with over 14 years of experience in the armed forces. Currently he is transitioning into civilian life via vocational advancement services, spending most of his time on gaining more academic expertise. After having studied Business Management(M.Sc. HSU HH, 2011), International Security Studies(M.A. GCMC & Uni BW Munich, 2020), and Risk Analysis (M.Sc. KCL, 2021), he is enrolled in AI: Ethics and Society(University of Cambridge, 2023). He seeks to combine his military experience with his diverse academic background and become an expert on the risks and benefits of AI in security and defence affairs. For this end, he is looking to gain professional insights in the work of think tanks, industry, and political organisations via internships.

NATO 2030: WHAT ROLE FOR INNOVATION AND EMERGING AND DISRUPTIVE TECHNOLOGIES?

by Laura Lisboa

Political and military alliances rarely last long. 2019, however, marked the 70th anniversary of NATO. A year later, SecGen Jens Stoltenberg identified the Alliance's ability "to change every time the world has changed" as key to the most successful alliance in history. With my contribution, I aim at discussing the role innovation and emerging and disruptive technologies (EDTs) can play in NATO's quest to remain a relevant political and military alliance in 2030.

In September 2021, Stoltenberg stressed the need for NATO to be 'future-proof' by keeping up with the rapid pace of technological change, accelerating innovation to remain competitive and retaining its edge. This statement is underpinned by the recognition that the technological edge and military superiority the Alliance has enjoyed over the years cannot be taken for granted.

Although it is still early to postulate a new technologic revolution let alone to predict its implications, NATO has to take strategic decisions that encompass uncertainty and risk. In an era of unprecedented technological advancements, this implies agreeing on strategies and common standards for the adoption and adaptation to EDTs, parallel to an approach to innovation that enables the timely development and delivery of military capabilities that use them.

Why? Specifically, it will enhance NATO's military superiority: improve operational readiness, foster credible deterrence and deepen interoperability between national assets. Without meaningful military investments that translate into credible forces, NATO risks diminishing its contribution to global security and becoming obsolete. More broadly, timely address to EDTs' opportunities and threats allows the Allies to have an active role in setting the ethics and values that shape the future of technology - a concern shared with other liberal democracies.

How is NATO tackling EDTs?

NATO's Coherent Implementation Strategy on EDTs identifies seven priority areas for innovation, all highly influential for capability development: artificial intelligence (AI), data and computing, autonomy, quantum-enabled

technologies, biotechnology and human enhancements, hypersonic technologies, and space.

As a first step, AI Strategy for NATO was adopted in October 2021. It aims to accelerate AI adoption, set principles of responsible use in defence and protection against threats from malicious use¹. As for further EDT strategies, allied governments take advantage in acting collectively through NATO: it ensures a focus on interoperability and the development of common standards.

Likewise, leaders from 17 European Allies laid the first stone for NATO Innovation Fund, designed to facilitate investment in promising dual-use technologies. The Fund is aligned with the agreed launch of DIANA, a new civil-military Defence Innovation Accelerator for the North Atlantic, expected to advance technological cooperation, promote interoperability and boost innovation through early engagement with academia, end-users and the private sector. As it is still early to assess its potential impact, we may rather hitherto argue it sets an initial vision for NATO's future approach to innovation. To contribute to this debate, I outline policy recommendations that can be implemented through the recently created mechanisms.

NATO's approach to Innovation

In times of growing strategic competition, NATO has to take advantage of its unique diverse nature to improve efficiency in timely delivering cutting-edge capabilities. This involves leveraging the development of EDTs through the strengthening of ties among Allies' world-class institutions and businesses. For this, the Alliance should:

1. Create an Alliance-wide network of eminent universities and research centres to increase multinational and complementary research on the development of dual-use EDTs. The age of 'Silicone Valleys' is over. Large, centralised innovation hubs will likely be replaced by broad, decentralised and deeply interconnected networks of centres of excellence. NATO is well-positioned to take the lead in such endeavour, with the potential to drive major benefits for societies, defence sectors and the Alliance, enhancing its relevance. In addition, this engagement may as well counter some reluctance of younger generations in engaging with the security and defence sectors.

2. Develop incentives for cutting-edge dual-use tech start-ups to flourish and thrive. Start-ups mirror the ability democratic societies have, to consistently deliver high levels of creativity and innovation - an advantage Allies enjoy over their main competitors. Moreover, speed is start-ups' key advantage, which gives them a sense of urgency often lost in defence departments. Innovation tends to slow in the absence of a perception of a pressing need to adapt, like a major conflict. Start-ups can thus play a meaningful role in speeding innovation in times of peace. Long and complex acquisition processes, however, often deter them from contracting with the public sector. To deepen its engagement with tech start-ups, NATO has to create conditions to accommodate their dynamics: facilitate timely investment and increase risk tolerance among Allies, build alternatives to long and complex acquisition processes, and ensure they have real chances of winning contracts over incumbents.
3. To agile the adoption of EDTs, NATO should direct its investments wisely towards the identified priority areas, favouring a piecemeal approach: start small, pursue investments pioneered by single or few nations for the adoption of dual-use EDTs that, when ready and showcasing success, can be scaled. To

- scale at speed, the Alliance may consider multi-national investments, involving governments and industries, but may as well assess the advantages and risks of partnerships with big private companies.
4. To be 'future-proof', NATO has to retain its information advantage and ensure that accurate information moves rapidly to those who decide and act on it. As so, initiatives developed in recent years within the Alliance do not focus merely on modernising old capabilities, but target technologies with the potential for redefining how NATO collects and shares information. In the near future, the Alliance should prioritise the exploitation of 'system of systems' approaches; assess the potential for cloud computing to enhance efficiency, interoperability and the secure transfer of information across Allies; and invest in quantum sensors, which offer unprecedented improvements in measurement and detection technologies and thus promising military applications.

Decisions taken now in respect to innovation and EDTs will play a significant role in taking a stronger and fitter Alliance into the next decade. It is about time to lay the groundwork for a transatlantic approach to these matters: for Allies to recognise its benefits and for citizens to engage in debate on NATO's future.



Laura Lisboa
Intern, Defence Investment
Division, NATO

Laura Lisboa is currently interning at the Defence Investment Division at NATO HQ. She holds a Masters in Politics and International Relations from the Catholic University of Portugal, where she worked as a Research Assistant and Grader for a course on Geopolitics and Geostrategy. After earning a degree in Engineering Physics from Instituto Superior Técnico, she decided to study social sciences to follow a career path that could have a more direct socio-political impact. Over the last years, she participated in seminars and exchanges in the United States, Japan, England, Germany and Portugal.

NATO'S RESPONSE TO THE QUANTUM COMPUTING CYBERTHREAT

by Lucas Moers

NATO is anticipating the next decades of military threat potential with its strategy on emerging and disruptive threats (EDTs). A specific feature of threat development is the transition from the physical domains to cyberspace, with the accompanying potential to combine domains in conflict operations and, thence, affect all aspects of the military, societal and individual spectrum. One of these developments is the quantum computer based on quantum physics rather than standard electronics. The current estimation is that this technology will reach maturity before 2030. This maturity entails that quantum computers are sufficiently stable and robust with error correction – i.e., with enough qubits – so that they can work with large numbers to break classic factorization encryption. Hence, NATO can expect that the current computing infrastructure will not meet the demands of a quantum computing environment. This essay first highlights the quantum computer threat and, accordingly, formulates specific NATO policy recommendations.

Quantum computing cyberthreat

As NATO societies have transitioned to an economy essentially run by digitally encrypted dataflows, the proper protection through encryption is vital and, therefore, society at large is severely threatened by quantum computing advancements. Quantum computers are unique as they use quantum bits that can be in multiple states at once instead of the classic computer's binary 1/0 structure. This means they can tackle an immense number of outcomes, resulting in greater computational abilities and opportunities. Aside from the scientific possibilities, quantum computers have the potential to break currently used cryptographic encryption tools. Up to this stage, modern cybersecurity systems are mostly based in a paradigm known as asymmetric, or public key, encryption; albeit some systems, such as bulk data transfers, continue to use symmetric encryption. Modern encryption attributes its success to the computational complexity associated with the factorization of large prime numbers, which represents a significant challenge to

modern classical computers. Yet quantum computers programmed with Shor's algorithm achieve a decryption computation in a fraction of the time. For instance, Google's Sycamore quantum processor performed a calculation in 200 seconds which takes a state-of-the-art supercomputer 10,000 years. Therefore, the development of quantum computing has severe implications for every IT-based application that relies on encryption, ranging from bank transactions to air traffic control to the chips in every digital device. Here, three distinct problems are discussed as the result of quantum computer advancements.

First, asymmetrical cryptography includes two issues, the first being its application in digital signatures. By applying quantum computers' computing power, systems become vulnerable to digital signature-falsification. Therefore, actors can exploit trusted relationships by impersonating validated entities, allowing information extraction because users speak freely as they expect to talk to a validated entity. However, this is a minor concern as the breaking of authentication is often timed or involves two-factor authentication and, therefore, less vulnerable.

Second, the main problem is with exchanging cryptographic keys through asymmetrical cryptography, as decrypted keys lead to symmetrically encrypted bulk data. Currently, intelligence agencies both in and out of NATO extract as much encrypted data as possible, which is stored until quantum computing is ready to break the encryption, whereafter this data is analyzed. Hence, retroactively, secrets of intelligence communities and alliances like NATO will be acquired and revealed.

Third, symmetric encryption also faces issues due to quantum's decryption capabilities as messages and systems are relatively easily and rapidly decrypted with quantum computing's Grover algorithm. However, this exposure can be countered by doubling passwords and encryption keys. Though this might seem an easy solution, this includes keys on hardware chips ranging from mobile phones, servers, and internet of things devices – i.e., the transformation requires investment of time and resources for both private and public actors.

NATO policy recommendations

Quantum computing's cyberthreat to NATO is, fortunately, not without solution. Accordingly, NATO needs coherent and coordinated action based on the defined security investments and strategies as rooted in the following policy recommendations:

- Direct investments are required for quantum-enabled solutions, including quantum cryptographic systems for trust in certificate authorities, digital signatures, and encrypted information.
- Quantum computing requires strategies need to:
 - Establish a crisis management strategy describing how to deal with quantum computing's innovations and uses below the level of declared war – e.g., Russian intimidation tactics.
 - Encourage public investment and innovation in EDTs as quantum technologies are being predominantly developed in the private sector, which leads to a private sector dependency with regards to military innovation.
 - Increase transparency to support technologically less developed NATO-countries, which are particularly vulnerable to EDT developments.

Finally, cryptography is just one piece of a much larger cybersecurity pie. For example, using the best encryption still allow one to interact with malicious URLs or files attached to an email. Similarly, encryption cannot defend against inevitable software flaws and exploitation, or insiders who misuse their access. However, when powerful quantum computing arrives, it poses a considerable security threat to encrypted dataflows. Because adopting new standards takes years, it is strongly advised to begin planning for a quantum-resistant NATO now.



Lucas Moers
Master Student in Crisis and
Security Management with a
specialization in Cyber Security
Governance, Leiden University

Lucas Moers is from the Atlantic Youth in the Netherlands. Currently, he studies a Master's degree in Crisis and Security Management with a specialization in Cyber Security Governance at Leiden University. He lives in the Hague, the international city of peace, and during many walks, talks, and books, he got inspired to do something in the field of security. He has a passion for cybersecurity and diplomacy. Therefore, in the long term it is his ambition to combine these two passions at the Ministry of Foreign Affairs.

NATO'S MISSING NORM CONVERGENCE: SETTING THE ATLANTIC SAIL FOR FUTURE CONFLICT

by Celia Schiller

Emerging and disruptive technologies (EDT) in the NATO alliance have taken a high stance with the document labeled "Foster and Protect: NATO's Coherent Implementation Strategy on Emerging and Disruptive Technologies" with the NATO Advisory Group on Emerging and Disruptive Technologies, with the NATO 2030 strategy, the NATO Innovation Board. However, the structure and aspiration towards norm convergence seems uncoordinated and moderate in its dimension. Some changes have been "long overdue". Taking on the stance of effective policy by focusing on a core issue at the intersection of politics and military means would be leading the alliance into better coordination and cooperation as there is no past threat legitimatizing a greater coherence within the alliance as the Second World War did prior to the foundation of NATO. Therefore, I argue that the stance within NATO on EDTs is a prime example of a slower process in the development and strengthening of NATO within today's military realm and point to the determination of systems of systems cooperation in order to overcome this problem and link the politics and military means of the alliance's members to boost NATO's effectiveness overall. Thereby, the historic restraint of uniting behind a common threat could be overcome by uniting behind a norm convergence.

Identifying A Focus: Systems Of Systems

A main point of future development concerning EDTs is the development of dual-use technologies. Dual-use technologies can be employed in a civilian as well as military realm and immensely relate to data exchange when it comes to the mentioning of AI. Hence, it contributes to the link of politics and the military means of the alliance's members to boost NATO's effectiveness overall. Thereby, the historic restraint of uniting behind a common threat could be overcome by uniting behind a norm convergence. One prime example of such a dual-use technology that hasn't been well known above the scope of the FCAS military system are systems of systems (SoS). Therefore, I take a look at SoS to emphasize the norm convergence that SoS bring about.

Systems of systems are designed to tackle the "evolving nature" of independent systems. The independent systems or constituent systems (CS) are dedicated a

specific nature or task and would, for the creation of a SoS, be merged, so that a greater system would be established, that is, thereby, more flexible. This flexibility of the SoS would also potentially assure a better response to hybrid threats against NATO in comparison to systems that remain national. SoS have a degree of "emergent behavior", meaning that a common behavior is created by the merging of the CS which could not be achieved by one solemn actor. Therefore, a SoS should be mutually developed with companies from the U.S and the EU, in order to set the sail within an Atlantic perspective, to check and balance different approaches considering a wide area of norms applicable to AI.

POLICY RECOMMENDATIONS

1. Merging SoS

It is important in order to face new challenges and create unity among NATO allies and the EU that has to be a strong partner concerning the exchange of norms "to consolidate the transatlantic alliance for an era of strategic simultaneity".

2. Talk about data

The legal burden appears to be the biggest one when it comes to norm convergence to bring about dual-use technology. Initially, it is because of the fact that the U.S. legal system does not hold the same standards for data protection as the EU which would have to be tackled with new regulations in the U.S. system. This could be a tedious process as such a law would have to initiate a change in the USA Freedom Act. Therefore, I recommend the implementation of a SoS that, with its building, defines a combination of European and U.S. norms and SCCs. The data would be handled within the joint system which could also be the ground for a new policy on both sides concerning the handling of personal data by foreign individuals within a system of systems. Before implementing this legal merge, it should be ensured that even the construction of this system is a bilateral engagement. Therefore, SoS R&D should be widened.

3. SoS R&D

Deriving out of the first recommendation, a second recommendation would be the enhancement of SoS R&D. Until now, on both sides of the Atlantic, different research projects in the field of SoSE have been established, which shows the interest and necessity of R&D in the realm of SoS.

4. Public-Private Partnerships

Such a project, that aims at improving norm convergence within NATO cannot be exercised without the consolidation and incorporation of private entities which relates to the underlying idea of dual-use technology. In the sense of norm convergence, if systems are to be linked, a structure of systems of systems will evolve and

connect networks with each other. Dr. Sandro Gaycken from the Digital Society Institute at ESMT Berlin pledges for disconnecting networks in order to assure cybersecurity. Thereby, new structures would evolve and hence contribute to the better integration of private entities that are actors within cyberspace as well.



Celia Schiller
M.A. International Affairs &
International Security Candidate,
Hertie School

Celia Schiller graduated from Jacobs University in Bremen with a Bachelor of Arts in International Relations after finishing her secondary education as a German national in the United States. She developed a keen interest for security studies, transatlantic issues, counterterrorism and cybersecurity during her undergraduate studies and practically applied those interests with an internship at the Federal Academy for Security Policy in Berlin and at the U.S. Consulate General in Hamburg. Currently, she is a Business Intelligence Trainee at Rheinmetall Defence and simultaneously pursues a Master of International Affairs & International Security at the Hertie School in Berlin.

ETHICS OF EMERGING AND DISRUPTIVE TECHNOLOGIES

by Selin Yılmaz

The world has entered into a new stage, emerging and disruptive technologies (EDT) appear in all aspects of daily life; paying your shopping with your credit card, having an online meeting with customers, submitting an application for work through LinkedIn. Not only in daily life but EDT also finds a significant spot in the defense and military field by providing an opportunity for sustainability, efficiency, and a higher level of protection. Even though EDT eases our lives and provides a stronger security, ethics of EDT has become a controversial topic for policymakers, organizations such as NATO and European Union (EU) as well as the academy.

Achievability of the Purpose must be Taken Into Consideration For An Ethical Usage.

According to European Defense Agency, ED Technologies; artificial intelligence, big data, quantum technology, robotics, autonomous systems, new advanced materials, blockchain, hypersonic weapons systems, and biotechnologies applied to human enhancements - to name only them - are expected to have a disruptive impact on defense and revolutionize future military capabilities, strategy, and operations. Can a technology with disruptive effects be ethical? This question must be answered as depends. From my perspective, the purpose and achievability of the said purpose must change the answer, as it is in law. Especially in the defense industry and military field this achievability plays a more essential role as it is directly or indirectly about human rights of both sides.

Emerging and Disruptive Technologies must not be used until Perfection of the Technology per the Current Ethical Understanding apart from Urgent Requirements.

Robert Baker, William D. Williams Professor of Philosophy Emeritus at Union College and Professor of Bioethics and Founding Director (Emeritus) of the Clarkson University-Icahn-Mount Sinai Bioethics program, defines morally disruptive technological innovations as those which “undermine established moral norms or ethical codes”. From my perspective, this definition implies new forms of ethics shall be set and

apply to innovative EDT because it is very likely that EDT undermines current and settled norms.

ED technologies are often used by states, non-state actors, and others actively and appear with unpredictable consequences. For example, Kargu-2, an armed unmanned aerial vehicle produced in and by Turkey is an armed, autonomous artificial intelligence mentioned in United Nations Report. Accordingly, Kargu-2 went after logistic transportations, meaning civilians because autonomous drones sometimes struggle to differentiate a tree and a human body and cause serious harm because they are yet to be produced with perfect technics for it. Turkey contradicted the said news, however, this does not change the possibility. Additionally, there is a strong ethical problem arising from the usage of EDT against troops withdrawn. Those troops may also be trying to surrender or be hurt. Those troops are untouchable according to the Geneva Convention. However, it is unknown if autonomous systems are capable of deterring this kind of situation. If the answer is negative, must the owner country be accepted as a breach of the Geneva Convention? My answer is yes, because, until the technology is perfect those technological tools must not be used in the field. However, this strict necessity is not realistic in today's technologic world. Thus, urgent requirements must be accepted as exceptions for security field.

Producing and User Countries must Share the Burden.

ED technologies are just mechanical. Can you expect an ethical approach from a mechanical? You cannot expect the tool to understand and act in pursuit of the ethics of policymakers. What happens if those mechanics cause death is still unknown. When there is not such a remote control behind a technological tool that is controlled by a person or a group of people, who will be responsible? If the death is by a mistake or technical problem, will the answer to the question change? Those questions must be answered before 2030 because their active usage may create irreversible mistake any minute. My personal view is that producing country and user country must share the burden. Also, Emerging and disruptive technologies in defense must be used after approval by NATO in member and partner countries to act per common ethics.

To sum up, important to realize that it is not possible for states, NATO, and the EU not to be a part of the improvement of the EDT. This is the reality of this century and getting more important each day; countries earn billions from this business. Significantly, these actors must create a framework by taking already existing ethics and morals, before 2030. Because those autonomous technologies are used in operations actively and open for

a technical problems anytime. If these actors be late for an ethical response this situation may create irreversible consequences harming the current morals. Thus, we must be aware of what kind of technical or field problems EDT may create and be ready to take action in such a scenario or to set a rule of usage by a remote control that is controlled by a human. For taking the situation into control, a framework must be worked on immediately.



Selin Yilmaz
President,
YATA Turkey

Selin Yilmaz has graduated from Yeditepe University Law Faculty on 2018. She studied at Amsterdam School of Law for a semester under Erasmus Exchange Program. During her studies, she gained national and international certificates varying from Information Technology Law, International Humanitarian Law, European Union Law, etc. She has become a member of Young Atlantic Treaty Association of Turkey in December 2017. In February 2018, she got elected as Vice President for Public Diplomacy of YATA Turkey as the only female member of the Board. On June 2020, she got elected anonymously by the Board as the President of YATA Turkey. She has volunteered in different organizations including Diversity House of Protestant Church in Amsterdam, Hope Foundation for Children with Cancer, etc. She has also been a part of Atlantic Treaty Association's Women, Peace and Security Task Force. She is a lawyer who established her own law firm in Istanbul, Turkey and the President of Yata Turkey.

PAN | NATO's European Pillar: Shape, Size, EL 2 | Function?



© Photo by Guillaume Périgois on Unsplash

Realizing that pre-Trump times in terms of military cooperation are not coming back and the idea of a European army doesn't appear too realistic in the near future, European politicians repeatedly emphasize the importance of strengthening NATO's European pillar.

In this workshop, we want to take a closer look at the conceptional idea behind the pillar metaphor, not only to add description to the problem but to make specific recommendations to the alliance as to how the concept could be brought to life: what are the functions a European pillar has to fulfill and what are its geographic limits? What resources are required and who will provide them? And how can European integration be fostered without driving the partners on both sides of the Atlantic further apart?

PANELISTS



Hugo Meijer,
CNRS Research Fellow, Center
for International Studies,
Sciences Po

Hugo Meijer is CNRS Research Fellow at Sciences Po, Center for International Studies (CERI). He is also the Founding Director of the European Initiative for Security Studies (EISS). His research interests lie at the intersection of foreign policy analysis and security studies. Currently, his research focuses on the reconfiguration of US hegemony in the face of a rising China and on its implications for American alliances in Europe and Asia as well as on European foreign and security policies toward China. Previously, he was Marie Skłodowska-Curie Fellow at the European University Institute (EUI, Florence), Lecturer in Defence Studies at King's College London and a Researcher at the Institute for Strategic Research (IRSEM, Paris).



Jan Fuhrmann
Security and Risk Consultant,
Secori Advisors

During the last legislative period, Jan Fuhrmann was a Parliamentary Advisor to Dr. Andreas Nick MdB (CDU/CSU), a Member of the Bundestag Committee on Foreign Affairs and Head of the German delegation to the Parliamentary Assembly of the Council of Europe. As a Parliamentary Advisor, he covered a broad range of issues related to foreign- and security policy. Mr. Fuhrmann's other professional experiences include, inter alia, the KfW Development Bank and the NATO Allied Command Transformation (ACT). He recently joined Secori Advisors, a boutique consultancy for cyber and information security, as Security and Risk Consultant.

Mr. Fuhrmann is also a member of the Young Foreign Policy Experts Working Group of the Konrad Adenauer Foundation. He holds a bachelor's degree in political science and sociology as well as a master's degree in political science from the Goethe University in Frankfurt am Main.



Eric Povel
Program Officer , Engagements
Section, Public Diplomacy
Division, NATO

Eric Povel has worked in the Hague and Brussels as lobby consultant for numerous public affairs consultancies, companies, NGO's and governmental bodies. In 1995, he was employed as the Netherlands Information Officer in the Public Diplomacy Division (PDD) at NATO HQ in Brussels. During NATO's enlargement process in the late 90s, he was also responsible for NATO information activities in new and candidate member states. 2006, he started working in the NATO Press and Media Section as a press officer to set up the Media Operations Centre (MOC) dealing with Afghanistan. As of July 2011, Povel was the Strategic Communications Coordinator, heading the PDD StratCom Cell in support of the Assistant Secretary General for Public Diplomacy, responsible for all operational and doctrinal StratCom issues at NATO HQ. Since 2012, he is Program Officer in the Engagements Section of PDD dealing with Afghanistan. He also holds country responsibility for Belgium, Estonia, Germany, Latvia, Lithuania, and the Netherlands.

CHAIRS



Peer Klaus Braak
Graduate Student of
International Security,
Sciences Po Paris

Currently, Peer is pursuing a Master's Degree at Sciences Po Paris in International Security. Besides his interest in transatlantic cooperation, he is focusing on the recent security developments of the Indo-Pacific region. His previous professional experiences include, inter alia, the German Embassy in Washington DC, the Training for International Diplomats by the German Federal Foreign Office as well as the In-house consultancy of the German Federal Armed Forces (BwConsulting). He joined YATA after he participated in the NATO's Future Seminar 2019. He remains a Transatlanticist at heart ever since having spent a year in the United States as a CBYX-Fellow.



Sofie Flurschütz
Graduate Student of
European Studies,
Fulda University of Applied
Sciences

Sofie Flurschütz is currently pursuing a Master's Degree in Intercultural Communication and European Studies at the Fulda University of Applied Sciences and scholarship holder of the Hanns Seidel Foundation. She holds a Bachelor's Degree in Journalism from the Ansbach University of Applied Sciences. During her studies she spent time in Austria, France and India. She is passionate about writing and has more than 7 years of experience in journalism, communications and social media. Sofie has participated and worked at conferences such as the Model United Nations Conference (2019), the Munich Security Conference (2019) and the Youth Forum for Security Policy (2021). Her latest work experiences are connected to the Second German Television (ZDF) and the Federal Press Office, supporting the Foreign, Security, and Development Policy Unit. Sofie attended the NATO's Future Seminar in 2020. For her, it was an amazing opportunity to improve her knowledge on climate security, policy-making and strategic thinking.



Tilman Rami
Graduate Student of
International Security,
Sciences Po Paris

Tilman studies as junior student STEM-teaching at the Rheinische-Friedrichs-Wilhelms University of Bonn and is about to graduate from grammar school next summer. For his research paper on Wirecard, he won the prestigious "Facharbeitspreis" in his hometown. Due to his work in the task force "Europe & international affairs" of Europe's largest political youth organization he is familiar with couple of unsolved problems. As intern Tilman gained experience in the informell economy not only at an international audit company but also at the regional headquarter of Deutsche Bank. Besides that he is coaching his own soccer team since 2017 and leads several projects like stock market simulations for schools, a poetryslam and a new podcast on politics starting in 2022.

**NATO FOR THE XXI CENTURY: EUROPEAN OWNERSHIP OF ITS OWN SECURITY IS BOTH
POSSIBLE AND URGENT**
by Alberto Cunha

Can we have an “European Pillar” that serves the interest of all NATO members? My main argument is that NATO does not need to create new institutions for an effective contribution of European for their own defence, but rather we need to make the existing structures work much more effectively – and this will only happen once there are clearly defined roles and responsibilities.

In addition, there is in my opinion a major problem with the on-going political discourse and negotiations regarding European “Autonomy” (be it the rather utopic “European Army” or the NATO-led process of the “European Pillar”). These issues are not new: arguably, they stem from a discussion originated in the 1990s from both Europe, namely France, but also in Washington. In fact, long before Mr. Trump was President, there were already concerns about European “burden-sharing” and that Europeans could develop their defence without detaching from NATO - which led to the famous “no 3-D’s” formulation by the Clinton administration.

My proposal seeks to allow for a real ownership by European member-states of their defence, which in my opinion should be done by a combination of political control by the EU with a Permanent Transatlantic Coordination mechanism. It would mean less ambiguity on the respective roles of NATO and CSDP by avoiding potential duplication of efforts by the EU, while ensuring permanent effective Transatlantic Coordination.

Permanent Political Coordination mechanism as an embryo for a European Security Council

I propose that the NATO European Pillar is organized by the EU and consist of the Common Security and Defence Policy (CSDP) structures. Efforts such as PESCO and would thus be under a clear EU political direction but would be reported to other NATO member-states and thus would not duplicate/detract from NATO’s own initiatives, such as “NATO framework nations”.

It is for the latter purpose that I propose that a Permanent Political Coordination mechanism exists between the CSDP and NATO, with a deciding role on

where to allocate the already existing pan-European resources more efficiently between the Transatlantic Alliance different priorities. It does not need to be a new structure, but rather an informal communication mechanism between representatives from the Defence Ministries and Armed Forces for NATO member-state represented.

I propose this as a mechanism which could meet, if necessary, in an urgent fashion, and co-headed by the EU Council President (for a swift coordination with EU heads of Government) and the NATO Secretary-general. This council shall meet every six months and in a “crisis meeting configuration” whenever convened by the co-heads.

The proposal is for the present but could also be the beginning of a new future for NATO. The mechanism could be the embryo for a future permanent European Security Council, and as such, apart from the most relevant military leaders from NATO and EU (namely the Supreme Allied Commander and Director General of the EU Military Staff), the following states should have permanent representation:

- France, Italy, Germany, Spain, Poland as members of NATO and EU;
- US, UK, Canada, Turkey as members of NATO;
- EU High Representative in the name of the Commission and thus remaining EU members; with a rotation for the other states of NATO/EU, on a similar model to the UN Security Council.

Towards an effective sharing of duties between the EU and non-EU NATO members

Because it is my firm opinion this mechanism could help address three main concerns regarding the current state of NATO-EU relationship:

- a) The concern, by the US and indeed many EU countries (certainly the eastern-most members, rightly concerned about Russia), that the development of the EU defence capabilities might lead to a duplication of military capabilities that would not complement but rather serve as an hinderance to NATO efforts in addressing the perceived security needs of EU members.

This council would provide clear demarcation of tasks/resources between NATO and the CSDP in a permanent forum for discussions that would take place behind closed doors and without needless “public spats” regarding the future of NATO and the “European

Army” (the latter of which have happened unfortunately all too often in recent years).

- b) The concern by several EU members that the “burden-sharing” increasingly demanded by the US and NATO itself, might hamper the integrated development of the European defence industry and/or lead to a greater strategic dependence on the US. This worry was an important motivation for the declared establishment of the EU Commission DG for Defence Industry and Space, and had been clearly stated, for instance, by France in their “Livre Blanc” of 2013. With this permanent forum of communication, EU members could more clearly transmit to NATO partners, and namely the US, how important for them is the linkage between “sharing the burden” with Washington and the possibility to develop a more concrete strategic autonomy for the EU. As this Permanent Political Coordination mechanism

could reaffirm, this does not mean the desire to see NATO or the US abandon Europe, which would be harmful to all parties concerned.

- c) The concern about the slow progress made in the EU’s CSDP reveals the little existing appetite in Europe for any “European Army” that would eventually replace NATO as the security guarantor of Europe.

Thus, the need is present for a much more effective political coordination between the EU and NATO structures that advances a European Defence that ‘leaves the paper’ and serves European security in a feasible and realistic way. It is in this context that my proposal for the creation of a Permanent Political Coordination mechanism between the CSDP and NATO is necessary and indeed urgent, given recent political developments such as: Brexit, the unilateral US withdrawal from Afghanistan (however justified militarily, Washington’s lack of communication with NATO members was widely resented in European capitals) and a growing element of isolationism to US foreign policy amplified under the presidency of Mr. Trump.



Alberto Cunha
PhD candidate in European Studies and teaching assistant in the Department of European and International Studies at King's College London

Alberto Cunha is a PhD candidate in European Studies and a teaching assistant in the Department of European and International Studies at King's College London - where he is also a member of two research/expert networks: Centre for German Transnational Relations and The European Foreign Policy Research Group. He is the author of two peer-reviewed articles published in an IR journal and three others in online publications: "A Alemanha de Merkel durante e após a crise do Euro: hegemonia relutante?" (2021, to be published in the next issue of R:I) "Europe's Hegemon? The Nature of German Power During Europe's Crisis Decade" (2021, in E-International Relations); "Post-Brexit EU Defence Policy: Is Germany leading towards an EU Army?" (2020, in E-International Relations) ; "Compreender os nacionalismos na Europa do pós-Guerra Fria" (2019, in R:I n.º 62 Junho); "Paving the New Silk Road: The Evolution of the Sino-German Strategic Partnership" (2017, in Observatório Político).

Prior to his PhD, he worked at two Portuguese embassies, and is now also the Academic Director at the nascent think-tank EuropaNova Germany.

A BERLIN-PLUS 'IN REVERSE'?

by Christopher Devenish

Last September, the almost two-decade long NATO mission(s) in Afghanistan came to an end. During this campaign, an organization designed to ensure the territorial defense of Western Europe against a conventional military force found itself involved in a conflict which combined elements of counterterrorism and counter-insurgency operations, development and capacity-building projects, and efforts at improving governance and human rights in central Asia. Clearly, the complexity of contemporary security challenges requires NATO to expand its definition of security. This requirement, in turn, opens opportunities for a European Pillar to provide valuable support to the Alliance.

Cooperation between NATO and the European Union (EU) has been ongoing since the creation of the EU's European Security and Defense Policy (ESDP, now CSDP). This cooperation was heightened in 2003 when, following years of discussion over a European Security and Defense Identity (ESDI) within the Alliance, leaders from the EU and NATO signed on to the Berlin Plus agreement. Created both to address concerns about maintaining NATO's relevancy amid the EU's developing ESDP and to avoid competing over scarce resources, the agreement gave the EU the ability to access NATO assets and capabilities when NATO had decided it would not act and when NATO members unanimously agreed to offer their support.

Immediately following its implementation, Berlin Plus became a key element of NATO-EU cooperation and was used to launch multiple EU-led missions in the Western Balkans. Both organizations have since realized the significant benefits that cooperation brings and have repeatedly emphasized their commitment to continuing and enhancing it (See the 2010 Strategic Concept and the 2018 Joint Declaration on EU-NATO cooperation). Creating a Berlin Plus 'in reverse' could have just this effect.

A 'reversal' would involve allowing NATO to access EU civilian CSDP capabilities for NATO missions under similar conditions to the original Berlin Plus agreement, i.e., a decision by the EU not to engage and unanimous agreement to support cooperation. Of course, the term 'in reverse' is not entirely accurate. For one, under Berlin Plus, NATO retains a strong degree of control over assets it lends to the EU; it is unlikely that NATO would support a reciprocal EU influence over capabilities that are lent to it. Nonetheless, NATO should seek mutual access to

certain EU capabilities. This would give any potential European Pillar a vital role and would provide NATO with resources that would allow the organization to better address modern security challenges.

This proposal is not entirely without precedent. The past several years have seen NATO military and EU civilian missions cooperating towards similar ends in campaigns in Afghanistan and, more indirectly, in Iraq and off the coast of Somalia. However, honing and formalizing this cooperation would: 1) Enhance mission coherence, 2) Enable NATO to access important capabilities while avoiding redundancy and duplication with the EU (original goals of the Berlin Plus agreement), and 3) Enable the two organizations to enhance their complementarity.

- (1) while current efforts at bilateral collaboration are intense, NATO and CSDP operations are nonetheless created and implemented by separate bodies with different political and strategic priorities. Strategic differences between NATO and the EU, though likely small, will inevitably feed into the tactical and operational decisions taken by their respective field units creating the potential for incoherence at all levels. Creating a mechanism to bring civilian CSDP capabilities and assets under, or at least closer to, NATO command structures would help to mitigate this, thereby improving the overall coherence of EU and NATO engagement.
- (2) modern conflicts interact with and are heavily influenced by civilian populations. Therefore, engagement with these populations is critical to the success of an operation. NATO, while primarily a military actor, has made significant steps in developing capabilities and methods to address these issues. Its Provincial Reconstruction Teams (PRTs) operated under the International Security and Assistance Force (ISAF) in Afghanistan and attempted to address the link between development and security issues. More recently, NATO's Counter-Hybrid Support Teams - made of both military and civilian experts - assist and advise NATO countries in improving their resilience and their responsiveness to hybrid threats. However, too much emphasis on developing civilian capabilities risks diverting resources away from NATO's primary focus on the territorial defense of its members. It further risks recreating capabilities that the EU has already developed. Granting NATO access to EU capabilities would

allow a European Pillar within NATO to contribute assets and capabilities in which it holds a comparative advantage.

- (3) the EU and NATO tend to share similar security perspectives and often mutually reinforce one another. This is not too surprising given the considerable overlap in membership. However, while the six non-NATO members of the EU are covered by an implicit security guarantee, Canada and the United States have rarely benefited from specific EU civilian capabilities. Allowing NATO to access civilian CSDP capabilities would thus improve the complementarity of the two organizations.

There are no doubt barriers to implementation, some related to the organization's different memberships. However, EU and NATO leaders have an opportunity to reaffirm their commitment to one another and to better align their approaches in the upcoming discussions on the Union's Strategic Compass and the Alliance's Strategic Concept. Committing – in their respective statements – to exploring the possible contours of a Berlin Plus 'in reverse' would help both organizations to demonstrate the vital support that a European Pillar could offer NATO.



Christopher Devenish
Graduate Student of
International Relations/
International Security,
London School of Economics/
Sciences Po Paris

Christopher Devenish is currently completing a Master of Science (MSc) in International Relations at the London School of Economics and a Master of Arts (MA) in International Security through Sciences Po. He specializes in European defense and security, transatlantic security relations, and intelligence studies. He is a fellow in the Irish Department of Foreign Affairs' Iveagh Fellowship and an alumnus of University College Dublin's Ad Astra Academy. Prior to his academic career, Christopher served for four years in the United States Marine Corps in various leadership roles and completed two deployments overseas.

INVESTING IN EU DEFENSE AND GALVANIZING U.S. SUPPORT

by Camille Ford

A European pillar for NATO should be premised on concrete capability developments by the EU and European partners in areas that are complementary to NATO, while permitting in the longer-term for the EU to meet its own strategic ends in times of divergence among NATO allies. However, considering the disparate levels of political will across most EU Member States (EUMS) and certain European NATO partners for the necessary investment to acquire such capabilities, the most viable path for the development of a robust European defense and security apparatus must be within the context of NATO. Of course, European defense does not equal EU defense, but the EU can serve as central infrastructure by which European defense capabilities improve by focusing on the contributions that can be made by the EUMS. Thus, the EU, despite not speaking for Europe as a whole, is a key starting point to building a European pillar for NATO. In effect, NATO should be the link that allows for the EUMS and non-EUMS to create a European defense.

As such, conceiving of a European pillar for NATO begins with addressing the obstacles which currently constrain the development of EU defense: an EU-wide lack of capabilities and defense integration, and disparate strategic priorities among EUMS. Over 20 years after the launch of the Common Security and Defense Policy (CSDP), the EU lacks the key capabilities to conduct military operations autonomously across the whole spectrum of the use of force. The EU has shown, through the military and civilian elements of CSDP and Frontex, that it has the capacity to take on missions abroad. However, CSDP and Frontex distinctly serve as expeditionary military missions that support the EU's foreign policy agenda. The EU does not provide for the collective security and defense of the EUMS or the European continent – only NATO does. With 22 states being members of both the EU and NATO, the institutions share values and face similar security threats such as Russia, cyberthreats or instability in the Southern region. Inevitably, a *de facto* division of labor has occurred among the institutions but, at present, this divide has been overly emphasized by the EU's limited capabilities and its role as a largely

civilian, threat-management actor, rather than a security and defense actor.

With the creation of the EU's Permanent Structured Cooperation (PESCO) and European Defense Fund (EDF), alongside the Capability Development Plan (CDP) and Coordinated Annual Review on Defense (CARD), the EU now has novel means to fund defense investments and develop high-end defense capabilities beyond crisis response. EUMS should leverage their existing comparative advantage in EU home affairs and internal security to solidify the EU's claim to greater security and defense capacity. In particular, the EU should assume more responsibility in its southern and eastern neighborhoods. And once capabilities are solidified at the neighborhood-level, EUMS can increase operational readiness for more extensive expeditionary missions that are at the higher-end of the use-of-force spectrum.

The U.S. perception of European strategic autonomy in the realms of security and defense has cast a long shadow on recent efforts to bolster the EU's defense capabilities. To overcome ambiguity, the EU and its European partners should directly involve the U.S. in strategic dialogues with those EUMS and non-EUMS that are most reticent to endorse enhanced European security and defense capabilities due to their concerns about the negative impact such developments may have on the transatlantic relationship. Unsurprisingly, the Baltic States, Finland, and Poland exhibit the highest threat perceptions of Russia in Europe and are thus most intensely focused on maintaining robust relations with the U.S., investing in defense modernization, and meeting NATO spending targets. Additionally, some European countries perceive Poland's engagement with PESCO as an effort to gain influence over the initiative and ensure that EU defense integration does not clash with NATO commitments. The U.S. should take the lead in assuaging concerns of conflict between European partners, NATO members, and within the transatlantic relationship by engaging in dialogue at the institutional level – both with the EU and NATO – but also through more informal channels outside the traditional institutional infrastructure such as the UK, Germany, and France's E3 arrangement. This will be particularly valuable for the EU, whose decision-making processes are often hampered by internal strategic cacophony and unanimity requirements. Ultimately, a European pillar for NATO cannot exist without close cooperation with the U.S.

In all, a European pillar for NATO cannot be conceived without greater investment in EU defense and security infrastructure. However, the EU will not succeed in mobilizing such investment without buy-in from the EUMS, non-EUMS European allies, the U.S., and

NATO partners. The success of a European pillar for NATO hinges on NATO retaining its primacy in matters pertaining to transatlantic security, and the EU should anchor its own security and defense ambitions within this reality.



Camille Ford
*Graduate Student of
International Security, Paris
School of International Affairs*

Camille is a first-year Master's student in International Security at the Paris School of International Affairs (PSIA) at Sciences Po, Paris. Coming to Paris from Washington DC, Camille previously worked at Foreign Policy Magazine, the American National Standards Institute, and Foreign Policy for America. She holds a B.A. in International Studies from Boston College. Her graduate studies center on transatlantic relations, european security and defense, and diplomacy. Camille is French, Swiss and American and speaks French, English, and Spanish.

AT THE FRONTLINES WITH RUSSIA: QUO VADIS GEORGIA'S & UKRAINE'S NATO INTEGRATION?

by Mariam Gamdlishvili

The recent visit of the U.S. Secretary of Defense to the countries of the Black Sea region (Georgia, Ukraine, and Romania) has been timely and shown another set of unwavering support of both – the United States and NATO, for Georgia's and Ukraine's Euro-Atlantic aspirations. At the same time, it seems that NATO and Russia entered to a new “cold war” in the relations, as Russia suspends its mission to NATO in response to the alliance expelling eight “undeclared” intelligence officers. Due to the convenient geopolitical location, the Black Sea Region (to which both Ukraine and Georgia belong) is one of the most important area in the world and plays an extremely important role in the modern global security affairs. After 2008 Bucharest Summit, for thirteen years the support and “open door policy” for Georgia and Ukraine are voiced, however, the progress with the Membership Action Plan (MAP) let aside the membership itself, has not been offered to the duo. This on its side, suggests that NATO's geographical limits are not exhausted, unless the door remains open and both Georgia and Ukraine continue to develop their interoperability with NATO. Being in the turbulent region of strategic importance, both Georgia and Ukraine continue to progress in the frames of their Euro-Atlantic aspirations. At the same time, both have to deal with ongoing Russian occupation and hybrid aggression.

The global spread of technology that can be of use in the production of weapons may result in the greater availability of sophisticated military capabilities, permitting adversaries to acquire highly capable offensive and defensive air, land and sea-borne systems, cruise missiles, and other advanced weaponry. Furthermore, technology aids the hybrid tactics with sophisticated approaches, will it be propaganda with its disinformation techniques or cyber-attacks. In addition, state and non-state adversaries may try to exploit the Alliance's growing reliance on information systems through information operations designed to disrupt such systems. They may attempt to use strategies of this kind to counter NATO's superiority in traditional weaponry. Alliance's security interests can also be affected by other risks of a wider nature, including acts of terrorism, sabotage, and

organized crime, and by the disruption of the flow of vital resources.

Despite positive developments in the strategic environment and the fact that large-scale conventional aggression against the Alliance is highly unlikely, the possibility of such a threat emerging over the longer terms exists. The security of the Alliance remains subject to a wide variety of military and non-military risks which are multi-directional and often difficult to predict.

These risks include uncertainty and instability in and around the Euro-Atlantic area and the possibility of regional crises at the periphery of the Alliance, which could evolve rapidly. Some countries in and around the Euro-Atlantic area face serious economic, social, and political difficulties. The resulting challenges within the European members of NATO could lead to crises affecting Euro-Atlantic stability, to human suffering, and to armed conflicts. Such tensions could affect the security of the Alliance by spilling over into neighboring states, including NATO countries, or in other ways, and could also affect the security of other countries. While the discussion over NATO's European pillar become more topical, the limits and engagement within it is questionable, NATO cannot ignore the current status quo of the Black Sea Region. Therefore, while discussing the European pillar, NATO should be inclusive towards its reliable partners – Ukraine and Georgia within its eastern flank strategy.

In general, the relations between Russia and NATO at this stage have a number of features. One is the nature of their pendulum. Starting from the period of the “Cold War” and, until recently, they are characterized by change of “cold snaps” and “warming”. The second feature is the fact that in recent years, these relations are in “catch-up” key. As we enter to another “cold snap”, the Euro-Atlantic integration of both – Georgia and Ukraine may continue at the stalemate, despite the cooperation and new formats, such as the recently signed between U.S. and Georgia memorandum on Georgia Defense and Deterrence Enhancement Initiative or U.S.-Ukraine Strategic Defense Framework. Therefore, it is crucial and important to include both countries in a deeper practical cooperation (previously contribution to NATO mission in Afghanistan). NATO and U.S. should consider the idea of Eastern European military presence, due to the changing geopolitical landscape in South Caucasus.

NATO is activated in different dimensions in the region, so Russia sees it as to be forced to respond to these challenges and mostly on the defensive. At the same time, if NATO will be actively growing geographically, occupying many niches, including most of those who had previously been occupied by Russia, the impact zone of Russia on many items will be narrowed. And as this trend continues, the further expansion of NATO capabilities

may proportionally weaken Russia. In being at the frontlines with Russia at both conventional and non-conventional military tactics, it is also clear, that Georgia and Ukraine cannot be left alone. The Euro-Atlantic aspirations of both are confirmed and supported continuously, but tangible results are long delayed.



Mariam Gamdlishvili
Senior Specialist,
Foreign Affairs Service of the
Administration,
Government of Georgia

Mariam Gamdlishvili is international relations and strategic/global communications specialist. She currently serves as a Senior Specialist at the Foreign Affairs Service of the Administration of the Government of Georgia. Mariam has been an Edmund S. Muskie Fellow at the George Washington University's Institute for Public Diplomacy and Global Communications and her experience includes working on Georgia's European and Euro-Atlantic integration, strategic and global communications, dis/misinformation topics at the Digital Forensics Research Lab of the Atlantic Council, Ministry of Foreign Affairs of Georgia, Georgian Center for Strategy and Development, Office of the State Minister of Georgia on European and Euro-Atlantic Integration. Mariam recently received a MA degree in Communications from the University of Southern Indiana in the frames of the Fulbright Program, funded by the U.S. Department of State. She also holds an MA degree in European Union Studies (CIFE Erasmus +), and BSc degree in International Relations. Mariam's research interests include international relations, communication studies, disinformation, soft power, global/political and international communications, public diplomacy, focusing on Eastern Europe, South Caucasus, and Russia.

HOW TO TRANSFORM NATO'S EUROPEAN PILLAR

by Roman Haupt

As this working group is about to address the topic of NATO's European Pillar, it seems advisable to first clarify, what this term means. It is well known that of an overall number of 30 NATO states, 28 are European. Currently, there is not a single non-European or nonAmerican country represented in NATO. Given their sheer number and considering that among NATO's European members are some that play an important role on the world stage, such as Germany and France, it is fair to say that NATO's European Pillar is indispensable within the alliance. Furthermore, it was often European countries that played a crucial role in shaping the alliance and that made way for progress in the past.

NATO's European Pillar today

Unfortunately, NATO's European Pillar is weak nowadays. While the US' security focus is shifting towards the Indo-Pacific area, Europe is left with a simple question: Can it defend itself against outer threats? Unfortunately, the recent pullout of Afghanistan has proven that it cannot, as it revealed an alarming military weakness of European NATO members. Surely, Europe's security focus is not primarily on Afghanistan, but more on its own territory. Nevertheless, the question must be asked, if European NATO states would be able to defend themselves in a military conflict, if they could not even fight successfully against the Taliban.

At the same time, conflicts between NATO's European members are increasing. To give just one example, the heavy dispute between Greece and Turkey about offshore natural-gas reservoirs in the Mediterranean Sea exemplifies existing tensions just too well. So, how does Europe have to redefine its position regarding NATO? Are there any specific policy recommendations one can make to ensure that its European Pillar remains at the heart of NATO?

A call for reforms and progress

As outlined above, NATO's European Pillar is in desperate need of reform to maintain a strong position

within the alliance! To achieve this, some measures have to be taken.

1. A strategic alliance between NATO and the European Union must be established. Although this idea is not new, there have never been more urgent times to translate it into practice, as the whole continent is facing new challenges, such as the rise of terrorism. 21 NATO states are also members of the EU. Both organizations have the fundamental aim to secure peace within Europe. Yet, they are still primarily operating separately from each other. This prevents them from tackling pressing issues effectively. Thus, resources must be concentrated, especially in areas where interests are shared. One measure to achieve this would be to set up a joint taskforce, fighting the increasing danger of terrorism. Simultaneously, egoistic interests of certain states, still blocking stronger cooperation must be overcome to equip both, NATO and the EU, with what is needed in the future. Therefore, new instruments must be developed to sanction such states, which could entail the option to exclude them from joint military operations.
2. The decreasing willingness of the US to give Europe unconditional military protection will not be put to an end, only because the former President Trump has left office. Therefore, NATO's European members must focus their abilities in a joint effort – only then will they be able to provide sufficient technological and military capacity. Single European states would simply not be able to defend themselves in potential conflicts with, for example China or Russia, as no European NATO member has a military big enough to compete. Consequentially, a rapid buildup of common European military forces is needed, to which all European NATO states would have to contribute. At the same time, this implies to develop a code of conduct, Europe's NATO members have to follow seriously, and which would prohibit single countries from taking military action against external states without agreeing it with its allies beforehand. This also coincides with the previous paragraph. If a European Union's army is to come into place, it needs to be set up in close cooperation with NATO.

To put it in a nutshell: While a strong North American-European axis remains vital to NATO's future success, Europe nevertheless must improve its own military abilities! The abovementioned proposals would signify great progress in that regard.

3. The question of whether further European states should be admitted to NATO must be addressed. Although this is a desirable goal, it is not practicable at the moment. Looking towards Eastern Europe, the only serious candidate left is Ukraine. Integrating Ukraine into NATO would be likely to undermine Russian influence in Eastern Europe. At the same time, Ukraine's previous leaning to the West led to an increasingly aggressive Russian behavior that could be best observed through the annexation of Crimea. While NATO should not be intimidated by its actions, it would also not be wise of Europe's NATO

members to risk further tensions with Russia, given the weak position they are currently in. Shifting the focus towards other European states which are still not members of NATO, their integration seems to promise great wins for everyone at the first glance. Most of them are countries that value the shared ideals of NATO, and naturally they are all interested in securing peace and stability within Europe. But one must also consider that the embedment of these states could create further conflicts, as it would become even harder to find a consensus on many issues within the alliance.

The conclusion to be drawn from this is that if more countries shall be embedded, significant reforms have to be put into practice first to keep NATO's European Pillar capable of acting. This would, for example, include to abolish the right for middle- and high-ranking officials to veto proposals at an institutional level.



Roman Haupt
Undergraduate Student of
Governance and Public Policy,
University of Passau

Roman Haupt is a current undergraduate student at the University of Passau, pursuing a degree in Governance and Public Policy. Despite his young age, he has had a great interest in international security politics ever since. As a strong supporter of NATO and the European Union, he made the role of European countries within the alliance his hobby. Roman is constantly looking for new opportunities to gain further knowledge in the field of international security and is dedicated to work ambitiously on concepts of how NATO can reinvent its role in the world. Simultaneously, he is committed to various organizations, among them the Model United Nations Society Passau and the Hertiestiftung Jugendbeirat Demokratie to shape society in a wider context. After finishing his degree in Passau, Roman wishes to continue his studies in the UK, where he wants to focus on law and international relations.

LEVERAGING THE RESOURCES AND DIVIDING THE LABOUR FOR A STRONGER EUROPE IN NATO

by Doris Manu

"The EU's current security environment is more volatile, unpredictable, complex and ambiguous than at any other time since the end of the Cold War. The EU therefore has a growing responsibility to safeguard its own security while defending its interests and values", said Member of the European Parliament David McAllister.

Indeed, security challenges in parts of Europe and in its neighbourhood have multiplied in recent years. On European soil, inter-state tensions are rising in the Western Balkans, but also along the EU border with Belarus. In the cases of long-standing "frozen conflicts", such as the Donbas in Ukraine and Transnistria in Moldova, there has been no progress in the negotiations. And such conflicts can easily escalate, as it happened recently in Nagorno-Karabakh.

Under these circumstances, security should be a political priority for the European NATO members, who would be most affected by active conflicts in Europe.

Yet, European members of NATO take less political ownership of their security and less responsibility for the security of their neighbourhood than they could.

Europeans largely rely on the support and presence of NATO's American pillar in Europe, and that is especially the case for NATO Central and Eastern European members.

At the same time, NATO is impacted by different priorities of its members, with more focus and resources of American NATO members going to security challenges in the Pacific. This creates the momentum for NATO's European members not only to take more ownership of their own security, but also to invest in the security of the neighbourhood.

How can the concept of NATO's European pillar work in practice?

Dedicating resources

Increased defence spending by European members of NATO in recent years came in response to American demands. However, this did not translate in a stronger European security and defence cooperation or notable investments in the European defence industry, nor security support to the neighbouring countries.

European NATO members should make a common contribution to NATO's budget that is directly proportional to NATO's European pillar security needs. Those

resources should be used for security and defence cooperation in Europe, but also for security support to the neighbourhood.

This could also benefit relations between NATO members in Europe. Increased intra-European cooperation, also outside the EU Common Security and Defence Policy and the Permanent Structured Cooperation, would strengthen the sense of political ownership for all NATO's European members.

Creating structures

The coordination of the activities of NATO's European pillar security and defence cooperation should happen in addition to the cooperation of EU NATO members through CSDP and PESCO. It is important to include as well NATO members who are not EU members, but the cooperation in the context of NATO's European pillar could also allow for the inclusion of European neighbours to whom security support would be extended. Strengthened regional cooperation across NATO and EU membership lines, as the one existing in the Nordic region, for instance, could supplement the European pillar.

A more practical cooperation could be done through European agencies such as the European Defence Agency.

Addressing the concerns about weakening transatlantic ties

The changes in the strategic landscape and the prioritisation of own security by American NATO members make a stronger case for security and defence cooperation of Europeans among themselves. The European pillar of NATO becomes more than a choice and more of a necessity when the security in Europe's neighbourhood is considered.

A more robust security support to the Eastern neighbours and non-NATO members in the Western Balkans should come from NATO's European pillar. In the absence of it, it will be Europeans who will be most affected.

The approach of the Central and Eastern European NATO members, who perceive stronger security cooperation and defence structures in Europe in opposition to strong transatlantic ties, is therefore misguided.

To sum up, a more volatile security environment requires that Europe does more to make itself and its neighbourhood truly secure. NATO's European members

can achieve this by a) making a common contribution to NATO which is proportional to their needs and using those resources to strengthen security cooperation in Europe, and b) creating structures to foster and support that cooperation.

By being a security provider to the countries of the neighbourhood and by being able to defend itself, Europe can have a stronger global role. And transatlantic cooperation, in all areas, can only benefit from a stronger and more credible Europe.



Doris Manu
Adviser to the
Government of Romania,
Office of the Prime Minister

Doris Manu works as Adviser to the Government of Romania – Office of the Prime Minister. Previously, she worked on EU-Western Balkans relations at the European External Action Service, the European Commission and the European Parliament. Her research interests are EU foreign policy and enlargement, identity politics and post-conflict reconciliation. She holds a Master in European Politics and Administration from the College of Europe, a Master in South-Eastern European Studies from the University of Belgrade and a Bachelor in Political Science from the University of Bucharest.

NATO'S FUTURE KEY TASK: INVESTING IN STRONGER POLITICAL UNITY AND CITIZEN'S SUPPORT

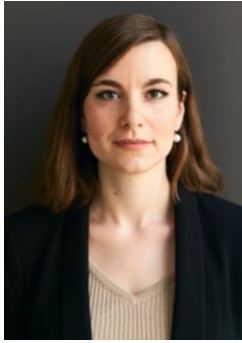
by Sophie Schäffer

On NATO's 70th anniversary in 2019, some people posed the question what NATO's *raison d'être* was in today's world, an organization originally founded as a counterbalance to a no longer existing power bloc. For a few, this question had a more existential ring to it: Does NATO still have this *raison d'être*? The textbook answer to the first question is that NATO protects and defends the Euro-Atlantic community with their one billion people and 30 member states. But, looking at the larger picture, and answering the second question, NATO fulfills an additional purpose: It stands for the liberal idea of the Euro-Atlantic community, and it defends these liberal values in times of much headwind. It is thus now the time to strengthen NATO and its community of member states. The challenges that NATO will face in the next ten to twenty years are manifold. Only stronger political unity, including among NATO's European member states, can achieve this.

Maintaining political support among member states' citizens in favour of the alliance is already crucial but will become more important in the near future. NATO's areas of action have already expanded from land, sea, and air, to cyber and space. Nevertheless, many of the threats NATO will face in the coming years are not primarily military, but rather of a hybrid nature. These threats do not target the alliance's militaries, but rather civil institutions. Its damage is not done by weapons, but by eroding the backbone of a society: the citizens' trust in the state and in each other. Included in this are phenomena such as disinformation, state-sponsored meddling in elections, targeting of critical infrastructure, or sponsoring illegal migration. It is thus NATO's key task to convey its purpose to the population, especially young people, who are too young to have witnessed NATO's founding period and original *raison d'être*, namely the

Cold War. Young people in (Western) Europe often take peace for granted, but they must re-learn that peace is not the norm in Europe, and that without peace, their way of life cannot be sustained. Moreover, foreign and security policy often seem rather abstract and faraway from everyday life. NATO needs to convey that without peace and freedom, other policy topics such as education, climate change, or equality cannot be tackled. The question that follows is how does NATO adapt to these challenges? The military and political dimension of NATO require each other. Staying strong militarily means continuing to invest in member states' armed forces and modern military capabilities. Strengthening NATO politically means using NATO as a forum to discuss, and where necessary to act, on issues affecting the shared security of NATO member states. What both goals prerequisite is the political will to act for shared security, thus, to strengthen NATO's political dimension. The reflection group initiated by German foreign Minister Heiko Maas, co-chaired by German former Minister of Defence Thomas de Maizière and American former Assistant Secretary of State for European and Eurasian Affairs Wess Mitchell, was a first step in that direction. Besides adapting to a changing security environment and delivering on its military responsibilities, NATO needs to enhance its political purpose. It could do so by building up stronger partnerships with institutions in civil society and the private sector. In times of increased populism throughout Europe, NATO must maintain the connection to the people it intends to protect. One way to achieve this could be to initiate townhall formats in cities (not only capitals!) in European NATO member states, where citizens can pose questions and discuss relevant topics with (former) NATO officials or NATO "ambassadors".

If NATO wants to continue to fulfill its purpose, it must make sure to communicate its *raison d'être* to the citizens of its member states. Freedom, democracy, the rule of law, and human rights are what makes NATO member states strong as nations and as an alliance. Investing in the alliance's political unity is thus investing in its future – and the future of the people it means to protect.



Sophie Schäffer
Graduate of International
Security and International
Relations, Sciences Po
Paris/King's College London

Sophie Schäffer recently completed a dual MA in International Security and International Relations at Sciences Po Paris and King's College London's Department of War Studies. She earned a bachelor's degree in Political Science from Freie Universität Berlin. Her interests include German and European foreign, security and defense policy and strategy, transatlantic relations, and national security. Sophie is a board member of Women in International Security Germany.

NATO AND THE EU STRATEGIC AUTONOMY: AN ALLIANCE TO STRENGTHEN EU-US DEFENSE TIES

by Marco Schiafone

NATO is still Europe's main security actor, but 'EU independence' could be a milestone in the Atlantic alliance as it would enable to strengthen EU-US defense ties in a multipolar world. NATO shall not be based on economic purposes: the idea of assuring the US commitment by increasing the EU's defense spending will not help the alliance. European members, as well as the US must express shared values and vision. What recently happened in Afghanistan is a clear symptom of the difficulties the transatlantic alliance is facing. The will of the US to withdraw from the Central Asian country forced the EU to follow up the ally's decision. It is time to have a balanced relationship and a European pillar within NATO.

Since 2010, questions have been raised on the "European Defence" or the "European army": the idea of cooperating with respective Member states' national armies or creating a totally new European body or yet, how to address defense spending of each member State; but lack of political will, as well as unity within the European Union, just brought tough and undefined proposals, such as the Strategic Compass as well as the European Intervention Initiative (EI2) and the idea to rely totally on the US defence commitment is not an option. European Member States and NATO itself should enhance and push for the EU's Common Security and Defence Policy (CSDP), which normally is considered as an alternative to defence provided by the Atlantic alliance - also because of its mismatch between EU and NATO members. Improving the CSDP would create a European forum of shared values, cooperation and principles - and more generally a positive outcome on political and military affairs, that will be reflected in the transatlantic partnership raising NATO's level of ambition in international security.

Moreover, the main idea is that CSDP threatens or hurts transatlantic cooperation, but it is a mean to improve NATO, not an alternative to it. This is what EU Strategic Autonomy in its defence dimension should be; indeed, closer cooperation of the EU keeps the US engaged. It is not about Europe separating from the US; it is about Europe being able to act at US side. This would give life to a more balanced transatlantic cooperation and, most of all, to a European pillar within NATO where the EU could take the lead. This doesn't mean the US and Europe are parting their common path, or that "NATO is

obsolete". On the contrary, it means the US and Europe both need to actively reconceptualize the transatlantic partnership and the notion of burden-sharing, helping coordinate the effort to its development.

In this regard, NATO - and more generally the new transatlantic relationship - needs to adapt its own structure to the new security landscape, while promoting and searching for greater cooperation between EU Member States.

Recently, a response arrived at the EU-US Summit in Brussels on June 15, 2021 where the transatlantic leaders - among other major issues discussed, as COVAX, G20 and trade - dealt with the EU's invitation to the US to join the Permanent Structured Cooperation (PESCO) Military Mobility project as an important step towards an ever-closer EU-US partnership in security and defence. It concerns the US engagement with the European Defence Agency (EDA) on the will to work together to raise the level of NATO-EU key strategic partnership. In fact, I would look in favor of a new potential engagement of the US with EDA, which in my view should be perceived and supported by NATO as a further step towards smoother and linear participation of the US government on one side and of the EU common position - expressed by EDA - on the other.

At the same time - and apart from the CSDP and EDA partnerships, I would recommend that NATO clarifies its nature and adapts to changes. More specifically, the Atlantic organization was born with a European dimension, with the aim of defending its member states, but, despite NATO has been described and defined as a regional organization, in the past years the active engagement in international security of the North Atlantic Alliance has clearly identified the global aim NATO has. It is time to develop a new role. In 2020, Secretary General Jens Stoltenberg stated that: "As the world changes, NATO will continue to change". Under NATO 2030, proposals showed the will of Atlantic Allies to redefine the organization's institutional role: from URSS to existential threats addressing climate change, autonomous weapons as well as cyber defence and transnational terrorism. NATO has to evolve from a Euro-Atlantic vision to a global perspective facing rising powers, as China or India. It is vital to expand its policies to new strategic areas. NATO should be no longer just "regional", it should be the most important defence alliance once again that masters emerging and new threats.

In conclusion, the most pressing areas to be addressed by NATO in the next years could be gathered in

(a) establishing sound cooperation with the EU - in Common Security and Defence Policy (CSDP) - in order to create a determined European ally in the transatlantic relationship,

(b) also through stronger cooperation between the US and the European Defence Agency (EDA),

(c) to reaffirm its institutional role and to consolidate the transatlantic relationship, NATO should be able to develop its structure as well as its aims together with new threats.



Marco Schiafone
Graduate Student of
International and European Law,
University of Turin

Marco Schiafone is currently an LL.M. candidate at the University of Turin where he focuses on International and European Law. He holds an LL.B. in Law with Transnational Law. During these years, he developed interests in security and foreign policy, transatlantic relations, terrorism and irregular warfare, as well as international organizations and West's relations with MENA and Central Asian countries. He previously worked as a Research Intern at CefES - Center for European Studies where he analysed the EU external action in the Middle East Peace Process.

**THE MAKING OF A GLOBAL ACTOR THROUGH
REGIONAL CONSOLIDATION**
by Silvia Tauro

Since the Trump administration, Brexit, the AUKUS pact and the US withdrawal from Afghanistan without consulting its NATO partners, the European pillar of NATO, or the lack thereof, has become a primary object of political discussion. Due to the increasingly transnational dimension of security and the rise of collective threats, a comprehensive European dialogue and collective strategic culture on interstate security must be established.

One of the biggest challenges will be the conceptualisation of a geographically cohesive European pillar on the defence front. Europe is not a united geopolitical subject, as it is very diverse in terms of security concerns. Whilst Russia is perceived as an existential threat in the eyes of the Baltic states, it is no longer a menace in the eyes of Western Europe. In fact, it represents a key energy partner for Germany, and a close ally for Hungary. As security transcends national borders, a European pillar will not remain limited to a specific geographical scope. Under American stewardship, Europe has essentially been split in two security blocs in the past months. The first bloc is made up of Western European countries, which have been backing the US in its confrontation with China, with the UK, Germany and the Netherlands at the forefront. The most blatant example of this strategy is the deployment of European frigates to the Indopacific. The second bloc acts as a container of Russia, and encompasses the region between the Baltic Sea, the Black Sea and the Adriatic, whose countries are characterised by a pronounced Russophobia (historical or recent). The six nations that border the geopolitical demarcation line designed and supported by the American superpower are Norway, Finland, Estonia, Latvia, Lithuania and Poland. It is clear that future confrontations will require the European continent to face diverse challenges on different fronts.

European NATO member states are very diverse in their functions and capabilities. The UK has historically been at the forefront for a stronger European security pillar inside NATO, representing 20% of European military

resources. Its withdrawal from the EU has drifted British security policies away from the European core. And whilst Germany advocates for a closer collaboration with its transatlantic partner, France and the Netherlands have been pushing for “strategic autonomy” and a more centralised European approach on security. Nonetheless, these differences could prove to be crucial assets for a stronger European pillar. The UK must push for a comprehensive integration of non-EU NATO members, e.g. Norway, a key partner in the Eastern containment. The UK and France reflect solidity as nuclear powers with expeditionary capabilities. Germany can assume the lead as an economic superpower and unifier among European nations. France and Germany are essential guarantors of the congruence between NATO and the EU.

There is the assumption that the creation of a European pillar may strain the continent’s relations with its transatlantic partners. European security concerns do not always align with American ones. Whilst China is one of the principal security concerns of the American administration, Macron pointed out that the last time he checked, China was not in the Atlantic, and therefore outside the area of competence of NATO. But NATO has historically led to a bilateral dependence between Europe and North America. Whilst European member states still heavily rely on US military defence and deterrence, Europe represents an optimal platform for exercising both symmetrical strategies towards Moscow – nuclear deterrence – and asymmetrical strategies towards Beijing – trade blockade. What must remain clear is that a European pillar is a complementary asset to strengthen NATO, not as an alternative to it. On the contrary, it might result in a more horizontal dialogue between partners. Future decision-making with the US is indispensable for a number of future security challenges, particularly in respect to the Indopacific, Russia and the Eastern Mediterranean.

A structural change to a European security pillar is crucial, and specific concerns must be addressed. Currently, few European NATO members meet the spending target of 2% GDP, and their military capabilities were not modernised. These resources will be indispensable for the creation of a strong European pillar and the development of military, administrative and strategic assets. All member states should strive for the

implementation of the goals set out in NATO's 2030 plan, as well as focusing on nation-by-nation improvements in the realms of cooperation, deterrence and defence, and horizontal consultation. The specifics of a more comprehensive European integration could include European headquarters, an expanded role of the EDA, a furthering of the Berlin-Plus Arrangements – enabling the EU to lean on assets from NATO for international missions, or a new institutional body altogether.

The three main European actors on security, France, Germany and the UK, ought to be at the forefront of a strengthened European pillar, and increase dialogue with the EU High Representative and NATO Secretary

General. More precisely, Germany and France put forward the idea of a “European Security Council”, to strengthen Europe’s security and foreign policy and keep the UK involved. This could centralise European dialogue on security concerns in a horizontal forum.

The transatlantic solidarity, epitomised by article 5, is only credible if underpinned by a set of common values, also within European borders. Thus, a European pillar within NATO ought to address the military, but also the political dimension. With the increase of burden and decision sharing for the sake of a strategic culture, European leaders must develop a cohesive approach on security matters.



Silvia Tauro
Graduate Student of
International Security,
Sciences Po Paris

Silvia Tauro is a Master's student in International Security at Sciences Po Paris, specialising in European and Middle Eastern Affairs. She is currently interning at Transparency International EU as a policy assistant. She holds an undergraduate degree in Political Science and International Relations from Sciences Po Paris. She attended two semesters at Tel Aviv University, focusing on Middle Eastern and conflict studies. She has experience in research, advertising and publication releases. Her main domains of interest include European security and foreign policy, Middle Eastern affairs, transnational security and risk analysis.

PAN | New Era of Transatlantic Cooperation: A EL 3 | Common Position Towards China?



© Photo by Hanson Lu on Unsplash

For decades this has been subject to accusations of exporting values and interfering in internal affairs. Today, China's foreign policy aims at propagating its ideological ideas with stunning dynamics, self-confidence and huge funds. In contrast, the German/European approach sometimes seems static these days. Of course, as liberal democracies they must act differently. So how can they better advertise democratic societies and defend themselves against attacks on a pluralistic opinion landscape, disinformation and hybrid warfare – without at the same time putting in danger what they are trying to defend? The panel deals with an essential part of future hybrid warfare, which crosses the boundaries of classical cultural policy as well as those of classical security policy. The answers we provide will be essential for shaping foreign policy in the future. At the same time, regional developments in the Asia-Pacific region must not be left out – is there an EU position and a common transatlantic approach?

PANELISTS



Gesine Weber
Program Coordinator,
Paris Office of the German
Marshall Fund of the United
States

Gesine Weber is a Program Coordinator at the Paris Office of the German Marshall Fund of the United States. Her work and publications focus on European security and defense, including EU-U.K. relations and the CSDP, French-German relations, and the EU-U.S.-China triangle in geopolitics.

Gesine is also pursuing PhD research on European defense cooperation at the Defense Studies Department of King's College London, where she is affiliated with several research groups. Prior to joining GMF, she worked as a parliamentary advisor to a member of the German Parliament, focusing on security and defense, and as a consultant on China for the Friedrich-Ebert-Foundation. She graduated with two masters' degrees from SciencesPo Paris and Freie Universität Berlin, and also studied Mandarin Chinese at the Beijing Foreign Studies University.



Gwendoline Vamos
Political Affairs Officer, NATO

Gwendoline Vamos is a senior officer in the Global Partnership Section in the Political Affairs and Security Policy Division at NATO Headquarters, Brussels. In this capacity, she is the lead on overseeing NATO's relationship with China. Before assuming this position in 2016, Mrs. Vamos served more than 10 years as the lead policy officer in the Russia and Ukraine Section in the Political Affairs and Security Policy Division at NATO, where she was responsible for NATO's bilateral relations with Russia. Before joining NATO, Mrs. Vamos worked at the European Commission in the Evaluation Unit for the TACIS and PHARE technical assistance programmes, as well as in a Public Affairs Consultancy firm in Brussels.

Mrs Vamos holds a Bachelor of Arts in Slavonic Studies from the Brussels Free University and a Master of Arts in Political Sciences from Sciences Po Paris.



Daniel Cisek,
Chief of Political-Military Affairs,
U.S. Embassy Berlin

Daniel Cisek is a U.S. diplomat assigned to the U.S. Embassy in Berlin with responsibility for security and defense issues. His prior diplomatic assignments included Moscow, Kiev, Islamabad, and Mumbai. He has also worked in positions focused on nuclear arms control and East Asia security issues at the U.S. State Department in Washington, D.C. He is originally from Chicago.

CHAIRS



Lisa Stappenbeck,
Research Associate, Bundeswehr
Planning Office

Lisa Stappenbeck is dedicated to the transatlantic relationship. She built a foundation in American Studies as well as Peace and Conflict Studies which she then strengthened during her work with the German Council on Foreign Relations, at the UN in New York as well as the State Department. After leaving intern life behind, she enjoyed working for the Canadian Embassy in Berlin for three fantastic years. Currently, she is contributing to incorporating innovation into the German Army at the position with the Bundeswehr.

***MOVING INTO UNCHARTED WATERS:
NATO'S OPTIONS WITH CHINA***
by Lok Hang Abraham Chan

The international arena has witnessed drastic changes in a range of areas such as the COVID-19 pandemic, digitalization, the rise of nationalism, the outspread of disinformation, and climate change across the globe in recent years. It is essential for the North Atlantic Treaty Organization (NATO) to evaluate its strategies in adapting to the current condition.

For decades, the West assumed that the People's Republic of China (PRC) would have, through increasing interactions with the West and its own economic development, included more democratic values and economic liberation into its system. Despite the Chinese President describing the Chinese political system as 'democratic', some internal and external behaviours of China have been taking the wind out of our sails. Since NATO was founded on the principles of democracy and promoting democratic values is one of the main missions of the Alliance, the concerns of Chinese expansion should not be fallen on deaf ears. There are three possible strategic approaches in handling the NATO-China relations as a reference to the diplomatic history between NATO members and partners and China.

1. The first option is the bandwagoning strategy followed by Greece and Hungary that aim at building closer ties with China. Some economic and diplomatic benefits could be anticipated, yet it would undermine the rulemaking power of the Alliance.
2. The second approach is to align with the United States, Japan and Australia to confront the Chinese expansion. Relations between NATO members and China would deteriorate and the operation in the Indo-Pacific or the Asia-Pacific could be costly, but this method extricates like-minded democracies from the ambitions and threats of the rising power.
3. The final proposal is to be neutral and distanced from the Chinese activities outside of the NATO territories. This is a stance which China would

approve of and it gives grounds for NATO-China cooperation. Such an approach would, however, put the internal stability of NATO at risk as it is incompatible with the foreign policies of the United States, Japan and Australia.

No matter which strategic approach NATO chooses, the following considerations should be taken into account: One observable phenomenon of China is its expansion on western social media in the forms of state-controlled media, investment in western media and the intensifying political comments by the Chinese diplomats. These Chinese online activities have given rise to the contagious fear of disinformation and propaganda in NATO democracies. The broadcast license of China the Global Television Network (CGTN) was, for instance, withdrawn by the Office of Communications (Ofcom) in February 2021 because of the breach of the Ofcom Broadcasting Code for maintaining due impartiality in its coverage. It was only until the French approval of CGTN's license that disentangled the Chinese state-owned broadcaster from that British reprimand under the European Convention on Transfrontier Television. Thus, a common strategy is needed in response to the complexity of cyber warfare while preserving the freedom of expression and the freedom of the press.

Another concern with the rise of China is whether the Indo-Pacific or the Asia-Pacific is of the interest of the Alliance, and how committed each NATO member is in the region. NATO has several global partners that uphold western democratic values, namely Australia, Japan, New Zealand, and the Republic of Korea, which are minorities in the region. These countries have demonstrated their commitment to Afghanistan and have been working closely with the leading powers in NATO. Should NATO show support to these politically like-minded partners in response? If so, what should be the scope and the intensity of the support? What kind of consultation or cooperation would be accepted by China?

If NATO has decided to be more active in the Indo-Pacific and the Asia Pacific, it is inevitable to face China in some of its top concerns: Taiwan (One China Policy),

the South China Sea (the Chinese nine-dash line and Philippines v. China), Hong Kong (Sino-British Joint Declaration) and Macau (Sino-Portuguese Joint Declaration). These topics are linchpin in Chinese politics and Chinese nationalism. Any action or comment by NATO could jeopardise the relationship with China and NATO partners. On that account, different strategies should be carefully prepared by the Alliance depending on whether China is being evaluated and regarded as a friend, a strategic partner, or an adversary of NATO.

Overall, the role of China is indispensable in the world order and therefore for NATO's security and development. Even though China is geographically distanced from the members, it is geographically close to the Alliance's global partners. Additionally, the regime has also been very active in its global expansion. NATO should evaluate China and how it should be perceived by the Alliance. The categorisation of China and the following strategies would have a long-lasting influence on NATO's internal and external stability.



Lok Hang Abraham Chan
MA Student of North American
Studies, Freie Universität Berlin

Lok Hang Abraham Chan is working towards a MA in North American Studies (Political Science and Economics) at Freie Universität Berlin, having previously studied at Sciences Po Toulouse and the University of Crete as an Erasmus student. He has worked for businesses and organizations in both Europe and Asia, supporting international procurement, humanitarian works at Moria Refugee Camp, and research on migration, legal-economic COVID-19 study and EU-China relations. Abraham is an alumnus of the Europaeum Oxford, the Egypt Government's Nasser Fellowship and the Global Leadership Challenge, a joint initiative of the Oxford Character Project, Alibaba Entrepreneurs Fund and St. Gallen Symposium. His main research interests center around international relations, international trade and migration.

NEW ERA OF TRANSATLANTIC COOPERATION: A COMMON POSITION TOWARDS CHINA?

by Anna Meyniel

2021 marks the centenary of the Chinese Communist Party (CCP)'s founding, as part of Xi Jinping's Two Centenaries goals. The goal was for the Chinese society to be "moderately well-off", which the CCP described as a doubling of the 2010 per capita income figures. In 2020, it more than doubled, reaching 32,189 yuan (about 4,961 US dollars) according to official data. This essay argues a common transatlantic and European cyber strategy is key to facing the coming challenges that China represents.

China's recent development is often described as expansionist, with regional hegemonic claims in the Asia-Pacific region and an enduring US-China rivalry. Our threat perception of China, is argued here, comes mainly from China's use and shaping of the cyberspace. The cyber sphere is the geostrategic place where China is pursuing its foreign policy aims and spreading its vision for the international system. It is also the sphere where, this essay argues, the EU and NATO can find the best renewal of dynamism for acting together in a common transatlantic approach. The cooperation between the two would help building a common cyber culture so that the cyber sphere also includes a liberal-democracy stance.

Indeed, what is key to understanding China's conception of the cyberspace is how it is a means to shape the international system in a way that is beneficial to China's domestic and foreign objectives. China has been the lead state in promoting a new digital normative order based on cyber sovereignty, which primary aim is to have national control over the internet. In the private sector, China is also a major actor that the EU and NATO should take into account in their common approach. As of 2021, Huawei holds 15.4% of the global 5G technology patents shares, and Chinese telecommunications company ZTE, another 5.6%, by far surpassing US, European or other Asian companies. 5G is emblematic of how China includes the cyberspace in its foreign policy strategy. As this technology is slowly integrated as an international digital

norm, it is key to understand how China views cyber capabilities and the implications for the international community. China also acknowledged having a "Blue Cyber Army", which efficiency is precisely due to close cooperation between non-military and military actors.

Both the EU and NATO have already developed cyber capabilities and are cooperating in the cyber sphere. However, there are different levels on which the two should be focusing for improving that cooperation and creating a democratic cyber culture, much needed to face the Chinese approach to the cyber sphere.

Separately, both the EU and NATO have thus had the chance to develop their cyber toolkit. Yet, these capabilities often seem to be multiple and uncoordinated, while both organisations could benefit from enhancing cooperation. Both can account for numerous actors in the cyber sphere. Only naming a few, the EU relies on a CERT-EU (Computer Emergency Response Team) or the EU Agency for Cybersecurity (ENISA), while NATO relies on the NATO C3 Board or the Cooperative Cyber Defence Centre of Excellence. The exaggerated number of actors makes it absolutely vital and urgent that both actors coordinate their efforts in the cyber sphere. Both of them have capabilities through which they can strengthen this cooperation, but enhanced cooperation is needed to build a common democratic cyber culture.

To summarise, NATO and the EU are already cooperating through the 2016 Technical Arrangement on Cyber Defence, in the areas of training, research and exercises and information exchange. Still, there is more to be done in order to build a strong common cyber culture capable of challenging China's. To protect a sense of democracy in the cyber space, two main areas of cooperation should be underlined.

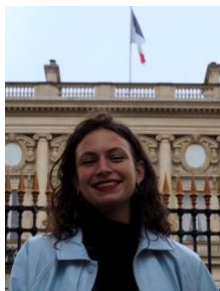
1. Creating a cyber culture common to NATO and the EU. In order to define the lines of a democratic cyber space, a common framework for a sanction regime should be prioritised in funding. Since 2016, NATO and the EU have been sharing cyber defence information, which should now focus on securing

electoral processes. The EU applied its first sanctions to cyber attackers in 2020, and this initiative should be followed by both actors. A Joint Cyber Unit, instead of the multiplicity of actors on both sides, could focus on the common threats to both entities, China, but also Russian interference on Western undersea communication infrastructures, for which NATO re-established a command post in the North Atlantic. Shaping the nature of a democratic cyber space by clearly condemning interference and malicious cyber activities, and building a common cyber force, is essential.

2. Increasing Transatlantic and European cyber resilience. The EU and NATO's ability to continuously deliver the intended outcome, despite adverse cyber events, rests on two main components.

- a. First, the dependence on Chinese technology, notably with Huawei and 5G. The lack of homogeneity in European cyber capabilities is preventing European technological companies to come up with a credible option on 5G networks, which both actors could enhance through training, recruiting, research and innovation. Both organisations also need to increase Private-Public-Partnerships to create a competitive and secure cyber culture.

- b. Second, there is a need to determine precise priorities in their cyber strategy and hence to strengthen deterrence capabilities on a regional level. Once common priorities are determined, crisis management systems should be reinforced, notably on existing programs that need more attention, like the CB4CyberResilience project. NATO also relies heavily on national infrastructure, which would be a first area of focus on such a cooperation. Likewise, the EU needs NATO for harmonising national military efforts and engage the capabilities of the United States.



Anna Meyniel
Graduate Student in
International Security, Sciences
Po, and Conflict, Security and
Development, King's College
London

Anna is a graduate student currently finishing her master in the War Studies Department of King's College London. During her undergraduate studies (Sciences Po Paris, 2020), she took an interest in cyber security, China-Russia cooperation and the Women Peace and Security Agenda. She worked on these issues at the French Embassy in Buenos Aires, in the Domestic Security Service, and during her time as president of the Sciences Po United Nations student union. After completing a first MA in International Security with a concentration in Diplomacy, she is now focusing her research on conflict resolution and the impact of the cyber sphere in the future of conflicts. She speaks French, English, Spanish and is learning Mandarin. She hopes to pursue her career in international organisations.

NATO'S EUROPEAN PILLAR

by Anna-Sophie Himmelreich

Chinese FDIs and Their Threat to NATO Member States' Industries

NATO and China are not enemies. Yet, there is growing competition between the transatlantic community and a rising China. This competition or rivalry does not directly include military aspects as the Indo-Pacific security is built on different patterns than NATO's collective security arrangement. However, much of today's rivalry includes a geoeconomic aspect where investment, trade and other economic flows have become domains of contestation as well as technology, energy, and infrastructure.

Beijing's Bold Moves towards Leadership

NATO's and its member states' slow responses to counter growing Chinese direct foreign investments (FDI) can potentially tilt the relationship between the two power blocs. When Chinese enterprises execute FDIs it mostly occurs under the umbrella of China's latest ambitious program which serves the growth of its domestic tech industry: Made in China 2025 (MiC2025). For this, the country has defined ten key industries - such as new energy and energy-saving vehicles, aerospace, new material, maritime equipment, and high-tech ships (Congressional Research Service, 2020) – industries with the highest potential of growth in the next three decades. However, the program is asymmetrical; while the Chinese government is highly encouraging its state-owned enterprises (SOEs) as well as private companies in investing in such industries abroad, it is restricting foreign investors to enter its own market.

MiC2025 has provoked heavy criticism as many countries see their industries and intellectual property endangered. The focus of Chinese FDI's lays mostly on successful businesses with an outstanding record of research and patent registrations (Dürr, Rammer, & Böing, 2020). The data and knowledge used in these companies is often transferred to the parent enterprise where these are used to further develop the technologies, which undermine the position of their Western subsidiaries on the world market and creating

an asymmetry and lack of fair investment terms. These practices are not in line with various WTO regulations (McBride & Chatzky, 2019).

China's striving for power position comes naturally, looking at the country's long history. The strategic culture in China is based on a sense of national humiliation that accents the treatment of China at the hands of Western powers in 18th and 19th centuries, and at the hand of Japan in the 20th century. Revering this deeply felt humiliation is a key driving force behind China's actions. Its long term goals include gaining a status equaling that of the U.S. The aggression with which the current Chinese government acts makes, however, many other actors nervous.

Timid Responses Versus Courageous Actions

Both the European Union and the United States have addressed the issue while noticing that the methods with which China tries to pursue its goals undermine the domestic industries of multiple NATO member states. Yet, they have notably failed to agree on a joint policy to curb Chinese FDIs. Germany, for instance, made several proposals to secure its domestic industry in cooperation with other EU nations such as France but eventually established an independent policy – six years after the announcement of MiC2025 (Hoppe, 2021). At the same time, previous U.S. President Donald Trump underlined his attempt to challenge China's tactics with his America-First doctrine, introducing tariffs on Chinese goods (Heering, 2019). China's strict Foreign Investment Law has prevented many investors from entering its market up to the present, but the country has also understood that it is on thin ice and provoking an economic war. Therefore, over the past five years, the law has steadily been eased, giving more possibilities for foreign investors to enter the Chinese market.

The international criticism on the matter has not stopped, as not all industries are open for FDIs: access generally is very restricted or accompanied with numerous regulations. The economic asymmetry between China and the rest of the world, thus, remains. The likelihood of other cleavages and frictions open up and further fueling the contestation remains high. This scenario should also be part of NATO's planning in

Europe, as it seeks to chart a more cohesive policy line vis-a-vis China.

A Future Path for NATO

The challenge for NATO is to establish a policy, which protects its member states while maintaining a respectful dialogue with China. This can only be accomplished if we understand China's interests as well as our own and draw clear lines in our action. It is most important that we establish policies that secure those industries which contain sensitive data against investments which are focused on their exploitation. An economic cooperation between NATO member states and China is desirable and such policies must therefore stay flexible in order to negotiate on a level playing field. Chinese economic aggression is a security threat to NATO, which must be recognize it as such and counter Chinese efforts as an united alliance with a joint policy. The purpose of the alliance should in this context be remembered: to create an umbrella under which member states can develop peacefully and to cooperate against in the defense against challenging outside forces. Like this, an eventual escalation of the conflict can be prevented.

Policy recommendations:

- NATO should directly address the asymmetry China creates through its FDIs and domestic investment policies. NATO and work in tandem with the European Union to seek solutions to the unfavourable investment domain.
- NATO member states should include China's policies as well as methods of countering them in the agenda of forthcoming summits on the matter in order to align interests of member states in terms of Chinese FDIs.
- NATO should establish guidelines for countries' legislatures, which protect their economy and knowledge against China's strategic practices. In particular, it should better identify strategic assets and technologies as well as value chains where China is gaining dominance and bridgeheads.
- Economy should be adopted as a new domain for rivalry and competition within NATO. At the same time, avenues for collaboration and dialogue should be maintained.



Anna-Sophie Himmelreich
Graduate Student in
International Relations,
University of Tallinn

Anna-Sophie Himmelreich is a master's student of International Relations at the University of Tallinn with a specialization on the impact of India and China's growth on the rest of the world. She completed her B.A. studies in International Management at the University of Applied Sciences Leipzig and the University "Tor Vergata" in Rome. With her background in business studies, she has worked for a British-Italian startup in Rome and for the Athens- office of the Konrad-Adenauer-Stiftung, a German think tank. Her main focuses are hybrid warfare, intercultural communication, and emerging powers. She is currently co-chair of the International Relations Society of Tallinn University.

WAGING THE WAR OF DISINFORMATION: EUROPE'S CAPACITY-BUILDING THROUGH DIGITAL COLLABORATION AND INTEGRATION OF CIVIL SOCIETY

by Antonia Mayer

Tackling disinformation has been on the European Union's agenda since 2015. Despite its current practices in cyber crisis management, the EU lacks a sustainable and proactive strategy for maintaining order in the information space that goes beyond the scope of existing cyber defense policies in the light of evolving cyber threats. Traditionally, cyber strategies have emphasized intergovernmental cooperation; however, private networks and civilians are increasingly the main target of disinformation campaigns. Thus, civil society must be a crucial part of the effort to solve the EU's limited action in countering disinformation attacks.

Disinformation proliferates not only during election campaigns, but wherever and whenever it can manipulate public discourse. The European Union (EU), Western governments and the North Atlantic Treaty Organization (NATO) are ill-prepared in countering disinformation attacks. EU policy-makers are yet to fully comprehend the new platform upon which warfare is being waged: disinformation is the newest cyber weapon to threaten EU's democracy. Unlike the EU, China has advanced its offensive strategy by building institutions such as the Cyberspace Administration of China to take advantage of this unprecedented competition and confirm its dominance. China knows that whoever owns information space, owns anti-democratic battlefields, controls information, and ultimately shapes global citizens' perception of reality.

While democracies tend to value information as indispensable to a lively democratic community, authoritarian regimes like China abuse information in two ways: domestically, leveraging their own primacy in the cybersphere to control and surveil their own populations. Internationally, they make use of the relative absence of Western governments in the space to weaken their democratic competitors abroad. Increasing

disinformation campaigns around Covid-19 have shed light on the limitations of the EU's strategy to counter disinformation and thus endanger and discredit the livelihood of democracies.

The EU must take a more dynamic stance in establishing a strategy for competition in the information space by cooperating more closely with its partners and civil society and respond in an institutionally cohesive and dynamic manner.:

- 1) The EU should extend its digital collaboration with partners and allies: Cyber resources are still closely controlled by national governments, which limits the effectiveness of the EU's cyber defense. Governments should draw on and support regional and EU resources using the potentials and capabilities of all member states. Thus, a more deepened "shared digital co-governance" measure is suggested. Such shared co-governance allocates resources and capacity-building without eroding individual national interests and including wide security requirements. While there have been numerous initiatives with the EU and NATO to wage the war of disinformation, such initiatives need to be better coordinated to ensure their effectiveness. These enlarged collaborations will set a precedent of an alliance-wide cyber policy to counter disinformation.
- 2) The EU should integrate civil society through the media, private and nonprofit sector: The potential of partnerships with the private, media and nonprofit sectors has not yet been fully tapped, particularly in these sectors' capacity to facilitate broader media literacy through new tools and educational structures. These partners can act as a channel to reveal disinformation to the public and help build resilient, attentive and critical consumers of information flows. Think tanks, NGOs, the media and the private sector need to be included to encourage, empower and engage people to tackle the threat with a grassroots response. Society as a whole is exposed to infiltrated disinformation on a daily basis, while it is much less exposed to counter-measures. Only if societies

understand what state-based disinformation is, how to detect and counter it, society will be no longer the vulnerable target but the active adversary of disinformation campaign.

Policy recommendations:

While cooperation with other actors already exists, these partnerships need to be extended and deepened both in Europe as well as externally. It is necessary to not only cooperate with governments but to consider networks in the private and nonprofit sectors to be of equal value to governmental cooperations. While information warfare, both globally and in the EU, mostly takes place on private

networks and devices, Europe has not yet integrated civilians into its strategy or indeed recognized the pivotal role that civilians play in this arena.

The sooner EU decision-makers realize that this information competition will determine the global order of cyber actors, the sooner the EU can work with its allies and its citizens to make cyberspace safer for democracy and to prevent the erosion of the European values of democracy, security, justice and freedom.



Antonia Mayer
Graduate Student in Political
Science, Rutgers University (USA)
and University of Konstanz

Antonia Mayer is a double Master's degree student in Political Science at Rutgers University, USA and the University of Konstanz, Germany. She holds a Bachelor's degree in Politics and Public Administration. During her undergraduate studies, she studied in both Moscow and Tallinn, as well as her native Germany. She has worked as a research assistant with the Chair of International Relations and Conflict Management in Konstanz and in the office of the Minister-President at the Representation of the State of Baden-Wuerttemberg to the European Union in Brussels. As a Fulbright fellow, she graduated from Rutgers in May 2020 with focus on Security Studies, European Politics and International Relations. In addition to her full-time studies, her fellowships at two German foundations, she engages in community-based activities that lie close to her heart. She will major in International Administration and Conflict Management, and will be graduating in Fall 2021 with her second Master's Degree.

FESTINA LENTE: NATO'S EYES AND EARS ON CHINA

by Ivano di Carlo

Throughout his reign, the first Roman Emperor had one motto “festina lente”. Make haste, slowly. The oxymoron, which has its roots in military strategy, sums up the advice he gave to his commanders: to get things done, it will take as much time as it is needed for them to happen. In layman's terms, it is fundamental to balance urgency and diligence, to act quickly but with caution. Two thousand years later, this recommendation should serve NATO and its member states to consider how to incorporate a contentious argument such as that of China in the daily work of the organisation.

A changing global order

In recent years, the stability of the international political and economic order has steadily weakened. The intensification of the US-China rivalry has contributed to the steady deterioration of international relations. A structural change in the distribution of power is undergoing with non-conventional threats increasing the prospect of broad instability.

NATO has not remained immune to these shifts and has recalibrated its policies and operations in various domains. Prompted by the need to counter the new complex and interdependent nature of threats and accommodate the different priorities of its member states, it has adopted a “360-degree approach” to security. Often viewed as an “imperfect compromise” risking to overstretch the Alliance, this approach encompasses the ability to deal simultaneously with threats emanating from a variety of directions.

Since 1949, NATO has survived many internal and external crises while continuously adapting to the changes brought about by the evolving international security landscape. Seven decades after its foundation, while Russia is still considered the major threat to NATO, China poses a novel multidimensional challenge due to its global power projection and geo-economic reach.

The rise of China – another item on NATO's menu

Under President Xi Jinping, China has indeed increasingly displayed a more active and assertive foreign policy on the global stage. Beijing's political ambitions, rapid economic growth, and continuous military and technological advancements have the potential to affect some of the core interests of the Alliance.

All of this has raised concerns. In the US, China is widely regarded as a strategic competitor and the signature geopolitical challenge of the twenty-first century, not just on security but also from a trade and technological angle. By contrast, although Europeans have increasingly hardened their stance towards Beijing, they do not see eye to eye with the US about how to deal with China's rise and are – at least in principle- hesitant to view Beijing with the same existential concern as Washington does, especially within NATO.

Diverging views do not necessarily mean that there is no potential room for compromise and cooperation. The London Declaration of December 2019 and the 2021 Brussels Summit Communiqué demonstrate how NATO is increasingly paying more attention to China.

With both sides of the Atlantic now recognising China as a systemic challenge, NATO's Strategic Concept expected to be released in 2022 -in parallel with the EU's Strategic Compass- will shed light on the future approach of the Alliance on China.

Looking for a shared vision and cohesion

President Joe Biden's overriding preoccupation is China. As a Financial Times article recently pointed out, “America is back – and wants everyone to focus on China”. Yet, many European leaders are worried that an American strategic rebalancing to Asia would lead to a reduced engagement in European security, thus posing the risk of diverting attention from Russia and diluting the Euro-Atlantic-centric model of NATO.

These different political trajectories are occurring in an already volatile context where a lack of a shared security vision and understanding persists across most of the spectrum of allies, even within the EU itself. Notably, divergent threat and interest perceptions between North America and Europe on how to deal with China are being

amplified by a general feeling of distrust, despite attempts to repair the frayed transatlantic ties. By doubling down on a confrontational approach towards China and overlooking the scepticism of other member states, the US could potentially erode NATO's political cohesion when it comes to identifying and prioritising future challenges and capability requirements.

The AUKUS agreement coming on the heels of the US withdrawal from Afghanistan left obvious scars on the EU-US-UK relations and highlighted the lack of structured transatlantic consultations. Recent steps such as the first meeting of the US-EU Trade and Technology Council, the US-EU Dialogue on China, and the potential launch of a dedicated dialogue on security and defence could only resolve some of the primary sources of irritants between the EU and the US.

Being a political and military alliance, for NATO is more challenging to develop a multifaceted approach towards China than the EU. For this reason, a common approach that seriously considers how to address China within NATO could only be achieved if it is preceded by a coherent and consistent vision among its allies. Otherwise, any strategy risks being watered down and weakened by diverging interests.

The latest test for NATO – striking the right balance

Cohesion in an alliance is the glue that holds the organisation together. Nevertheless, there are significant differences in the extent to which countries are eager to compromise and support any new policy falling outside their basket of interests.

Regardless of the state of the transatlantic relationship, NATO cannot find itself unprepared by ignoring to address the potential implications that China's rise has for its security and defence architecture. Still, the Alliance must also acknowledge that its ever-expanding agenda and objectives might become a mere list of words if not supported by any political will and military capabilities. On top of that, the Alliance is not necessarily best placed to

deal with specific matters that remain a national (or EU) responsibility, such as the monitoring of foreign direct investments, export control mechanism, identification of possible risks and vulnerabilities in global value chains, illicit financial flows, and acquisition of key infrastructure. As the world changes, NATO has to adapt faster. At the same time, member states within the Alliance should cautiously identify the most appropriate means to reconcile NATO's changing strategic outlook with its traditional functional and geographic mission. Any rush into framing a more robust NATO's China policy could eventually paralyse the Alliance. Against this backdrop,

NATO should:

- Reinvigorate cooperation with the EU and examine which organisation is best equipped to deal with selected problems threatening the North Atlantic Alliance at large
- Rethink the nature of burden-sharing for a more capable and autonomous Europe
- Identify opportunities to engage global partners in the Asia-Pacific region and consider whether to group them in a new partnership programme (e.g., Mediterranean Dialogue)
- Increase consultation and dialogue among member states while improving societal resilience to resist interference from third countries and other non-state actors
- Strengthen NATO's situational awareness of all activities that may impact transatlantic security and defence
- Elaborate a comprehensive security strategy to deal with China's growing global power -in view of an ever-growing Russia-China cooperation-without moving away from NATO's traditional missions and tasks



Ivano di Carlo
Policy Analyst,
European Policy Centre

Ivano di Carlo is a Policy Analyst in the Europe in the World Programme at the EPC. Before joining the EPC, he worked at NATO, the European Investment Bank, the University of Warwick and Boeing. His primary research interests include global economic governance, security and defence, Russian and Chinese foreign policy. He holds an MA in International Political Economy from the University of Warwick. Furthermore, he holds a Double MA in Public Policy and Political Analysis from the Higher School of Economics in Moscow, and in International Politics and Markets from the University of Bologna, where he also obtained a BA in International and Diplomatic Affairs.

NEW ERA OF TRANSATLANTIC COOPERATION: COMMON POSITION TOWARDS CHINA?

by Madeline Deyo

Democracies must strategically leverage their right to free and open communication to understand, inform, and educate populations. A progressive, tailored, and practical communications strategy could effectively create a shift from static to dynamic while engaging more people, preserving a pluralistic opinion landscape, and concurrently enhancing transatlantic and national security.

One of the most fundamental differences between liberal democracies and their adversarial states is the access to free and open communication. Whether that be free speech, print, or social media, democracies can use one of their most significant and founding principles to withstand attacks on our pluralistic opinion landscape from foreign adversaries. Democracies should use the tools they have to counter the malicious efforts of adversarial states to protect their democratic values against fragmentation. NATO Allies and partners should use the quintessential principle of a democracy, freedom of speech, to their aggressive advantage over our adversaries.

Plurality is a challenge to preserve, making democracies hard to defend. Pluralities provide opportunities for people of all races, ages, sexes, and ideologies to inclusively exist in a democratic society. As a result, pluralistic societies come with the structural disadvantage of fragmentation and competing values and voices. Foreign threat actors further complicate this potential disadvantage by targeted hostile information activities that purposefully increase polarization among other outcomes. This results in fragmentation, increasing opinion gaps, and a rise in populism. The list of dangers is long and it varies by country.

I assert that we need an increase in tailored communications strategies that help support both the vulnerabilities and opportunities of NATO Allied audiences in order to meet the challenge of making our

societies more resilient and in turn, strengthening the Alliance. There should be more practical communications strategies tailored to the challenges of the Allies to send effective messages, from NATO, member states, and partners. NATO needs partners on both sides of the Atlantic buying into the increasingly important solutions that communications provide to security challenges. They need an increase in the volume of communications stretching over different segmented audiences within Allied countries and partner nations. This responsibility rests in the hands of capitals around the world, and supported by NATO.

These communications approaches should be tailored to intended audiences rather than a one size fits all plan. After all, our democracies are not one size fits all. They consist of pluralities of opinions and challenges that require specific messaging to targeted audiences to achieve a desired outcome. In order to protect the plurality of voices democracies provide a platform for, and use these voices to our advantage, we need to effectively reach our populations before someone else does. This is a potential vulnerability many countries currently face. The challenge of preserving pluralism produces the advantage of more prosperous societies, which in the end, are resilient to threats.

The shift to a dynamic approach means more investment in communication avenues to secure solutions for the future. It means accepting a holistic approach to the opinion landscape and meeting people where they are at instead of expecting new or aspiring audiences to understand topics only people in the academic and policy sectors do. In order to reach unconventional and desirable audiences, NATO must reach beyond their conventional avenues.

To engage young audiences specifically, NATO should bring a person-first communications centred approach to transatlantic cooperation. It's important to maintain that communications, though not the prevailing solution to transatlantic security, is a vital aspect that helps inform the three hundred and sixty degree approach that must

be taken when coming up with international security solutions.

Communication has the potential to be a tool to resist foreign policy aimed to derail transatlantic solidarity. It can bridge the theoretical concepts and policy ideas into real world practical solutions worthy of creating change.

In addition, the language in which these issues are conveyed must be accessible and digestible to the

audiences whose behaviour we are intending to change.

We must strive to communicate effectively and impactfully to allow for a dialogue about these security issues to transcend their usual audiences and to fulfil the need to take a different approach – perhaps a more dynamic approach.



Madeline Deyo
Graduate in Political
Management,
Carleton University

Madeline Deyo is an intern in the Public Diplomacy Division at NATO. Madeline is Canadian with previous experience in the Government of Canada working in both the intelligence and defence departments ranging in topics from public affairs to cyber policy. Madeline holds a Bachelor's Degree from McMaster University in Communications and a Master's Degree in Political Management from Carleton University.

***FROM ARTICLE V TO ARTICLE III: NATO
RESILIENCE AS A MEANS TO COMPETE AND
COOPERATE EFFECTIVELY WITH CHINA***
by Nicolas Reeves

Afghanistan uncovers an uncomfortable truth

Following a 15-day airlift, U.S. Army Major General Christopher Donahue boarded the last C-17 Globemaster scheduled to take off from Hamid Karzai International Airport in Kabul, thus concluding the chaotic finale of NATO's 20-year involvement in the War in Afghanistan. This ignominious end to the only mission for which NATO had ever invoked Article V—that “an attack against one...shall be considered an attack against them all”—instigated criticism from Washington's European allies. After all, many of them had agreed to the withdrawal not out of conviction that it was the right choice, but out of realization that remaining in Afghanistan without U.S. support was futile.

Buried beneath this criticism, however, lies an uncomfortable truth: Washington can and will single-handedly dictate the fate of NATO military engagements if it feels compelled to do so. The Afghanistan withdrawal serves as a case in point; although over 51 members and partners of the transatlantic Alliance participated in the war, the conviction of Presidents Donald Trump and Joseph Biden that U.S. and NATO involvement in the conflict had to end was enough to bring the mission to a close.

In the U.S.'s defense, its unilateral approach mirrors European perceptions of America's proper role in the transatlantic Alliance. Out of 16 NATO member-states surveyed in a 2020 Pew Research Center study, Lithuania, Canada, the U.S., the U.K., and the Netherlands were the only countries in which a majority of respondents indicated that their military should intervene under Article V if Russia started a conflict with a NATO ally. Meanwhile, majorities in France (57%), Germany (63%), Spain (72%), Greece (65%), and Italy (75%) stated that the U.S. would defend a NATO ally in such a conflict, while only small minorities in these

member-states indicated that their country should do the same.

Though it is undeniable that America's military might lends credibility to Article V, the notion of one-party responsibility evident in these opinions of the U.S.'s role in NATO constrains the Alliance's ability to meet the challenge China poses to transatlantic security today. This is because this (mis)conceptualization of U.S. responsibility in NATO carries with it a restrictive definition of the Alliance's value in the security environment of the 21st century. After all, the framers of the North Atlantic Treaty drafted Article V with the danger of a Soviet military attack against one of the Alliance's member-states in mind. While Russia's 2014 annexation of Crimea demonstrates that this threat continues to loom over NATO's Eastern flank in particular, the security questions China poses of the Alliance are markedly different.

**Article III: The key to a common NATO position
towards China**

China does not pose a direct military threat to NATO. Rather, the country could endanger member-states' security through its technological prowess in artificial intelligence and the cyber domain, and through its strategic investments in wireless networks, ports, railroads, and other critical infrastructure. The bilateral inroads China has made with almost all NATO member-states also threaten the Alliance's ability to function as a consensus-based institution.

Therefore, Article V—and the issue of U.S. unilateral behavior that comes with it—is not the correct prism through which to view NATO's capabilities vis-à-vis China. Rather, NATO's strength as part of a larger pivot to China lies in the call for resilience embodied in Article III's instruction that member-states “maintain and develop their individual and collective capacity to resist armed attack.”

In the context of China, developing the capacity to resist attack means regulating the cyber domain, strengthening cyber defense capabilities, insulating defense supply

chains from reliance on products produced by Chinese companies, and scrutinizing Chinese investment in member-states' critical infrastructure. In other words, NATO should use its resilience-building function to declare the domestic security domain off-limits to Beijing. Such a move would create the conditions necessary for balanced, rules-based competition and cooperation with China in other areas, such as trade, development cooperation, and tackling climate change. This resilience-centered approach would thus lay the groundwork required to establish a transatlantic consensus that privileges diplomatic and economic engagement over military escalation with China, preventing the return of an iron curtain or war between global powers in the process.

Policy Recommendations:

Avoiding a new Cold War is crucial: the challenges the world faces today, especially the existential threat of climate change, can only be addressed through global cooperation. For such a path to prevail over the sometimes-bellacose rhetoric coming out of Washington, however, the conceptualization of NATO as a hierarchy

led by the U.S. must be replaced by a vision that emphasizes equality among member-states, both in terms of their ideas and their commitment to mutual defense. It is in the spirit of these principles that I submit the following proposals upon which to base a common NATO position towards China:

1. Mandate that member-states meet the 2% GDP defense-spending target by 2030, broadening the definition of this to include spending on non-Chinese 5G technology and other critical infrastructure, whether domestically or in other NATO member-states.
2. Go beyond establishing a cyber defense strategy and protocol for member states, as outlined in the NATO 2030 Reflection Group's November 2020 report. In addition, NATO should create a working group, housed within the Cyberspace Operations Centre, to craft cyberspace rules and norms to which nation-states should adhere. The short-term goal of this exercise would be adoption by member-states, with the medium-term goal being adoption by member-states of other multilateral institutions.



Nicolas Reeves
Graduate Student in
International Development and
Political Science,
Sciences Po Paris

Nicolas Reeves is pursuing a dual master's degree in international development and political science from the Institut d'Études Politiques de Paris (Sciences Po) and Freie Universität Berlin. Nicolas graduated from the George Washington University in 2019 with a B.A. in international affairs and economics, and a minor in Arabic. After finishing his degree, Nicolas spent the 2019-2020 academic year in Egypt as a Center for Arabic Study Abroad (CASA) Fellow at the American University in Cairo. Following the conclusion of his CASA Fellowship, Nicolas returned to Washington, D.C. and worked for one year as a Program Assistant for the National Endowment for Democracy.

MEETING THE CHINA CHALLENGE: EMBRACING DIVERSITY IN THE ALLIANCE

by Stefan Munk

In June of this year, NATO Secretary General Jens Stoltenberg stepped in front of the cameras after the first NATO summit attended by President Biden and called China's rising influence a challenge to alliance security. Such far-reaching remarks – and the equally harsh Chinese rebuttal – were virtually unimaginable only a few years ago. How did we get here?

The basic underlying story is pretty simple. By most recent estimates, China's economy could overtake the United States' sometime around 2030. Projections are of course uncertain and economic prowess does not automatically translate into other forms of power. Still, this illustrates a challenge to the status-quo: a security strategy relying on the US alone outspending China is not a viable option in the long run. With China becoming more assertive globally, including in the North Atlantic area, Western democracies will thus have to rely on their partners in the systemic competition with China.

In that context, it has become increasingly clear that NATO must be a building block in a joint effort. Besides the statement after this year's summit, China featured prominently in the 'NATO 2030' report on the future of the alliance. Lawmakers in the NATO Parliamentary Assembly even drafted a transatlantic China strategy in 2020.

These documents set out some cornerstones of alliance cooperation on China. They include, for instance: better information sharing and common risk assessment, enhanced resilience against Chinese cyber-attacks, cooperation with NATO's Indo-Pacific partners.

So far so good. But while it is important to flesh out strategic priorities all alliance members can agree on, there are some inherent limitations in exclusively pursuing this consensus-based approach. Initiatives embraced by all 30 member countries will inevitably be somewhat vague, and avoid critical points. The Chinese threat to freedom of navigation is not seriously broached in any of the aforementioned outlines, for example.

Strength in diversity

Some variety is only natural in a diverse alliance such as NATO and hence needs to be encompassed within any strategy on China that seeks to translate statements into meaningful action.

Coming back to the example of freedom of navigation: while there is agreement in the alliance on the respect for international law, there are only a limited number of European countries able and willing to transfer maritime assets to the Pacific region: primarily Britain and France, but also the Netherlands and Germany may fall within that group. This does not mean that NATO should not play a role in coordinating and leveraging these presences, however.

On other issues, like cyber-attacks and disinformation, there is more consensus and they thus feature in the strategic documents. But here too, a more granular approach can make sense. Within NATO, there are members that are confronted with these technological challenges constantly, such as the Baltic republics and Finland. The expertise of these countries can thus be drawn on in a NATO effort to counter Chinese cyber capabilities.

Now, one could argue that this sort of particularizing approach is precisely what allows external actors to exploit fissures within NATO – a danger explicitly mentioned in the NATO 2030 report. If overdone this could indeed be the case, hence the need for common principles. However, it is possible to overstate the need for uniform action on every front. Such reasoning omits that throughout its existence, NATO has invariably relied on different contributions from among its members, depending on their capabilities, geographical location, and the like. Just as Portugal was not expected to provide the brunt of the primary manpower to deter the Red Army in central Europe, nowadays Luxembourg cannot be expected to conduct freedom of navigation operations in the South China Sea. A failure to recognize this reality risks paralyzing the alliance, and pushing members towards less coordinated action instead.

With this historical backdrop, NATO should not be afraid to draw strength from its diversity – a diversity of means, not of strategic ends. Only by being aware of these differences, they can be adjudicated accordingly and

flexible cooperation can leverage the benefits of operating in the alliance framework.

Towards a flexible strategy

To facilitate this approach, a key first step is to create a systematic overview of where the priorities and abilities of alliance members lie. National particularities need to be examined in depth at this stage – but also their willingness to integrate into a joint effort. For example, France has been rather active in the Pacific region, but has at times been unwilling to coordinate its efforts within a NATO context.

Based on that overview, the second step should be to think about taskforces, in which likeminded states can cooperate under the roof of NATO. In terms of groups formed, issues like freedom of navigation and cybersecurity (areas in which one can work with existing

NATO infrastructure) and other priorities as outlined in the NATO communiqués on China should undoubtedly be incorporated. But also activities outside of the usual scope of NATO can be included, above all in the field of economic resilience.

The taskforces would ultimately be in charge of implementing the approaches they develop. It should be noted that all these activities would mostly take place on the staff level. The broad outlines have been set in a political framework with high public visibility, whereas the role of the task forces would be to flesh out concrete implementation internally to assure participation without being subjected to outside pressure. Through this approach, paired with the flexible involvement of alliance members according to their abilities, it is most likely that NATO's China strategy will actually bear fruit.



Stefan Munk
Research Correspondent on
Foreign and Financial Policy,
German Parliament

Stefan is currently working as a research correspondent in the German Parliament on foreign and financial policy. As a fellow of the European Recovery Program, he completed his Master's degree in International Affairs at Columbia University in the United States. There, he focused on great power competition between China and the US, as well as its effects on Europe. Simultaneously, Stefan served as a Junior Researcher at the European Institute for Asian Studies.

A MORE INCLUSIVE ALLIANCE: NATO'S CHINA CHALLENGE

by Mary Yamamoto

The NATO 2019 Leader's Summit marked a pivotal turning point in acknowledging China as a legitimate threat to a rules-based international order. Yet, while NATO's public recognition is recent, China's geopolitical ambitions have been increasingly assertive for decades. This change in NATO's prioritisation challenges an organisation rooted within a European context that has historically focused on Russia. As the security landscape continues to rapidly evolve, so do the tactics of NATO's adversaries; as such, a flexible, innovative, and inclusive response is needed among the transatlantic allies.

China has a key advantage in its governance structure; unlike in liberal democracies, the Chinese Communist Party (CCP) utilises its ability to implement cohesive, long-term, and centralised foreign policy without changes in focus and approach that are often brought by democratic transfers of power. Under President Xi Jinping's leadership, China has adopted a substantially more assertive foreign policy and geopolitical approach, all backed by a global economic workhorse.

The security landscape at NATO has been traditionally embodied by its continued focus and prioritisation of Europe, and more specifically the direct threat that Russia poses to the Alliance. However, China has increasingly pushed the bounds of its economic, political, and cultural influence into the European fora. This has included economic coercion against European nations, nuclear weapons development, modernisation of its military, and increased military cooperation with Russia. More locally, China has been more aggressive with its Indian border and the South China Sea, and continues to work to consolidate power in Hong Kong and Taiwan. When faced with any criticism, the Chinese foreign policy machine responds with its assertive diplomatic "wolf warrior" campaign it uses to refute any international objections.

Further, under President Xi Jinping, China's foreign affairs approach has expanded well beyond the confines of classical security policy. The CCP continues to wage an extensive campaign in their mission to present and posture as an alternative to western liberal democracies.

One such facet has been the One Belt One Road initiative to provide humanitarian and development assistance. While lauded by key international players such as the UN, it has also been the source of security concerns in the regions where it has been engaged in developing. China has also extensively leveraged cultural and educational exchanges; for example, implementing Confucius Institutes in academic institutions abroad as a propaganda arm, or the use of "panda diplomacy," — utilising giant pandas loans to foreign nations as a negotiation tactic—as a supplement to its already extensive foreign policy.

In many ways, the way China has been engaged in their foreign policy is radically different and much more comprehensive than what has been utilised in traditional security policy. As such, when dealing with these non-traditional threats to the alliance, non-traditional—and in some ways, non-European—diverse approaches are not only needed, but required. The allied response cannot be rooted in traditional or "static," methods, and NATO must leverage the strength of its trans-Atlantic partnerships and adapt its approach where needed.

NATO Members, Partners and Allies should:

1. Engage more strongly with allies in Asia Pacific regions: While NATO is primarily a European and North American institution, the Alliance's adversaries are not limited in the same way. Asian geopolitical allies have been engaged with China more directly and for much longer; through closer partnerships, NATO allies can be more proactive in its approach to China. It is also vital to engage and highlight Asian liberal democracies and geopolitical partners more rigorously to strengthen collective defence.
2. Present an alternative by highlighting strength in diversity: While China has advantage of a unified voice from top to bottom, Allies do always have the same level of cohesion and unity. However, NATO members and partners should work to more strongly emphasise its strength in diversity—especially in regards to the various ways democratic systems can be instituted—as an alternative to the CCP system of governance.
3. "Walk the walk" as a coalition of liberal democracies: Allies should be pushing one another to be

more inclusive on key issues such as human rights, gender equality, human security, disability and race. Adversaries are quick to leverage failures in these areas as a sign of weakness. Allies must acknowledge and

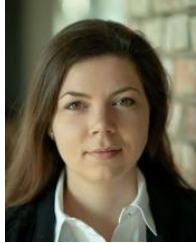
respond to the fact that adversaries are utilising these approaches in their own hybrid warfare. As such, best defence is to reduce that weakness through promoting and practicing inclusivity and diversity.



Mary Yamamoto
Intern with the International
Military Staff Office of the
Gender Advisor, NATO

Miary Yamamoto is an intern with the International Military Staff Office of the Gender Advisor at NATO. Miary holds a Bachelor's degree from Dalhousie University in political science and gender studies, and a Master's degree in international affairs from the Norman Patterson School of International Affairs at Carleton University. She previously worked at Global Affairs Canada, as well as Immigration, Refugees, and Citizenship Canada as an Evaluator. Miary's research interests include post-conflict peace processes and intersectional analysis.

FURTHER CONTRIBUTORS



Veronika Fucela
Chairwoman,
Youth Atlantic Treaty
Association Germany

Veronika Fucela is the Chairwoman of the Youth Atlantic Treaty Association Germany (YATA Germany), which is fostering public dialogue on NATO and transatlantic relations among the younger generation in Germany. Youth Atlantic Treaty Association Germany, also a member of YATA International, is with 600 members the biggest German youth organisation empowering discussion on security and foreign policy matters. Professionally, Veronika is serving as a parliamentary staffer for an MP in the German Bundestag working on German foreign policy, specializing in Central and Eastern Europe. Previous to that, she was a Project Coordinator at the German Atlantic Association. Veronika holds two MAs in International Relations and Politics.



Kamala Jakubeit
Program Coordinator,
Berlin Office, German
Atlantic Association

Kamala Jakubeit is a Project Coordinator at the German Atlantic Association's Berlin Office and board member of the Youth Atlantic Treaty Association Germany. She earned her Master's degree in European and International Relations from Linköping University, Sweden. Prior to that she studied Governance and Public Policy – Staatswissenschaften – at Passau University. In 2018 Kamala completed a five month internship in New York at the Permanent Mission of the Federal Republic of Germany to the United Nations focusing on the developments regarding the Security Council, Germany's membership in the United Nations Security Council and in particular issues regarding Libya, Iraq, Democratic Republic of the Congo, Sudan and Ukraine. During her studies, Kamala gained a considerable amount of practical experience during her six month stay in Ghana, her five months traineeship at the European Parliament, at the German Embassy Dublin, the Institute for Peace Research and Security Policy, and the Federal Ministry for Environment, Nature Conservation and Nuclear Safety.

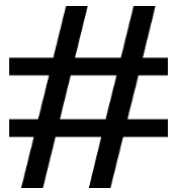


Pieter Brandt
Major,
German Air Force

Pieter is a Major in the German Air Force's technical branch. He studied aeronautical- and spacecraft engineering in Munich before gathering experience as a technical officer in a tactical jet fighter wing, in the German Eurofighter procurement and development office as well as in several NATO training courses in Germany and the USA. Back at the federal armed forces university in Munich, he was responsible for the military education and training of junior officers during their academic studies. He served as squadron commander in operation "counter Daesh" in Jordan and is currently based in southern Brandenburg as squadron commander in a transport helicopter wing. In July 2019, Pieter was elected as a member of YATA Germany's executive board.

CONTACTS

Name	Contact Info
Kamala Jakubeit Program Coordinator German Atlantic Association	kamala.jakubeit@ata-dag.de + 49 176 73 55 75 55
Pieter Brandt Member of YATA Germany's executive board Youth Atlantic Treaty Association Germany	pieter.brandt@yata-germany.de
Leonhard Simon Member of YATA Germany's executive board Youth Atlantic Treaty Association Germany	Leonhard.simon@yata-germany.de +49 173 6269036



#NATOTalk2021
#WeAreNATO
#NATOsFuture



@yata.germany
@DtAtlGes



@yata_ger
@DAGATAGermany

Cosponsored by:

