NDC Research Paper
Research Division – NATO Defense College – Rome

NATO 2030: new technologies, new conflicts, new partnerships

Edited by
Thierry Tardy

Research Division

No. 17
Feb 2021

NATO 2030:
new technologies, new conflicts, new partnerships

Edited by
Thierry Tardy

NDC Research Paper No.17 – February 2021

NATO Defense College – NDC Research Papers Series

Series editor: Thierry Tardy
Copy-editing: Mary Di Martino

NDC Research Paper 17 – 2021
"NATO 2030: new technologies, new conflicts, new partnerships"
Edited by Thierry Tardy

Keywords
NATO2030, emerging disruptive technologies, grey zone conflicts, partnerships

ISSN: **2618-0057**
ISSN (online): **2618-0251**

Limited copies of this NDC Research Paper are available and may be obtained directly from
NATO Defense College, Research Division
Via Giorgio Pelosi, 1 - 00143 Rome, Italy
E-mail: publications@ndc.nato.int
Website: http://www.ndc.nato.int
Follow us on twitter: https://twitter.com/NDC_Research

Printed and bound by *http://www.lightskyconsulting.com/*

Table of contents

Contributors

Benedetta Berti is Head of the Policy Planning Unit in the Office of the Secretary General at NATO. Previously she held research and teaching positions at West Point, The Institute for National Security Studies and the Foreign Policy Research Institute. She is the author of four books, including *Armed Political Organizations. From Conflict to Integration* (Johns Hopkins University Press, 2013) and her work has appeared in Al-Jazeera, *Foreign Policy, Foreign Affairs, the Wall Street Journal* and *The New York Times*.

Andrea Gilli is a Senior Researcher in the Research Division of the NATO Defense College where he works on issues related to technological change and military innovation. He has been Visiting and Post-doctoral Fellow at Johns Hopkins University and Columbia University as well as Stanford University (where he remains an Affiliate) and Harvard University.

Marc Ozawa is a Senior Researcher in the Research Division of the NATO Defense College where his focus areas are Russia, Eurasia, the High North, and energy security. He is also an Associate Researcher of the Energy Policy Research Group at the University of Cambridge. He has published works on European-Russian relations, Russia's relations with neighboring states (Baltics, Scandinavia, and China), and energy security policy.

Thierry Tardy is the Director of the Research Division at the NATO Defense College. He is also Visiting Professor at the College of Europe in Bruges. His research and teaching areas cover NATO's policy and adaptation, European security, the EU's Common Security and Defence Policy (CSDP), NATO-EU relations, the politics of crisis management, and UN peace operations. He has recently published *French Interventions in Africa. Reluctant multilateralism* (ed. with S. Recchia, London, Routledge, 2021).

List of abbreviations

AI	Artificial Intelligence
C3	Command, Control and Communication
CCDCoE	NATO Cooperative Cyber Defence Centre of Excellence
CHST	Counter-Hybrid Support Teams
CISA	Cybersecurity and Infrastructure Security Agency
CoE	Centre of Excellence
CSDP	Common Security and Defence Policy
ENSEC	Energy Security
ESC	Emerging Security Challenges
EU	European Union
GDP	Gross Domestic Product
ICI	Istanbul Cooperation Initiative
IPCP	Individual Partnership and Cooperation Programme
ISAF	International Security Assistance Force
JSID	Joint Intelligence and Security Division
MD	Mediterranean Dialogue
MENA	Middle East and North Africa
NATO	North Atlantic Treaty Organization
NCIA	NATO Communications and Information Agency
NDC	NATO Defense College
NGO	non-governmental organizations
PaG	Partners around the Globe
PfP	Partnership for Peace
PPU	Policy Planning Unit
R&D	Research and Development
UN	United Nations
UNHCR	United Nations High Commissioner for Refugees
US	United States

Acknowledgements

This *Research Paper* brings together three texts that were initially produced as background papers for events the NDC Research Division organized in coordination with the NATO Policy Planning Unit (PPU) in the context of the NATO 2030 process.

The first event (24-25 September 2020) dealt with grey zone conflicts; the second (28-29 October 2020) addressed emerging disruptive technologies; the third event (10-11 December 2020) examined NATO's partnerships.

The NDC Research Division is grateful to Benedetta Berti from NATO's PPU for her introduction to this Report and to Ruben-Erik Diaz-Plaja (PPU) for his overall support to our three events, as well as to the following persons for their contribution to the events and/or feedback on earlier drafts of this *Research Paper*.

NATO 2030: Adapting NATO to Grey Zone Challenges – 24-25 September 2020

Dalia Bankauskaité, Benedetta Berti, Chloé Berger, Heather Conley, Richard Connolly, Ruben-Erik Diaz-Plaja, Keir Giles, Stephen Mariano, Jeffrey Michaels, Dumitru Minzarari, Andrew Monaghan, Francisco Prata, Kristi Raik, Chris Riley, Jens Ringsmose, Michael Rühle, Cynthia Salloum, Charly Salonius-Pasternak, Marcin Terlikowski, Brian Whitmore.

NATO Technological Superiority at 2030 – 28-29 October 2020

Izabela Albrycht, Benedetta Berti, Jacques Bughin, Edward Christie, Skip Davis, Ruben-Erik Diaz-Plaja, Carl Benedikt Frey, Mauro Gilli, Michael Horowitz, Joel Mokyr, André Loesekrug-Pietri, Jon Lindsay, Stephen Mariano, Peter Newell, Andrea Prencipe, Niccolò Petrelli, LtGen Olivier Rittimann, Kaidi Ruusalepp, Nina Silove, Zoe Stanley-Lockman, Sarah Tarry.

NATO2030: NATO's Partnerships and Security Networks in a Contested Multilateral Order – 10-11 December 2020

Chloé Berger, Petr Chalupecky, Marta Dassù, Ruben-Erik Diaz-Plaja, Trine Flockhart, Xavier Godefroid, Gunhild Hoogensen Gjørv, Jolyon Howorth, Seth Johnston, Markus Kaim, Rory Keane, James H. Mackey, Stephen Mariano, Antonio Missiroli, LtGen Olivier Rittimann, Liga Rozentale, Mark Webber.

Introduction

Benedetta Berti

NATO's history is marked by both profound continuity and deliberate adaptation. Over the past seven decades, NATO's mission, the defense of the Euro-Atlantic area, and its constitutive values – democracy, individual liberty, the rule of law – have not changed. Similarly, the Alliance's founding principle, namely the commitment Allies have made to defend each other and work together for their common security and defense, is as relevant today as it was when the Alliance was established in 1949.

At the same time, NATO has adapted throughout its history to ensure it always remained capable to fulfil its mission and guarantee the defense and security of the almost one billion citizens it was established to protect. In the last decade, this meant that the Alliance had to boost its ability to tackle more sophisticated non-conventional threats. It has done so by investing in resilience as well as by enhancing its tools to fight terrorism, counter cyber threats, and respond to hybrid challenges. Even more fundamentally, since 2014, NATO has responded to the changing security environment by implementing the biggest adaptation of its collective defense since the end of the Cold War. This has led to deploying combat-ready troops in the East of the Alliance, modernizing NATO's command structure and Headquarters, enhancing the readiness of Allied forces and to an increased and sustained Allied commitment to invest more in defense.

In this context, NATO 2030, Secretary General Jens Stoltenberg's initiative, is driven by the belief that, to remain a strong and agile Alliance, NATO must continue its adaptation and focus on how to respond to a rapidly changing security environment.

At the December 2019 NATO Leaders Meeting, Allied Heads of State and Government asked the Secretary General to lead a forward-looking reflection on NATO's future. They asked him to provide concrete recommendations to NATO leaders in time for the 2021 Summit. In response, the Secretary General launched NATO 2030, focusing on the key question of how to prepare the Alliance for the next decade.

To inform his thinking, the Secretary General decided to reach out and gather ideas from a wide number of actors: he appointed an independent group to provide him with their advice, established the NATO 2030 Young Leaders to hear the recommendations of

the "next" generation, and launched a number of dialogues with civil society, youth and the private sector. The rationale behind this approach is solid: in an increasingly complex world where security challenges are more diverse and diffuse, it is especially important to engage with a broad set of stakeholders and to take different perspectives into consideration. The NATO Defense College's work on NATO 2030 fits within this broader set of discussions and contributes to the policy debate on NATO 2030 and on NATO's future more broadly.

The timing is especially ripe for a reflection on NATO's future adaptation. Looking at 2030, the Alliance needs to prepare for a more uncertain and competitive world. This requires understanding how the shifting global balance of power will affect both the international rules-based order as well as Allied security. It will be essential to consider how to best ready the transatlantic Alliance and how to forge a common approach to tackle these systemic challenges. At the same time, preparing for the future also means accounting for exponential technological changes and their impact on how conflicts are understood and fought; as well as stepping up efforts to combat climate change and prepare to mitigate and counter its security impact. It is also important to stress that while NATO needs to adapt to new challenges, it must also continue to strengthen its ability to tackle existing ones.

NATO 2030 thus gives the Alliance an opportunity to both take stock of the impressive adaptation occurred over the past decade and to redouble its efforts to prepare for the upcoming one. To do so, the Secretary General put forward three broad goals: to keep NATO strong militarily, to make the Alliance stronger politically, and to ensure it adopts a more global approach. The papers presented in this volume contribute to the thinking on how to meet each of these goals.

First, keeping NATO strong militarily is of course central to ensuring the Alliance's ability to fulfil its mandate. Collective strength and solidarity are equally crucial to maintain Allied unity and cohesion and to underpin the Alliance's political role. Ensuring NATO stays strong militarily requires sustained Allied investment in defense, but also a focus on Allied resilience and on technological innovation. Andrea Gilli's paper on "NATO, Technological Superiority and Emerging and Disruptive Technologies" tackles the crucial question of how to ensure NATO's technological superiority in the future. The paper rightly recognizes that historically the Alliance's ability to deter and defend has always been predicated upon maintaining a technological edge over competitors and potential adversaries. Looking at a future of exponential technological change and geopolitical competition, it is evident that preserving Allied technological superiority will become simultaneously more complex and more important. NATO has recognized the growing importance of investing in innovation and in preventing a transatlantic gap when it comes to the adoption of emerging and

disruptive technologies in security and defense. This is why, in recent years, the Alliance has redoubled its efforts in this field. Building on this progress, it is important to examine what more NATO could do towards 2030 when it comes to technological innovation in general and emerging and disruptive technologies specifically. Gilli's paper points to a number of important areas, including by stressing the need to think creatively about what role NATO can play to foster transatlantic innovation and encourage more Allied investments and cooperation on R&D. A similarly interesting and related notion is the need for NATO to reflect on its role when it comes to transatlantic training and education, both crucial to fostering cooperation and boosting interoperability.

Second, NATO 2030 focuses on how to strengthen NATO's political role. On the one hand, this means ensuring NATO remains the platform where North America and Europe consult and coordinate on all issues relevant to their common security and defense. On the other hand, a more political NATO is also an Alliance that is better able to rely on both military and non-military tools to fulfil its mandate. The importance of this issue emerges clearly in Marc Ozawa's paper "Adapting NATO to grey zone challenges". The essay examines NATO's tools and responses to a world in which competitors and potential adversaries increasingly rely on political, diplomatic, economic and military tools to challenge Allied security. The author argues that responding to these hybrid challenges requires the Alliance to update its broad strategy and expand its toolkit. This conclusion aligns with the Secretary General's call to update the 2010 Strategic Concept to take into account the new strategic environment. In addition, enhancing NATO's ability to respond to grey zone challenges, from information warfare, to asymmetric approaches and economic coercion, also means continuing and enhancing the Alliance's work on resilience, as the first line of defense against both conventional and non-conventional challenges. In this respect, Ozawa rightly argues that NATO should both expand the lens through which it looks at resilience and widen the actors it involves in its consultations on this issue. Expanding NATO's work on resilience could include, among others, using NATO more as a platform to discuss, identify and mitigate economic vulnerabilities that could be exploited to both sow disagreements and undermine Allied security. Similarly, broadening consultations on issues related to resilience and countering hybrid threats could lead to both more regular NATO meetings of Allied national security advisors and more robust engagement with the private sector.

Finally, the Secretary General's vision for NATO 2030 highlights the importance of adopting a more global outlook. Even though NATO is a regional Alliance, the challenges it faces are global, from terrorism to climate change. In this context, the question of how to better leverage NATO's partnerships becomes especially important. Thierry Tardy's essay,

"From NATO's partnerships to security networks" affirms the importance of partnerships as one of NATO's key political tools and looks at how to further enhance them towards 2030. In a world of growing geopolitical competition, one of the key questions for NATO 2030 is how to further strengthen the Alliance's political dialogue and practical cooperation with like-minded partners to deal with global challenges and defend the rules-based international order. Another important priority should be to examine how to further invest and leverage in partnerships to contribute to peace and stability in NATO's immediate neighborhood.

The three papers developed by the NATO Defense College's researchers engage with the Secretary General's 2030 vision by looking at how the Alliance can enhance its ability to innovate, strengthen its toolkit against hybrid threats and further leverage its partnerships as an important political tool. The breadth of topics reflects the fact that NATO finds itself in the most complex and challenging security environment since the end of the Cold War. In turn, this requires in-depth thinking about how to continue to deter and defend and tackle existing challenges as well as how to redouble efforts to adapt and innovate to address emerging ones.

1

NATO, technological superiority, and emerging and disruptive technologies[1]

Andrea Gilli

Since its foundation, NATO has enjoyed a broad, and ever-increasing scientific, technological and military superiority. In fact, the Soviet Union and its satellite states ultimately failed to stand up to NATO prowess: their economies were not sufficiently large and more importantly they could not keep pace with the free market-based economies of the Atlantic Alliance.[2] To a significant extent, as wealth-creation shifted from production- to knowledge-intensity, free societies enjoyed an increasingly marked competitive advantage: they could generate more ideas more quickly, spread them more widely, and exploit them more effectively. We may associate the end of the Cold War with the fall of the Berlin Wall. But in reality, the accelerating power of microchips offers a more cogent explanation for the turn of the era. After the fall of the Soviet Union, globalization unleashed a kind of power which further strengthened NATO: new members added new and different know-how and capabilities to the Alliance's pooled resources; offshoring of manufacturing permitted NATO Allies to specialise in higher-value activities which dominate global supply-chains; and high-entry barriers to advanced research prevented competitors from rivalling NATO scientific, technological and military superiority.[3]

This situation is, however, potentially changing. NATO Allied Command Transformation initiated the *Emerging and Disruptive Technologies Roadmap* in 2018 to take into account powerful and rapid evolutions, and revolutions, in technology which could shake NATO Allies' position.[4] Although scholars and analysts do not fully agree on the magnitude of the

1 Additional considerations and reflections on this topic can be found in A. Gilli, "'NATO-mation': strategies for leading in the age of artificial intelligence", *NDC Research Paper*, No.15, NATO Defense College, Rome, December 2020.

2 S.G. Brooks and W. C. Wohlforth, "Power, globalization, and the end of the Cold War: reevaluating a landmark case for ideas", *International Security*, Vol.25, No.3, Winter 2000/01, pp.5-53.

3 A. Gilli and M. Gilli, "Why China has not caught up yet: military-technological superiority and the limits of imitation, reverse engineering, and cyber espionage", *International Security*, Vol.43, No.3, Winter 2018/19, pp.141-189.

4 NATO Defence Ministers Meeting, 27 June 2019.

change, the consensus is that by 2030, NATO Allies risk losing their leadership in the most advanced technologies and eventually, they risk entering into conflicts where adversaries are better equipped in some areas. What is important to note, however, is that NATO has not lost its technological leading edge yet.[5] While defeatism is widely popular among some intellectual segments of the Alliance, there is no reason to think that the Alliance cannot maintain and even extend its scientific, technological and military superiority. Thomas Fuller noted, the darkest hour is just before the dawn: NATO technological superiority has not yet been eclipsed. As NATO Secretary General Jens Stoltenberg notes, "one of the main reasons why NATO is the most successful alliance in history is that we have been able to change every time the world has changed. And we need to continue to change, because the world continues to change".[6] Technological change is changing our world, NATO has thus to act – as the 2020 Reflection Group's Report on NATO 2030 also highlights.[7] In order to address this challenge, NATO Allies must adopt a whole-of-NATO approach: individual actions at the domestic level ought to be coupled with initiatives to leverage the potential and capabilities of the Alliance. As the Experts Group's report highlights, Allies must compete to achieve dominance in the realm of emerging and disruptive technologies, and NATO "should serve as a crucial coordinating institution for information-sharing and collaboration between Allies".[8] NATO Secretary General goes even one step further, since "emerging and disruptive technologies are having a profound impact on how the Alliance carries out its core tasks […] NATO will play a key role in driving this change".[9]

This chapter advances some recommendations to this effect, all held together by a common thread: the central role of human beings. Technological superiority is the product of strategic assessments, investment decisions, organizational capabilities and individual researchers, scientists and engineers, among others. In order to preserve and extend their technological leadership, NATO Allies must count on individuals who have the competency to both correctly understand technological trends, to invest at the right time in the right technological domains, fields and areas, and to design organizations that attract talent and permit individual researchers, scientists and engineers to excel. NATO can still lead in technology in 2030. But for this to happen, its Allies must want to achieve this goal, and be willing to focus on human capital.

5 A. Gilli and M. Gilli, "Imitation, innovation, disruption: challenges to NATO's superiority in military technology", *NDC Policy Brief* No. 25, NATO Defense College, Rome, December 2019.

6 Remarks by NATO Secretary General Jens Stoltenberg on launching #NATO2030-Strenghtening the Alliance in an increasingly competitive world, 8 June 2020.

7 "NATO 2030: united for a new era. Analysis and recommendations of the Reflection Group appointed by the NATO Secretary General", Brussels, 2020.

8 "NATO 2030: united for a new era", p.13.

9 " NATO ambassadors and military leaders meet to discuss disruptive technologies", NATO, 1 october 2019.

Technological superiority

We live in an age of unprecedented technological change. This is affecting our lives, societies, and economies. Progressively, this change is also affecting the international system. Discussion about a possible artificial intelligence (AI) race, transnational regulation of data, the impact of digitalization on trade flows as well as on supply-chain dependencies are not becoming increasingly salient by pure chance. For years, scholars and analysts have been postulating that it will not take much for such a wave of technological change to affect Great Powers relations, the military balance, and nuclear stability. Something different, however, may be looming on the horizon.[10]

Throughout its entire history, NATO has enjoyed a position of technological superiority which, after the end of the Cold War, has further widened. However, such scientific, technological and military superiority cannot be taken for granted any longer. At least five reasons account for this.

Relative fall in R&D expenditure. First, as societies grow wealthier and older, consumption absorbs an increasing amount of resources to the detriment of investments, especially long-term investments. This happened during the Roman Empire, but NATO Allies have also, in general, reduced R&D investments over the past decades. Within the transatlantic area, private companies' R&D expenditure has, in some cases, increased: but private companies' R&D spending tends to be narrow, short-termed, and business-oriented, and thus less likely to favour long-term technological superiority at the national or at the Alliance level.[11]

Strategic distractions. Second, since the humanitarian campaigns of the 1990s, NATO Allies have focused on out-of-area, low-intensity operations in unsegregated environments against inferior adversaries. Tactics, doctrines, strategies, force structures, logistics, procurement, as well as research has been directed to these goals. As a result, NATO Allies have neglected several realms and capabilities: anti-submarine warfare, air-defence, and long-range strike are just some examples.[12]

Great Powers competition. Third, other Great Powers have not remained idle. NATO Allies have put their way of fighting, and vulnerabilities on open display through multiple campaigns and operations – opponents have taken notice, and they've upgraded their plans and capabilities with new technologies. Space and the electromagnetic spectrum, for

10 I. Albrycht, M. Rekowski and K. Mikulski (eds.), *Geopolitics of emerging and disruptive technologies*, The Kosciuszko Institute, Krakow, 2020.

11 Congressional Research Service, "Global research and development expenditures: fact sheet", *Fact Sheet R44283*, Washington, DC, 2020.

12 C. Brose, *The kill chain: defending America in the future of high-tech warfare*, Hachette Books, New York, NY, 2020.

instance, have become more contested because these very opponents and other countries have made targeted investments. As a result, adversaries can now potentially undermine the whole of NATO Allies' military machinery: these realms depend entirely on a command, control and communication (C3) structure through which NATO Allies' armed forces operate.[13]

Accelerated technological change. Fourth, accelerated technological change has also opened new opportunities, including the creation of brand new fields. In such areas, early investments may yield major economic and political returns, including higher financial payoffs, long-term buy-in of customers, and limited competition from adversaries. Artificial intelligence, autonomy and robotics, big data, quantum computing, 5G communications are among such fields. With the advent of these and other relatively new technology, the playing field has been levelled to a certain extent. NATO Allies, in several instances, have been late to the game, failing to recognise the importance of these areas. This explains why some non-NATO countries including China, Israel or South Korea[14] are making major strides in these and other domains.

Disruption and transformation. Finally, the wave of technological change is not only massive, it is also transformative. Disruption and innovation occur everywhere, from the labs of major corporations to the garages of small start-ups; from transnational networks of researchers and engineers to the production plants of both established and raising entrants. Tesla or SpaceX have entered two extremely competitive markets, and in less than a decade, broke through and rose quickly among its competitors: how many other Teslas or SpaceXs will emerge, and where will they emerge? We may be in for some surprises, geographically speaking, to see emerging companies hailing from unexpected countries or continents. But we may also have industrial surprises. If Tesla and SpaceX carried out such feats, can the arms industry do the same?[15]

13 N. D. Wright (ed.), "AI, China, Russia, and the global order: technological, political, global, and creative perspectives. A strategic multilayer assessment (SMA) periodic publication", US Department of Defense, Washington, DC, 2018.

14 NATO Science & Technology Organization, "Science & technology trends 2020-2040: exploring the S&T edge", Brussels, 2020.

15 E. Brynjolfsson and A. McAfee, *The second machine age: work, progress, and prosperity in a time of brilliant technologies*, W. W. Norton & Co., New York, NY, 2014.

Technological superiority and technological revolutions

In order to understand the threat to NATO technological superiority, it is necessary to contextualise, conceptually and historically, the challenge at hand. To a great extent, the world we live in is the product of the steam- steel- and later electricity-based late 19th century Second Industrial Revolution. This era levelled the playing field and ushered in unprecedented wealth creation and accumulation of capital by permitting many countries to enter into industrial production.[16] Progressively, however, the quest for superior performance called for more advanced knowledge which, in turn, soon became an entry barrier for potential competitors. This process accelerated towards the 1960s, with the Third Industrial Revolution, one built on vacuum-tubes, first, and silicon-based microchips, next, along with many other electronics-related technologies. Economies of scale lost out to economies that run on knowledge-intensity.

As a result, it became irrelevant if a country could outcompete its rival in the production of computers if those computers did not outperform its rival's product.[17] Competition became much tighter. Due to the expansion of international trade, industrial specialization of different parts of the value-chain became increasingly predominant. The production of semiconductors is a particularly vivid illustration of this trend: those designing the chips are located elsewhere from those who produce them; those who produce chips use equipment developed in other countries, and those countries in turn rely on software also designed elsewhere. Precision-guided munitions, stealth aircraft design, real-time communications, persistent intelligence, surveillance and reconnaissance would not be possible without the growth of the semiconductor industry. However, the globalization of production, with its emphasis on specialization, has made it more difficult to lead in technology, unless analysis if refracted through the lens of Alliances instead of countries, and comparative advantages can be pursued and exploited more effectively.

This brings us to nowadays when analysts and scholars speak of a Second Machine Age or of a Fourth Industrial Revolution. We are at the potential beginning of a new and major transformation. This revolution will build on robotics and automation, on machine learning for pattern recognition and predictive analytics, on 5G communications for massive real-time transfer of data, as well as cloud and quantum computing for increasing the speed and efficiency of calculations. These, *inter alia*, are generally known as disruptive and emerging technologies. Three considerations are in order.

16 A. Gerschenkron, *Economic backwardness in historical perspective: a book of essays*, The Belknap Press, Cambridge, MA, 1962; A. D. Chandler Jr., *Scale and scope*, The Belknap Press, Cambridge, MA, 1990.

17 S. G. Brooks, *Producing security: multinational corporations, globalization, and the changing calculus of conflict*, Princeton University Press, Princeton, NJ, 2006.

Emerging and disruptive technologies. First, the rise of several emerging and disruptive technologies – from artificial intelligence to quantum computing, hypersonic weapons to 5G networks – has led many to speculate that a new industrial revolution is coming. Whether this is correct will only be known *ex post*. What we do know, *ex ante*, is that there will be both a process of convergence among innovative countries, and a process of divergence between innovative and non-innovative countries.[18] Predicting which countries will lead and which will lag is inevitably difficult. However, we can make some educated guesses about the factors that will play a key role. Because of the knowledge-intensive nature of the current technological transformation, countries excelling in R&D and education are more likely to succeed.[19] An important question concerns the ease of appropriating others' knowledge and know-how. This may determine the shape and intensity of international competition: if barriers to knowledge are high, the gap between the two groups will remain significant. If barriers are low, technological capabilities will be more diffused, with major implications for the structure of international politics.

Technological revolution and long-term change. Second, while the word "revolution" is often associated to sudden changes, technological revolutions have been, in reality, the product of cumulative processes.[20] This is because the adoption and diffusion of technology are slow and complicated, not least because of the need to invest in complementary assets. Deductive logic and available evidence about emerging and disruptive technologies suggest that their effects will be cumulative and this is particularly true for warfare.[21] For instance, machine learning algorithms remain brittle and thus can be easily neutralized by enemy tactical or operational systems. Similarly, quantum computing will require major and increasing investments, and its integration into military forces will require parallel investments.

Technological transition and technology strategy. Third, given the previous two considerations, the challenge for NATO will be two-fold: 1) preserve its scientific, technological and industrial leadership in the so-called Third Industrial Revolution areas; and 2) consolidate its leadership in the so-called Fourth Industrial Revolution domains.

18 T. F. Bresnahan and M.Trajtenberg, "General purpose technologies 'engines of growth'?", *Journal of Econometrics*, Vol.65, No.1, January 1995, pp.83-108.

19 A. Agrawal, J. Gans and A. Goldfarb (eds.), *The economics of artificial intelligence*, University of Chicago Press, Chicago, IL, 2019.

20 J. De Vries, "The industrial revolution and the industrious revolution", *The Journal of Economic History*, Vol.54, No.2, June 1994, pp.249-270.

21 S. D. Biddle, *Military power: victory and defeat in modern warfare*, Princeton University Press, Princeton, NJ, 2004; A. Gilli and M. Gilli, "The diffusion of drone warfare? Industrial, organizational, and infrastructural constraints", *Security Studies*, Vol.25, No.1, 2016, pp.50-84.

The challenge will be a delicate one to navigate. A good number of Allies is dramatically lagging behind in emerging and disruptive technologies. This technology and industrial gap is already creating political friction on issues such as taxation of digital transactions and data regulation. Without a serious attempt to modernize technologically, a two-tiered Alliance could start to take shape, and political difficulties will inevitably arise. In order to understand the challenges ahead, it is useful to look at NATO's potential competitors.

Technological superiority and technological competitors: China and Russia

Any discussion about NATO technological superiority necessarily means talking about Russia and China, its two most likely technological competitors. Threats and challenges also come from other countries, such as Iran or North Korea, as well as from other players, like terrorist groups and insurgents, but the latter are not in the position of questioning NATO technological superiority. China and Russia, however, potentially are.

Russia's technological capabilities. From a technological and industrial perspective, Russia and China complement each other. Simply put, one possesses or is more advanced in the capabilities the other lacks, and where one lags behind, the other makes up for it. More precisely, Russia's scientific, technological and industrial capabilities are degrading, undermined by inefficiency and corruption, and its economy never really mastered electronics.[22] However, thanks to the know-how accumulated during the Soviet times, the Russian industry can still develop advanced weapon systems of the Third Industrial Revolution which many countries, including China, have struggled to produce, such as nuclear-propelled submarines, jet fighters and integrated air-defence systems. Russia has a solid educational system, especially in math and the natural sciences. This, in turn, produces remarkable human capital. However, at this stage, Russia does not seem to possess all the components of the ecosystem required to fully exploit the emerging and disruptive technologies of the Fourth Industrial Revolution. In fairness, even where Russia "excels", there are severe shortfalls and drawbacks. In practical terms, this means that in the next decade or so, Russia may exploit some emerging or disruptive technologies at the tactical or operational level, but it is very unlikely to gain any technological leadership and make any strategic gains from the current technological transformation. The war in Crimea and Eastern Ukraine are testament to this: Russian forces, or their proxies, ingenuously exploited new technologies or capabilities, such as cyber, the electromagnetic spectrum and drones.

22 S. Oxenstierna and F. Westerlund, "Arms procurement and the Russian defense industry: challenges up to 2020", *The Journal of Slavic Military Studies*, Vol.26, No.1, 2013, pp.1-24.

But Russia can hardly claim any lasting technological superiority. Furthermore, the current oil crisis, if it persists longer, will harm Russia's prospects of military modernization.

China's technological capabilities. Conversely, China's scientific, technological and industrial capabilities are significantly more advanced than Russia's in some emerging fields, like 5G communications, quantum computing and artificial intelligence. However, China is not yet on par with Western countries when it comes to traditional technologies, neither commercially nor militarily.[23] Semiconductors are a case in point: the degree of complexity and manufacturing sophistication they require is extreme and despite several efforts, China has not yet mastered their production, nor has it mastered the production of the manufacturing equipment for semiconductors.[24] Similar considerations apply to other high-end, knowledge-intensive industrial products, which China has long struggled to produce, such as aero-engines. Unsurprisingly, China's stealth fighters or nuclear submarines significantly underperform in comparison to international competitors. For the short-to-medium term, it is reasonable to expect that China will continue on two paths. On the one hand, it will keep trying to access, legally and illegally, advanced technologies developed primarily in Western countries, and assimilate them in its domestic economy. On the other hand, it will probably keep injecting investments into emerging and disruptive technologies, where its race to the top is more plausible. Whether China will achieve technological leadership, or not, will depend on a set of factors, including:

- the pace of technological change around the world: faster rates of growth make catching up more difficult;
- whether the nature of the new technologies will be knowledge-enhancing or knowledge-destroying: if new technologies require new skills and machine tools, the follower may be at an advantage, provided it possesses those skills and manufacturing equipment;
- the importance of creativity and innovation in the entire process of technological growth: The Soviet Union proved able to imitate technologies, but then increasingly struggled to innovate. Speculations suggest that China may face the same challenges.[25]

23 S. W. Harold, *Defeat, not merely compete China's view of its military aerospace goals and requirements in relation to the United States*, RAND Corporation, Santa Monica, CA, 2019.

24 S. M. Khan and C. Flynn, "Maintaining China's dependence on democracies for advanced computer chips", *Global China: accessing China's role in the world*, Brookings Institution, Washington, DC, 2020.

25 C. Benedikt Frey, *The technology trap: capital, labor, and power in the age of automation*, Princeton University Press, Princeton, NJ, 2019.

NATO's human-centric technological leadership

As intimated previously, NATO Allies must preserve both their combined leadership in Third Industrial Revolution technologies and consolidate their superiority in the Fourth Industrial Revolution domains. As paradoxical as it may sound to many, any action or initiative geared towards these goals must be centred on individuals.

NATO's strength lies in its human capital: this is not rhetoric, these are facts. Technological superiority is the product of technological assessments, which are made by individuals; it is the result of strategic choices taken by leaders; it is the sum of the work of creative and competent researchers and scientists working in teams where formal and informal rules yield achievements, collaboration and responsibility. Human beings are central in every phase of this process.[26] This is why the NATO 2030 strategy for technological superiority – whether implicit or explicit – must focus on the role of individuals. The more important are the tasks left to human beings which cannot be automated, either because it is uneconomic, or because computers lack human flexibility, ingenuity and dexterity.[27]

Thus, if computers deliver speed, data storage, constant communications and computational power, the strategic role of human beings in conceptualizing strategies and in decision-making ends up acquiring superior importance.[28] Like a high-speed train or a supercar, the machines do the bulk of the work, but human beings are the ones taking key decisions or acting in critical contingencies, in addition to fine-tuning the hardware with the surrounding environment. This is particularly true because even a small mistake caused by the human factor could spell a fatal failure. At the strategic level, human beings can not only decide in what domains to compete in and how to compete, but also what phases to automate: this process is driven by cognitive, cultural, institutional and political factors. There is an additional consideration. Machines are not yet optimized for broad strategic thinking because some inputs cannot be easily turned into digital data and because human beings, in contrast to machines, are superior in conceptualization. There are, however, some obvious risks. First, human beings are subjected to numerous and impactful cognitive biases.[29] Second, current leaders are not educated and trained for the challenges of our era of accelerated technological change. Last, there is a real risk of fragmentation: leaders must possess sufficient technical proficiency to understand possibilities; have in-depth expertise

26 M. C. Horowitz, *The diffusion of military power: causes and consequences for international politics*, Princeton University Press, Princeton, NJ, 2010.

27 A. Gilli (ed.), "The brain and the processor", *NDC Research Paper*, No.5, NATO Defense College, Rome, 2019.

28 A. Agrawal, J. Gans and A. Goldfarb, "The simple economics of machine intelligence", *Harvard Business Review*, November 2017.

29 D. Kahneman, *Thinking fast and slow*, Farrar, Straus and Giraux, New York, NY, 2011.

to gain domain knowledge; and display strategic vision to ponder options and courses of action. As expertise become more and more specialised and technologies less and less understandable to non-experts, it becomes more and more difficult to find individuals who meet all these expectations.[30]

What should NATO do, then?

NATO can support, coordinate, and promote its Allies' efforts and guide them towards the achievement of long-term goals. These are some actionable proposals:

R&D. Research and Development is the lifeblood of future technological, economic, and social growth, as well as security and stability. Over the past two decades, NATO countries have endured several crises: the dotcom bubble, 9/11, the subprime mortgage crisis, and the eurozone crisis; and more recently the invasion of Ukraine and the COVID-19 pandemic. Despite some increases in recent years, NATO Allies have by-and-large, reduced defence funding and, in several cases, reduced non-military R&D funding. This comes at a particularly critical moment because other nations, including NATO's strategic competitors, are massively investing in R&D. At the 2014 Wales Summit, NATO Allies committed to the 2 percent / 20 percent pledge for defence and modernization spending. For the future, NATO Allies could envision a similar measure to apply to R&D. This not only sets a bar for percentage of GDP expenditure on R&D, but also seeks to strategically leverage the Allies' different technological competitive advantages.

Leadership. The challenges NATO Allies face require competent and flexible leaders. For instance, with the introduction of artificial intelligence, "the ultimate challenge is finding people who understand the business as well as the technology and data". While to some this may appear trivial, the reality is that some "people understand the business but don't understand the technology and data […other] people understand the technology and data, but not the business". In such a catch-22 situation, "organizations need people who can connect all three of those circles". This is far from easy, no less so in the world of defence.[31] Strategic-level education, training as well as wider initiatives aimed at increasing the technological quotient of current and future leaders are extremely important, as highlighted by the US National Security Commission on Artificial Intelligence.[32] Within NATO, there

30 A. Asoni, A. Gilli, M. Gilli and T. Sanandaji, "A mercenary army of the poor? Technological change and the demographic composition of the post-9/11 US military", *Journal of Strategic Studies* (forthcoming).

31 Protiviti, *Competing in the cognitive age: how companies will transform their business and drive value through advanced AI,* Protiviti, Alexandria, VA, 2019.

32 E. Schmidt *et. al.*, "Second Quarter Recommendations", *Quarterly Series*, No.2, National Security Commission on Artificial Intelligence, Arlington, VA, 2020.

are several organizations which work on strategic-level education and training, from the NATO Defense College in Rome to the NATO School in Oberammergau.

Strategy. Carl von Clausewitz famously highlighted the importance of strategic genius, which is an extremely rare quality. Improving strategy-making is difficult. Devising strategies in a time of accelerated technological change is even more challenging. Exercises, simulations, and wargames which include new technologies represent a potentially powerful tool to get a handle on this uncertainty. Even tactical exercises can generate important lessons with implications at the operational and strategic level.[33] There is an important repository of expertise within the Alliance in this domain, which could be exploited and expanded. Institutions within NATO, like the NATO Defense College in Rome or the NATO School in Oberammergau, have inherent advantages in wargames and simulation for educational purposes. In other cases, Allied Command Transformation with units such as Joint Analysis and the Lessons Learned Centre are particularly appropriate and fit to run experimental wargames and exercises. Allied Command Operations, in contrast, has permanent oversight over training and operations and possesses an unmatched source of data to test and to experiment.

Organization. No organization can devise the most appropriate strategy or exploit the most insightful wargame if information does no flow easily and quickly. A crucial condition for the free flow of information is empowering human capital. This is the reason why organizations have flattened over the course of the past century. Evolving from the vertical, siloed Second Industrial Revolution corporation, companies have adopted a more horizontal, flexible structure. For military forces, this poses a challenge because a military force is, ultimately, about command. Over the past decades, NATO armed forces have repeatedly and effectively displayed the capacity to adapt, reform and innovate – just like horizontal organizations. For the future, empowering human capital may entail simple solutions such as granting more time to single individuals for experimentation.[34] At Google, for instance, each employee is granted 20 percent of corporate time – 1 out of 5 days a week – to pursue individual projects. This is how Gmail and Googlemaps, among others, emerged.[35] NATO Allies could start adopting similar measures in their Ministries of Defense Research Centers and Educational Institutions, and then progressively extend the principle in other smaller areas.

33 N. Friedman, *Winning a future war: war gaming and victory in the Pacific war*, Naval History & Heritage Command, Washington, DC, 2020.

34 M. Du Sautoy, *The creativity code: art and innovation in the age of AI*, Belknap Press of Harvard University Press, Cambridge, MA, 2019.

35 E. Schmidt and J. Rosenberg, *How Google works*, Grand Central Publishing, New York, NY, 2014.

Grand Challenges. Industrial cooperation is already difficult, when it comes to an armaments program, this is even more so. In an age of accelerated technological change, NATO Allies need to harness their respective scientific, technological and industrial bases, as well as the ingenuity and competence of its human capital. Rather than picking winners, NATO Allies could streamline their different national-level and Alliance-level initiatives and launch Grand Challenges to truly promote disruptive innovation. The recently created pan-European Paris-based Joint European Disruptive Initiative serves as an interesting model.

Creativity and equality. With the change in technology over the past century, we have observed the transition from the Second to the Third and from the Third to the Fourth Industrial Revolutions. We have also witnessed a dramatic rise in inequality. *Average is Over* notes economist Tyler Cowen. NATO's core mission is not directly concerned with welfare inequality; but welfare inequality will have an impact on its core mission. In his legendary *Fleet Tactics*, Captain Wayne P. Hughes noted that, as a World War II teenager, he bought a copy of Jane's *All World's Warships*, and thus became passionate, and later a master, of naval warfare. This is not too different from Bill Gates who unleashed his passion for computing because, quite remarkably, the high school he attended in the late 1960s was among the few in the world that had a computer. Barriers to technology are, however, raising. This means that the pool of potential scientists, scholars, entrepreneurs or researchers risks shrinking in relative, or even absolute terms. For instance, in order to run machine learning algorithms, users need large datasets (which are generally government-owned) and enormous computing power (which only companies can afford).[36] While NATO, as an Alliance, may not have readily available solutions, recognizing this challenge is of the utmost importance for its technological superiority in 2030 and beyond.

Human capital and education. According to an old saying, *those who know do, those who don't teach*. Academic institutions all around the world, and within NATO countries in particular, are under stress. They have so far failed to exploit the digital revolution. Faculty is generally old and not diverse. Students' skills do not become markedly advanced after college. In fact, several companies have even stopped asking for university grades and, in some cases, even degrees: a sign that university-level education is increasingly seen as not useful, effective or as a path to intellectual and professional growth. In other words, higher education is failing its users, students, and the main beneficiary: society as a whole.[37] NATO, alone, cannot fix this problem. However, it is going to pay some of the associated costs. The

36 M. Rasser *et al.*, *The American AI century: a blueprint for action* Center for New American Security, Washington, DC, 2019.

37 C. B. Frey and M. A. Osborne, "The future of employment: how susceptible are jobs to computerisation?", *Technological Forecasting and Social Change*, Vol.114, January 2017, pp.254-280.

student of today is tomorrow's officer and the leader of 2030. For this reason, NATO, in concert with its Allies, can adopt measures which, at the very least, can help generate the human capital it will need. One possible solution is to sponsor more proactive university classes which, in turn, endow students with the skills of the future, including teaming and conceptualization. *Hacking for Defense*, the Stanford University-born innovation class, is an interesting model which could be adopted at almost no cost. The simple idea would be for defence organizations to identify a set number of problems – both at the national and multinational level – they cannot solve and ask universities to provide solutions. Students would learn to work in groups; would acquire relevant team-working skills; and gain more familiarity with the world of technology and defence. There is also no reason why this model could not be converted into a competition among NATO countries' universities. In early 2021, NATO successfully experimented with this concept, by launching its first policy Hackaton, "New Ideas for NATO 2030".

Conclusion

The year 2030 is not tomorrow, nor is it the day after tomorrow: it is yesterday. Our future is shaped by what we have already done. When we think about the future, we are not thinking about the future, we are realizing that we have, for too long, not thought about the future. Technological superiority is a fundamental asset in a world which remains violent, unjust, crisis-prone and dangerous. Technological superiority will not ensure victory and success, but it can facilitate it. For its entire history, NATO Allies have enjoyed a position of technological leadership. Such leadership is currently coming under threat. A multiplicity of factors account for this. The game, however, is not yet set. NATO Allies can still preserve and even extend their technological superiority. This is the logic underpinning NATO 2030, as the Secretary General highlighted: NATO Allies can still maintain their technological edge, and this requires, *inter alia*, "to develop common principles and standards for new technologies, and to enhance cooperation between allies in areas like joint research and development".[38] Such coordinated action at the national and Alliance-wide levels will, ultimately, empower NATO Allies' human capital – which as of now, is the main source of the entire Alliance's competitive advantage.

38 S. Sprenger, "NATO chief seeks technology gains in alliance reform push", *Defense News*, 9 October 2020.

2

Adapting NATO to grey zone challenges from Russia

Marc Ozawa *

NATO is facing a growing intensity of grey zone challenges. Both states and non-state actors continue to develop new methods to disrupt, confuse, and disable in order to advance their strategic interests. These tactics, taking place in the "grey zone" – or below the threshold of traditional warfare – present a growing challenge for the Alliance not only as a threat to NATO operations but also in terms of undermining Alliance cohesion and confidence in the democratic institutions that are the foundation of allied societies. These challenges were identified in the London Leaders Meeting and highlighted by Secretary General Stoltenberg as part of the "new normal" to which NATO must adapt.[1] At the launch of NATO 2030, Secretary Stoltenberg discussed the need for NATO to address emerging, non-conventional threats and pointed to NATO's dual track approach towards Russia.[2]

In conjunction with the contributions made by participants of the Secretary General's Reflection process, this chapter examines grey zone challenges, particularly those posed by Russia, and what NATO can do in response. It addresses the following questions: What kind of grey zone threats is NATO likely to experience in the near to midterm? How effectively has NATO responded to grey zone tactics, and what strategies would position NATO favourably in the future? Finally, how has COVID-19 impacted NATO's grey zone environment?

Although the grey zone applies to actions taken by multiple states, Russia presents a particular concern for the Alliance ever since the illegal annexation of Crimea, and as such,

---

* The author would like to thank Michael Rühle for his feedback and comments on earlier drafts.

1 NATO, "London Declaration", (accessed 2 February 2021), http://www.nato.int/cps/en/natohq/official_texts_171584.htm; NATO, "NATO2030", (accessed 6 January 2021), http://www.nato.int/cps/en/natohq/176155.htm

2 NATO, "Remarks by NATO Secretary General Jens Stoltenberg at the Public Launch of the NATO 2030 Expert Group's Report", (accessed 2 February 2021), http://www.nato.int/cps/en/natohq/opinions_179952.htm

it will be the focus of this chapter. However, the analysis may also be applied to other actors such as China, the main difference lying in the type of grey zone behaviour that each actor demonstrates. For instance, whereby Russia may currently exhibit an emphasis on disinformation operations, China undoubtedly represents a greater potential economic challenge for the Alliance.

The main conclusion is that NATO must further adapt and develop an expanded toolkit for countering aggression.[3] As Secretary General Stoltenberg has emphasized, adaptation has been and must continue to be a priority for NATO.[4] With respect to the grey zone, there are at least two dimensions required for this. The first is fundamental, namely a revision of NATO's mandate to deal with conflict in the grey zone. This is in line with what the Secretary General has expressed. The Reflection Group's assessment likewise advocated for a new Strategic Concept or similar strategic document.[5] The second dimension is both tactical and operational – establishing concrete steps that NATO can take to expand its current approach. For the tactical steps advanced in this chapter to be achieved, NATO would need to devote additional resources to grey zone related initiatives along with bolstering its partnership activities. Although partnerships will be examined in a subsequent chapter, we argue here that there is a need to both deepen existing partnerships and expand the framework of NATO's partnerships to include more stakeholders in addition to the EU, Partnership nations and current institutional partners.

The recommendations presented in this chapter would allow NATO to participate more actively along the entire grey zone continuum, branching out from purely military affairs (in which NATO has arguably risen to the challenge presented by Russia) into other areas such as political and economic security. Moreover, the measures we advance support all three of the adaptational goals put forth in the Secretary General's vision for NATO 2030 in terms of strengthening NATO militarily, politically and globally.[6]

The chapter is divided into four sections. The first section explains what "grey zone" activities are in the context of NATO by comparing Western and Russian conceptions of the entire grey zone. The second introduces the challenges that Russian grey zone tactics have presented to NATO. The next identifies and critiques the steps NATO has taken to date. Finally, we offer recommendations for NATO in dealing with future grey zone challenges from Russia and beyond.

3 The workshop that informed this paper principally focused on Russia as the main source of aggression in a grey zone context, but some comparative examples from China were also included.

4 NATO, "Secretary General addresses the NATO Parliamentary Assembly – Adapting NATO for 2030 and beyond" (accessed 2 February 2021), http://www.nato.int/cps/en/natohq/news_179663.htm

5 NATO, "NATO2030".

6 NATO, "NATO2030".

Western and Russian perspectives of the grey zone

Before proceeding, it is important to clarify what is meant by the "grey zone", which is often used interchangeably with "hybrid" warfare.[7] There are two aspects that demand attention – the first is from a NATO perspective, and the second is from a Russian understanding of the term. Concerning the former, there is a conceptual debate among Western scholars about what constitutes activities in the "grey zone".[8] Broadly, the grey zone is understood to be conflict that takes place short of the threshold of conventional warfare. This definition resembles hybrid warfare, which occupies the same area. While there is some disagreement about the time horizon of grey zone and hybrid warfare (grey zone tactics may be less strategic than hybrid approaches and thus more short-term), a more widely used distinction concerns the type of actor.[9] Typically, actors in the grey zone are states, in contrast to hybrid actors that may be either state or non-state actors. For the purposes of this analysis, the term grey zone is more relevant to the discussion because Russia is a state actor and NATO, being an Alliance of states, conducts operations on behalf of states.

In order for NATO to plan for grey zone challenges posed by Russia, it is also important to understand what Russia considers to be the grey zone. The term *seraya zona*, or grey zone in Russian, is a new term in Russian debates insofar as it relates to warfare. The term is understood to be a US-Western conceptualization of what, in Russian, may be referred to as *nelineinaya voina*, or non-linear warfare.[10] The Russian term encompasses all means that are not considered to be traditional warfare. Yet the end goals of both non-linear and traditional warfare are still political in nature – to orchestrate political change for the adversary.[11] Non-linear warfare is not a new term. It is a practice going back to the Cold War, and it is for this reason that Russian analysts do not view grey zone conflict as anything new.[12] In Russian debates, the more important distinction is the type of conflict along a continuum ranging from social and economic to diplomatic and political.[13] The

7 "Gray Zone Project | Center for Strategic and International Studies" (accessed 21 January 2021), https://www.csis.org/grayzone

8 A. Dowse and S. Bachmann, "Explainer: what is 'hybrid warfare' and what is meant by the 'grey zone'?", The Conversation (accessed 21 January 2021), http://theconversation.com/explainer-what-is-hybrid-warfare-and-what-is-meant-by-the-grey-zone-118841

9 A. Patalano, "When strategy is 'hybrid' and not 'grey': reviewing Chinese military and constabulary coercion at Sea", *The Pacific Review*, 9 January 2019.

10 V. N. Startsun, "Понятие 'Серойзоны'", *Voenniye Aspekty Mezhdunarodnogo Prava*, Vestnik Voennogo Prava, 340, No.116, March 2018, pp.77-86.

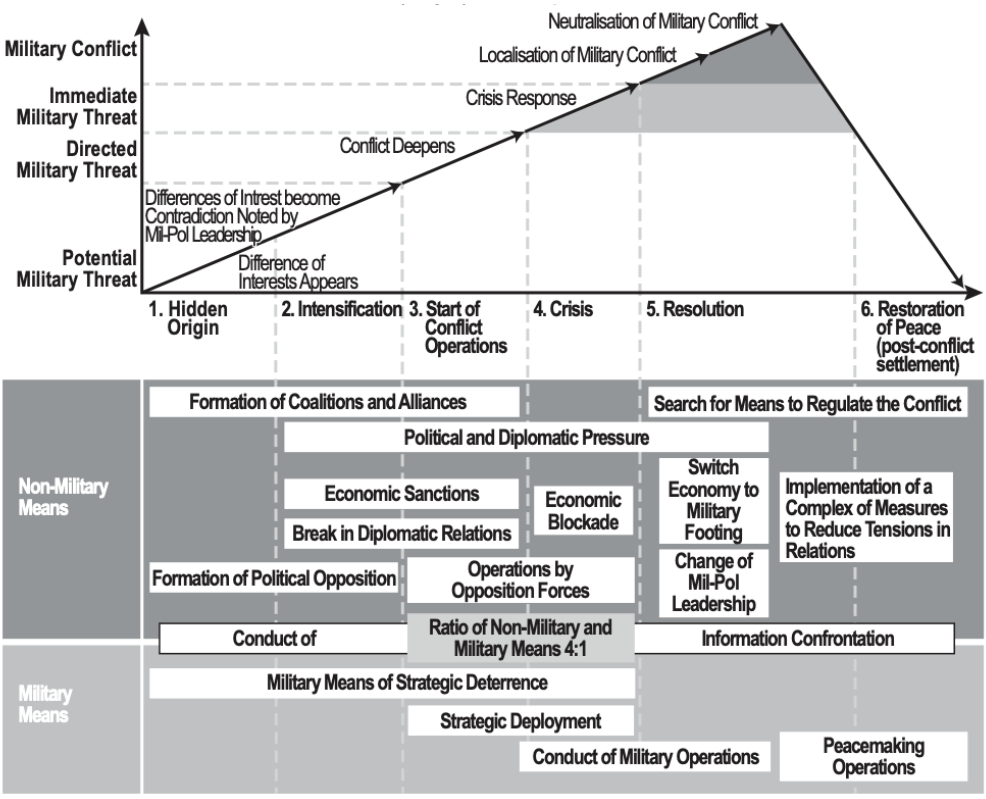
11 M. Galeotti, *Russian political war: moving beyond the hybrid*, 1st edition, New York, NY, Routledge, 2019.

12 P. Pomerantsev, "How Putin is reinventing warfare", *Foreign Policy* (blog), accessed 21 January 2021, https://foreignpolicy.com/2014/05/05/how-putin-is-reinventing-warfare/

13 V. Khudoleev, "Военная наука смотрит в будущее", Krasnaya Zvezda, 26 March 2018, http://archive.redstar.ru/index.php/component/k2/item/36626-voennaya-nauka-smotrit-v-budushchee?attempt=1

following Figure, from a report accompanying General Gerasimov's remarks to the Russian Academy of Military Sciences, illustrates this conceptual framework.

Figure 1. Role of Non-military Methods in Deciding Inter-state Conflicts – Basic Phases (Stages) in Development of Conflicts



Source: D. Johnson, "Russia's Conventional Precision Strike Capabilities, Regional Crises, and Nuclear Thresholds", Livermore Papers on Global Security, No.3, February 2018.[14]

When Russian analysts invoke the terms *seraya voina* or *gibridnaya voina* (hybrid warfare), they are responding to Western debates about what Russian military strategists consider to be non-linear warfare. Practically speaking, the difference between the Cold War concept

14 D. Johnson's translation of original by V. Gerasimov, "Tsennost' Nauki v Predvidenii", *Voenno-Promyshlenny Kur'er*, 27 February 2013.

and that of today is the role of technology as an enabler of non-linear warfare making certain tactics more attractive and likewise, more frequently used by Russia.

With both perspectives in mind, this chapter defines grey zone conflict for NATO as any approach that Russia may use against NATO that falls below the threshold of conventional warfare. This includes state-initiated hybrid warfare.

External and internal challenges

For sake of linking this analysis to a broader security debate, we distinguish four categories of grey zone tactics which currently affect NATO and individual member states. The first three are external in nature, including information warfare, asymmetric approaches and economic coercion. These three types of grey zone challenges are synonymous with established analyses on Russian grey zone warfare.[15] Additionally, there is a fourth category that is internal to NATO – the institutional and resource constraints that challenge the Alliance's ability to respond to the first three challenges.

Information warfare. Information warfare refers to the manipulation of information and the promotion of certain destructive narratives. The theatres of operation most commonly used are social media and an eco-system of state-linked news and information sources. The purpose of information campaigns against NATO is to sow division, confusion, and to damage the credibility of the Alliance. Information warfare may also be used to undermine democratic societies by interfering in the election process. The purpose will be to orchestrate conditions to influence election outcomes such that Kremlin-favoured politicians and parties will be elected. This type of information warfare ranges from what is known as "psychological operations" in the intelligence services to actual tampering with election infrastructure to manipulate voting counts.[16] It may also come in the form of campaign financing, either through direct contributions (usually through business intermediaries) or providing indirect loans to political campaigns through Kremlin linked banks. Information warfare may also undermine trust in democratic governance by sowing division along social and ethnic cleavages.

Asymmetric approaches. Second, asymmetric approaches may or may not include kinetic activities. Most examples fall below kinetic engagement on the spectrum of conflict. They can include cyber-attacks and the targeting of critical infrastructure such as communication

15 J. Schauss *et al.*, "What works: countering gray zone coercion", *CSIS Briefs*, Center for Strategic and International Studies, Washington, DC, July 2018, variously described as hybrid warfare, irregular warfare, asymmetric warfare, or political warfare (and in this brief, gray zone challenges).

16 T. Rid, *Active measures: the secret history of disinformation and political warfare*, Illustrated edition, Farrar, Straus and Giroux, New York, 2020.

or energy systems. One of the first examples of asymmetric approaches was the 2007 cyber-attack on Estonia's capital, Tallinn, in response to the government's decision to move a Soviet war memorial. This enraged Russian leadership and some of the Russian-speaking population of Estonia.[17] For twenty-two days, the country was bombarded with cyber attacks that crippled financial, government, and communications operations.

Asymmetric approaches may also take the form of covert operations to exert political influence. This can include the use of private militaries or unmarked soldiers such as the "little green men" that appeared in Crimea.[18] It may also manifest in cyber-attacks on election infrastructure as opposed to public opinion manipulation through information warfare. While US intelligence authorities assessed that Russia held back some of their capabilities during the 2016 elections, Microsoft has reported that attacks on election staff and infrastructure has become much more sophisticated compared to 2016.[19]

Economic coercion. With respect to economic coercion the tools have usually been access to energy supplies, investments, and financial opportunities. This type of coercion may target a state, company, or individual, but even when directed at individuals, the ultimate goal is broader in scope. According to a study from the Swedish Defence Research Agency, Russia has a history of applying economic pressure through the access of natural gas to eastern European countries by either cutting off supplies or through the sale price.[20] The study concludes that the more favourable a country's policies are towards Russia, the lower the prices and better terms of contract are offered.[21] When individuals are engaged in grey zone economic coercion, it is usually because they carry political sway in their countries and can advocate for Russian sponsored projects, such as pipelines. This kind of pressure serves the purpose of lobbying a position that benefits Russia from a foreign policy perspective.

Resources and prioritization. The final type of challenge is one of resources and prioritization. Financial resources to support NATO operations have always presented a challenge for the Alliance. The issue of the two percent pledge aside, how much of NATO's organizational budget is sufficient - for taking the steps and implementing programs for

17 "How a cyber attack transformed Estonia", BBC News, 27 April 2017, sec. Europe, https://www.bbc.com/news/39655415 (accessed on 21 January 2021).

18 "All roads lead to Ukraine in Putin's global hybrid war", Atlantic Council, 5 January 2021, https://www.atlanticcouncil.org/blogs/ukrainealert/all-roads-lead-to-ukraine-in-putins-global-hybrid-war/

19 D. Sanger and N. Perlroth, "Russian intelligence hackers are back, Microsoft warns, aiming at officials of both parties", *The New York Times*, 10 September 2020, https://www.nytimes.com/2020/09/10/us/politics/russian-hacking-microsoft-biden-trump.html (accessed on 14 September 2020).

20 R. L. Larsson, *Russia's energy policy: security dimensions and Russia's reliability as an energy supplier*, Swedish Defence Research Agency (FOI), Stockholm, 2006.

21 M. Ozawa and I. A. Iftimie, "Russia's energy policy. Dependence, networks and special relationships", *NDC Research Paper* No.13, NATO Defense College, Rome, November 2020.

countering grey zone threats – is another question, one of resource prioritization. NATO's historical legacy as a military organization makes military operations an easier candidate for financial prioritization compared to potential new programs, initiatives and centres directed at grey zone challenges. Furthermore, because different members maintain varying views on the level of threat posed by Russia, the lack of unified political will may present an additional obstacle. Those member states who joined NATO after the Cold War generally have a greater threat perception of Russia. Likewise, the same states, particularly those in the Baltic Region, have the most experience with Russia in the grey zone, their perceptions conditioned by the experience of Soviet domination during the Cold War, sharing territorial borders with Russia, and their relative power asymmetry. Conversely, many West European states have maintained positive economic and cultural relations with Russia even during the Cold War. While recognizing the challenges posed by Russia, member states in southern Europe are more focused on other issues besides Russia such as terrorism and migration. This plurality of views on Russia within the Alliance can understandably create obstacles in arriving at consensus decisions on resource prioritization and opportunities for Russia to exploit those differences.

What all of these grey zone challenges have in common is that they take advantage of the vulnerabilities of NATO's decision-making processes and those of democratic societies. Authoritarian states are better able to safeguard against information warfare and some types of asymmetric approaches because of the grip they maintain on information.

An emerging prioritization of the grey zone within NATO

NATO's responses to grey zone challenges have been swift and consequential, yet there is still work to be done.[22] What follows is a series of measures that NATO has taken in response to grey zone challenges presented by Russia. They were identified and implemented in 2014 after Russia's illegal annexation of Crimea. While these responses move NATO in the right direction, it is clear that grey zone conflict is on the rise and will be a permanent feature of NATO's security environment for the foreseeable future. This suggests that accomplishments must continue to be supported and even expanded. It will require persistence to stay focused on the threat and further adapt as adversaries' strategies and tactics change.

Information-sharing and exercises. In response to grey zone threats, NATO has created the Joint Intelligence and Security Division (JSID) for intelligence sharing across

22 M. Rühle and C. Roberts, "NATO's response to hybrid threats", in M. Ozawa (ed.), "The Alliance five years after Crimea: implementing the Wales Summit pledges*"*, *NDC Research Paper* No.7, NATO Defense College, December 2019, p.62.

the Alliance. This has expanded NATO's ability to gather, analyse and share intelligence. Although NATO members have always had the option of sharing intelligence with one another, the new division has streamlined the process and provided a dedicated hub for aggregating and disseminated information directly aimed at countering grey zone coercion.

With respect to disseminating grey zone tactics to military operations,[23] the incorporation of hybrid elements into NATO exercises has also been helpful albeit less visible. The value of these measures will become more apparent in the event of an actual military attack that incorporates grey zone elements. As grey zone tactics change, NATO must likewise stay alert to this evolution and constantly recalibrate military exercises accordingly.

Resilience. The effort made in the field of resilience is another important step because it can potentially thwart the effects of non-kinetic attacks. Although not directed solely at grey zone challenges, in 2016 NATO began implementing a series of "baseline requirements",[24] which aim at promoting societal resilience at the state and local level. As agreed at the 2016 Warsaw Summit, these include: "(1) assured continuity of government and critical government services; (2) resilient energy supplies; (3) ability to deal effectively with uncontrolled movement of people; (4) resilient food and water resources; (5) ability to deal with mass casualties; (6) resilient communications systems; and (7) resilient civil transportation systems".[25]

The effects of these guidelines are difficult to measure and more long-term in nature. However, the 2020 US election is but one instance that points to institutions, if not society as a whole, appearing to have become more resilient to Russian influence operations. For example, whereby the United States Senate Select Committee on Intelligence catalogued the steps Russia took in order to sway the presidential election to favour Donald Trump in 2016,[26] the former director of the US Cybersecurity and Infrastructure Security Agency (CISA) declared the 2020 election as "the most secure in American history" in part because of lessons learned from the previous election.[27] What fractures that have created chaos in the aftermath of the US election are more domestic in nature, but they have been exploited by Russia.

23 NATO, "NATO's response to hybrid threats", http://www.nato.int/cps/en/natohq/topics_156338.htm (accessed 13 January 2021).

24 M. Rühle and C. Roberts, "NATO's response to hybrid threats".

25 "Resilience: the first line of defence", *NATO Review*, 27 February 2019, https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html

26 "Publications | Intelligence Committee", accessed 13 January 2021, https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures

27 D. E. Sanger and N. Perlroth, "Christopher Krebs hasn't been fired, yet", *The New York Times*, 14 November 2020, https://www.nytimes.com/2020/11/13/us/politics/christopher-krebs-election-security-trump.html

The problem of attribution. Attribution is the process of tracking the steps of a perpetrator and then assigning them to an individual, group, or entity. It is not always straightforward. Attributing an attack is fraught with varying degrees of precision. As such, it is not an exact science and can provide adversaries a modicum of deniability. This can present a dilemma for NATO. NATO members did, however, come to an agreement at the 2016 Warsaw Summit that hybrid attacks in the grey zone could potentially trigger Article 5.[28]

Although the Warsaw Summit communiqués was a positive step insofar as it connected attacks in the grey zone to NATO security guarantees, in practice, collective attribution has been elusive.[29] The Reflection Group report also arrived at this conclusion stating that "NATO Allies must adhere to the common guidelines agreed at NATO when formulating security and defence-related national-level policies toward Russia, and must clearly and consistently communicate the indivisibility of the security of the Euro-Atlantic area, as unanimously expressed in Summit communiqués or, when cyber or other incidents are involved, in common attribution".[30] This presents an internal challenge for NATO with respect to unity and political will.

Although there remains the challenge of "collective attribution", one interesting case could represent a step towards collective attribution for at least some member states. In the Skripal case,[31] sixteen Allies, NATO, and the EU joined in not only attributing Russia publicly as the perpetrator but also in expelling Russian diplomatic staff inflicting a high penalty for Russia's actions.[32]

NATO-EU cooperation and knowledge centres. NATO has also cooperated with the EU primarily working through informal interactions at the staff-to-staff level with projects (playbooks and operational protocols) to help align responses. Following the 2016 NATO-EU Joint Declaration, seven areas for enhancing cooperation were identified. Of these, hybrid threats are listed first, which signals the importance of grey zone related actions.[33] In fact, four out of seven areas directly relate to the grey zone including cyber security,

28 NATO, "Warsaw Summit Communiqué – issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8-9 July 2016", (accessed 6 January 2021) http://www.nato.int/cps/en/natohq/official_texts_133169.htm

29 L. Morris *et al.*, *Gaining competitive advantage in the grey zone*, RAND Corporation, Washington, DC, 2019.

30 NATO, "NATO2030".

31 In March 2018, two Russian nationals allegedly operating on behalf of Russia's military intelligence organization, the Main Directorate of the General Staff (GRU), attempted to assassinate a retired Russian double agent, Sergei Skripal, in the English town of Salisbury with the nerve agent Novichok. It ultimately resulted in the poisoning of Skripal, his daughter, and three other British nationals, one of whom died.

32 A. Chughtai and M. Petkova, "Spy row diplomatic expulsions", https://www.aljazeera.com/news/2018/4/3/skripal-case-diplomatic-expulsions-in-numbers (accessed 21 January 2021).

33 "EU-NATO Cooperation – Factsheets", https://eeas.europa.eu/headquarters/headquarters-homepage/28286/eu-nato-cooperation-factsheets_en (accessed 15 January 2021).

defence industry research, and exercises.

Perhaps the most visible product of this growing cooperation is the formation of a new hub for hybrid threats. In 2017, NATO and the EU joined in the Finland-led European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). This is "an independent, network-based international organisation countering hybrid threats".[34] The Hybrid CoE brings together representatives from NATO and the EU as well as outside organizations, academics, and experts to exchange ideas and inform their respective organizations of the changing nature of threats. The centre publishes studies to inform the public and shed light on hybrid tactics employed by adversaries. Although the Hybrid CoE is still in relative infancy, one of its most important functions is that it offers a venue for interactions removed from the distractions (and constraints) of Brussels.

NATO has also created its own centres of excellence on topics of growing importance in grey zone tactics. Among them are the NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE) and the NATO Energy Security Centre of Excellence (NATO ENSEC CoE). These bodies assist in supporting situational awareness and fostering unity and political will among the Allies. Like the Hybrid CoE, both the CCDCoE and the NATO ENSEC CoE publish studies informing practitioners, policy makers, and the analysts community on grey zone related topics. From a NATO perspective, not only does this contribute to building organizational and societal resilience, it also helps to adapt and plan for the future through maintaining a current and forward-looking orientation concerning grey zone coercive tactics. Beyond the CoEs, NATO's Communications and Information Agency (NCIA) shows promise for supporting NATO's strength in the cyber domain.

Additionally, not all member states have equal cyber capabilities and the resources for countering grey zone tactics. Therefore, offering support to member states through the creation of Counter-Hybrid Support Teams (CHST), is another positive step. Whereby the NCIA helps to build long-term human capital within NATO, the CHST may be deployed rapidly to assist Allies at their request.

Expanding organizational awareness. In addition to the formation of knowledge centres, NATO has taken steps to cultivate the diffusion of knowledge within the organization. The first example is the expansion in the types of meetings among the Allies. This occurs by bringing in advisers and national security staff rather than solely heads of state and defence ministers.[35] NATO has also brought new knowledge from the outside, ensuring that it is transmitted and discussed to a broader audience within the organization, from the

34 "Hybrid CoE – The European Centre of Excellence for Countering Hybrid Threats", https://www.hybridcoe.fi/ (accessed 15 January 2021).

35 Rühle and Roberts, "NATO's Response to Hybrid Threats".

political level through to the managerial and tactical levels. This process may eventually carry information through to national militaries and government agencies over time. It is an important yet deceptively simple step that promotes subject awareness throughout NATO for several reasons. The first is the incorporation of a wider pool of information from relevant practitioners and academics, both of which are needed in order to understand and formulate counter measures and strategies for dealing with grey zone challenges. The next is in NATO's ability to identify grey zone attacks through greater situational awareness. And finally, expanding the list of participants within NATO can help to raise not only awareness but also facilitate the building of political support among member states.

While bringing in new ideas and distributing information within the organizational structures, these same groups will need support to act once political decisions are made. To this end, NATO has created new teams and staff positions dedicated to grey zone related areas such as innovation-technology issues and combatting disinformation.[36] Within NATO Headquarters, the formation of the Emerging Security Challenges Division (ESC) in 2010 was also an important step in this regard, notwithstanding the obstacles of funding and recruiting new staff particularly in a resource-strapped environment.

Engaging the private sector. While NATO has made progress in engaging the private sector, the response could be stronger in light of the demands that grey zone tactics have presented. There is the need to further engage with social media, technology infrastructure providers, which NATO currently conducts through ACT and ad hoc workshops and meetings at NATO Headquarters. This could, however, be expanded, and as one Microsoft executive pointed out, many of these companies have representative offices in Brussels and have interest to liaise and work with NATO.[37] Thus, there is a missed opportunity when these companies are not regularly engaged. A major obstacle to regular engagement with technology stakeholders has been the issue of security clearances. If NATO Allies prioritized engagement with partners, not only in the private sector but also with the EU and partners countries, mechanisms could be developed for overcoming this issue. For example, contractor companies such as Microsoft participate in programs that require security classification at the national level through compartmentalised offices. These national public-private partnerships could provide a model for future NATO engagements with the private sector.

36 *Ibid.*

37 Non-attributed, "Expert comments from NATO Defense College Workshop 'Adapting NATO to future grey zone challenges'", Rome, 24 September 2021.

NATO 2030 and preparing for an ever-advancing goalpost

The grey zone presents the Alliance with an array of challenges that may not be new for NATO but are nonetheless demanding. If NATO expands support and properly resources the initiatives it has already taken, this will do much to assist efforts in countering grey zone tactics by making NATO, member states, and Partners more situationally aware, resilient, and adaptive. However, the danger of having created new programs is that it may give the impression of having already solved the challenges posed by the grey zone. And in this case, the challenges are complex and long-term. The steps that NATO has taken must continue to be supported, developed and re-evaluated in order to be truly effective especially given the fact that results may be difficult to measure and could take years to be realized. It is also critical for the Alliance to take a definitive position on whether it can counter and prepare for new security challenges without distracting from its core military defence *raison d'être*. This may be resolved if and when a new Strategic Concept comes to fruition.

The conceptual debate about what activities constitute "grey zone" challenges for NATO should be resolved. More than just a question of semantics, it has tangible implications for what NATO can do and how the Alliance may respond to conflict in the grey zone by ensuring that the steps NATO will take are fit for the evolving needs. A lack of clarity can may treat all grey zone challenges as equally important, which is problematic when prioritizing resources. Moreover, the longer it takes for NATO to respond to future challenges, the more difficult it may become to effectively counter the next generation of grey zone operations, particularly those that target domestic politics, NATO cohesion and democratic institutions.

In order for NATO to achieve what it set out to accomplish in the 2014 Wales Summit Declaration, it also needs to prioritize the funding of grey zone related initiatives. This will require raising awareness of the importance of grey zone challenges among member states. This in itself will present a challenge in light of the COVID-19 pandemic as nations become more strapped for cash under increasing economic distress.

In addition to what NATO has already done, another step could be the creation of a unit dedicated to countering foreign election meddling through informing and coordinating the responses of social media companies and other private sector stakeholders such as tech companies and NGOs. Furthermore, NATO could develop performance metrics for the effectiveness of knowledge centres, response forces, and military exercises. The ability to demonstrate positive results would help to sustain institutional and political support among member states.

Finally, the engagements with Partner countries and institutions in recent years have been a positive development, but they could be further expanded. NATO might increase

the array of activities across the spectrum of grey zone challenges with partners particularly in the areas of information exchange, innovation, and inter-organizational cooperation. In order to work more effectively with other institutions such as the EU, it is imperative to build mechanisms for overcoming the classified information wall. To this end, national best practices on how to engage with the private sector could provide lessons for NATO.

3

From NATO's partnerships to security networks *

Thierry Tardy

NATO's partnerships have evolved a great deal over the last 20 years, in terms of their objectives, their institutional design, the partners involved, and the way partnerships are being operationalized. Back in the 1990s, partnerships were largely intended to anchor Eastern European countries to the West and transfer NATO standards to the MENA region. When NATO became much involved in stabilization operations (especially in Afghanistan), partnerships then focused on establishing links with countries or institutions that would offer the material resources to share the crisis management burden. By defining cooperative security as one of NATO's core tasks, the 2010 Strategic Concept gave greater prominence to partnerships.

In 2021, NATO *de facto* reaches out to three categories of partners, through partnerships which are more or less well-established with: states (in four geographical groupings: Partnership for Peace (PfP)[1], Mediterranean Dialogue (MD)[2], Istanbul Cooperation Initiative (ICI)[3], and Partners across the Globe (PaG)[4]); institutions such as the United Nations or the European Union; and non-state actors (non-governmental organizations, private entities, etc.).

A lot has been achieved through partnerships, and most of them have been favourable for NATO's policy and strategic posture but they have also met with a number of challenges.

Over the last decade, partnerships have become less central than they were when

---

* The author is grateful to Chloé Berger, Ruben-Erik Diaz-Plaja, Tomáš Šindelář and Veronica Rodrigo for their comments on earlier drafts of the text.

1 The PfP counts 20 countries: Armenia, Austria, Azerbaijan, Belarus, Bosnia and Herzegovina, Finland, Georgia, Kazakhstan, Kyrgyzstan, Ireland, Malta, Moldova, Russia, Serbia, Sweden, Switzerland, Tajikistan, Turkmenistan, Ukraine and Uzbekistan.

2 The MD counts 7 countries: Algeria, Egypt, Israel, Jordan, Mauritania, Morocco and Tunisia.

3 The ICI counts 4 countries: Bahrein, Kuwait, Qatar and the United Arab Emirates.

4 The PaG counts 9 countries: Afghanistan, Australia, Colombia, Iraq, Japan, Republic of Korea, Mongolia, New Zealand, and Pakistan.

enlargement and operations were essential drivers for cooperation, and as priorities have shifted following NATO's renewed espousal of collective defence from 2014. NATO's current design around Deterrence and Defence on the one hand, and Projecting Stability on the other, can be interpreted as a sign that cooperative security, and thus partnerships, have lost preeminence.

While launching the NATO 2030 process in June 2020,[5] NATO Secretary General stated that "one of the purposes of NATO 2030 is to look into how we can further strengthen partnerships".[6] And indeed both the *political* dimension of the Alliance and its *global* reach – two of the three avenues to be explored by the reflection process – make partnerships a key element of the discussion. What does a more political Alliance mean for partnerships? How can partners be involved in NATO's global approach? Are partnerships not instrumental for a more effective Alliance, at the three military, political, and global levels?

This paper aims to examine NATO's partnerships in the context of the NATO 2030 process. It first looks at some of the current characteristics of partnerships, it then identifies challenges, and finally looks forward with some strategic-level considerations or recommendations.

Characterizing partnerships

At least four key features of partnerships inform the discussion on potential developments and associated constraints.

Heterogeneity. Partnerships need to serve a purpose. They are about a) material or b) political/ideational gains, or both. Material gains include: access to information, capabilities, or territory; interoperability; visibility, profile (for example, partnering with a military or a humanitarian actor can help shape one's own identity as a military or humanitarian actor). Political/ideational gains include: political clout (through power aggregation); influence (over a partner); stability (in a region that matters to partners); normative agenda setting (for example before NATO's enlargement or more generally through good governance activities); trust (through socialization); legitimacy (for example by getting a UN Security Council resolution authorizing an operation).

5 The NATO 2030 process was launched by NATO Secretary General in June 2020 following a mandate by Allies at the December 2019 London Leaders Meeting. It is about thinking through the future of the Alliance by *inter alia* looking at its military, political, and global dimensions. It is to be concluded by the 2021 NATO Summit. https://www.nato.int/cps/en/natohq/176155.htm

6 Remarks by NATO Secretary General Jens Stoltenberg on launching #NATO2030 – "Strengthening the Alliance in an increasingly competitive world", 8 June 2020.

There are also different types of partnerships, based on how strategic *versus* operational they are, geographical *versus* functional, or based on the types of partners – states, international organizations and/or non-state actors. The form that partnerships take varies depending on the degree of interaction and institutionalization of the links between partners, ranging from political dialogue to joint operations, including information-sharing and capacity-building.

These various elements suggest that partnerships are heterogenous in their formats and objectives. They offer a wide range of options, goals, and ruling principles, which make them difficult to apprehend in general terms. As an example, political dialogue between NATO and a third country or institution on the effect of climate change, or NATO working with the UNHCR in response to a natural or man-made disaster are arguably different from NATO operating jointly with third countries in kinetic operations; partnering with a third country in Central Asia is politically and practically different from partnering with the EU or the World Health Organization. This raises questions about the meaning of "partner" or "partnerships", as well as about defining criteria that lead to becoming a partner or accepting a new member in an existing partnership.

Geopolitics and adaptation. In many ways the history and nature of NATO's partnerships tell the story of the Atlantic Alliance, its evolving missions and the environment in which it operates.[7] Following the end of the Cold War, as NATO enlarged, it moved away from the Euro-Atlantic area and diversified its missions, and has increasingly partnered with third states as well as with other security and defence actors.[8]

In this sense, partnerships have mirrored both the evolving security environment and the means of NATO's adaptation. More specifically, the creation of various partnership frameworks in the 1990s (starting in 1994 with the Partnership for Peace and the Mediterranean Dialogue) came as a response to profound changes in the international system and, as far as NATO was concerned, the shift away from collective defence to crisis management and cooperative security. In the same vein, reaching out to partner countries and other international security institutions – including the United Nations and the European Union – allegedly allowed NATO to be more effective and congruent with its environment.

Seeing partnerships as reflections of the evolving nature of the security environment as well as instruments of adaptation is important to our analysis as we look forward; it

7 See D. Yost, "NATO and international organizations", *Forum Paper* No.3, NATO Defense College, Rome, 2007.

8 Scholars talk about various waves, or streams, of partnerships since the end of the Cold War; see T. Flockhart (ed.), "Co-operative security: NATO's partnership policy in a changing world", *DIIS Report*, Danish Institute for International Studies, 2014; M. Kaim, "Reforming NATO's Partnerships", *SWP Research Paper*, Berlin, 2017.

suggests that partnerships carry a strategic dimension, that tangible results are practically never achieved if the politics are not there, but also that partnerships must be approached in an open, non-static, manner. It follows that for any security institution having good (or effective) partners is an integral part of the institution's strategic vision or posture. For NATO, it also means that the post-2014 shift back to collective defence questions the very notion of partnership on, at least, two levels:

- to what extent are existing partnerships a priority for NATO at a time when the security environment is taking the Alliance back to its core collective defence task?
- how can partnerships help NATO in this "new" collective defence task (for example, by making private actors more important as they help tackle hybrid threats)?

Unavoidable Partnerships. The evolution of the security environment is such that contemporary security governance is by nature multifaceted and multi-actor. Practically all current defence issues require the involvement of *several* defence/security actors operating at different levels over time and space.

Such characteristic implies that a certain level of interaction among different security actors will always be required, leading to the notion of partnership. In other words, partnerships are inherent to contemporary security governance, they are not optional; the question is not whether NATO should partner, but rather with whom, how, and for what purpose.

Interests versus values. Lastly, while the NATO narrative is strong on the mix of interests and values that the Alliance claims to promote and defend, the question is how to factor in and ensure the right balance between interests and values in shifting partnership activities.[9]

First, the idea that partnerships serve NATO's interests needs to be constantly adjusted to the concomitant partners' interests, which in turn inevitably shape those of NATO and its member states. As an example, NATO's interests in Iraq or Afghanistan may differ from those of Iraqi or Afghani actors, and the latter impact the former. Finding compatibility between the various types of interests expressed by the different types of actors involved can be a challenge.

Second, if defence sector reform, defence capacity-building activities or building integrity programmes usually include a value-based angle, assuming that partner countries share NATO's values is neither realistic nor necessarily useful. This relates to how NATO understands the notion of stability (in "projecting stability"), which may be interpreted more as being interest-driven (a situation that constitutes no threat to NATO irrespective

9 The Report of the Reflection Group states that when partnership with a particular security actor is not possible, "a commitment to work towards shared security on the basis of mutual respect" should be sought. "NATO 2030: United for a new era", p.11.

of the value situation) than as being value-driven (for example the fact that projecting stability still contains a democracy-promotion agenda is questionable).[10]

The centrality of value promotion arguably decreases as the need to partner for strategic reasons increases. Value-promotion made sense in the enlargement perspective, but could be less of a priority in the current environment of great power competition (there was already a shift from Partnership for Peace to Mediterranean Dialogue, to the Istanbul Cooperation Initiative, and then partnerships with countries like Afghanistan or Pakistan, with value-promotion being less central to the MD and ICI partnerships, and to the two above-mentioned countries).

Challenges to partnerships

With these premises in mind, we turn to the challenges that potentially undermine the overall coherence and effectiveness of NATO's partnerships. Five strategic-level challenges are identified, in relation to a) drivers of cooperation; b) the hierarchical nature of partnerships; c) the geographical nature of partnerships; d) the internal dimension of partnerships; and e) the contested multilateral order.

Drivers of cooperation. Over the last 30 years, NATO's partnerships have been driven by three sets of objectives. In the 1990s, partnerships were mainly aimed at inducing transformation in countries on the immediate periphery of Europe, either with a perspective to joining the Alliance (for most Partnership for Peace countries) or not (for the Mediterranean Dialogue countries). In the post-9/11 and Afghan context, the drivers of partnership was twofold: stability in the MENA region, and getting capabilities for operations.

Against this backdrop, since the withdrawal of the International Security Assistance Force (ISAF) from Afghanistan in 2014, and in the context of a resurgent Russia, what is now driving partnerships is less tangible, and partnerships in general have suffered as a consequence.[11] In principle, partnerships should serve NATO's two broad missions of deterrence and defence on the one hand, projecting stability on the other (and *a fortiori* the three core tasks). Yet, in practice, the connection between partnerships (as instruments) and NATO's evolving missions (as an end) has been difficult to make, and NATO's partnership agenda has suffered as a result.

10 R. Belloni, "Stabilization. Rethinking intervention in weak and fragile states", in S. Lucarelli, A. Marrone, F. Moro (eds.), *Projecting stability in an unstable world*, NATO ACT, IAI, University of Bologna, 2017.

11 The Report of the Reflection Group puts that "the functioning of partnerships in recent years has been adversely affected by blockages due to bilateral disputes between partners and Allies, as well as by inadequate funding and over-reliance on voluntary trust funds". "NATO 2030: United for a new era", p.57.

With collective defence back to the forefront, the drivers of cooperation with third parties have become less salient; as for projecting stability, the complexity and volatility of the situation on the southern periphery of the Alliance (MENA region) has made partnerships as necessary as difficult to operationalize.

In this context, one challenge is to identify "new" drivers for cooperation and match the partnership efforts to the importance of these drivers (for example by admitting that cooperative security is no longer a priority or on the contrary by defining a new strategy for Projecting Stability).

Strategy, hierarchy and local buy-in. Second, the objective of delivering a strategic effect through partnerships is difficult to reconcile with the local buy-in imperative. On the one hand, it is assumed that partnerships can only produce an effect if the activities implemented through them are mutually-reinforcing, and therefore serve local partners' interests as much as they serve NATO's. In fact, in principle, the activities carried out by NATO in partner countries are demand-driven, i.e. they result from the identification of a need and a request by the partner.

On the other hand, the more a process is locally-owned, the less the external partner (NATO) is able to keep control, ensuring that the desired strategic effect is delivered. Most cooperative security activities are confronted with these tensions, when local actors consent to the international presence while disassociating themselves from the objectives or methods of the interveners. The extent to which interveners can shape the local environment is weakened as a consequence. For example, NATO's strategic effect in Afghanistan is paradoxically undermined by the degree of ownership or independence of the Afghan Armed and Police Forces that can to a degree shape their own agenda as they wish, and resist aspects of the NATO mandate that they are not comfortable with. In the same vein, NATO's impact on the stability of Iraq relies on the alignment of Allies' and Iraq's armed forces (trained by NATO) long-term interests, which cannot be taken for granted over time. Most partnerships reflect a degree of asymmetry between partners and in the long run the disparity tends to undermine the effect sought, as one actor sees itself as losing out in the relationship.

This takes us back to the notion of partnership itself. The word "partnership" has been useful over the years and carries some positive connotations related to mutual interests or gains for the partners involved. In terms of communication, the notion of partner suggests a sense of "we-feeling", i.e. partners belong to a group of actors who share interests and possibly values too.

This said, "partnership" can also convey a sense of hierarchy. Partnerships that put partners on the same level are rare and asymmetry is often the rule. In NATO's case,

partnerships are indeed often hierarchical (with NATO being politically in a dominant position) and can easily lead to an uneven relationship. Projecting stability, or capacity-building reveals the asymmetry between an actor that theoretically enjoys stability or has a given capacity and another that does not, the partnership being built around a transfer of stability or capacity. For NATO and its member states to be able to minimize as much as possible the (political and cultural) side effects of such asymmetry is crucial.

Geography. Third, the four partnership frameworks with third states were designed with a geographical rationale, although geographical groupings have also had a political dimension (for example, the fact that Central Asian states are in the PfP together with Sweden and Finland can hardly be explained only by geography).

With many former PfP countries joining the Alliance and profound political changes in the MENA region, the geographical rationale for partnership has lost ground. Typically, the geographical scope of the MD and ICI fail to match the geopolitical realities in the region.

In 2011, the so-called "Berlin package"[12] aimed at addressing some of the shortcomings of the geographical groups by introducing flexibility in the way partnerships are being implemented, and allowing partners to engage with NATO on the basis of their interest for a particular issue rather than because of their affiliation to a geographical group (facilitated by the single menu of partnerships activities). This is the so-called "30+n" format, that allows for more pragmatic engagement, also with states that do not belong to any formal multilateral partnership framework.[13]

Nonetheless, none of the four existing regional frameworks enjoys any political coherence, and in fact all suffer from their internal heterogeneity and political dynamics, so the time may have come to revisit geographical frameworks.

Internal politics. Fourth, one of the challenges faced by NATOs' partnerships lies in the connection between NATO's internal cohesion and the extent to which the Alliance can effectively partner. Effective partnerships can only reflect a strong internal consensus among NATO member states on the usefulness of a particular partnership and the level of investment that it requires. It is unlikely that a non-cohesive Alliance could produce an effective cooperation with a third party; in other words, partnerships can hardly compensate for a dysfunctional Alliance.

Yet, Allies have different priorities that can (negatively) impact partnerships. The Partnership for Peace, the Mediterranean Dialogue, the ICI, as well as NATO-EU

12 NATO, "Active engagement in cooperative security: a more efficient and flexible partnership policy", Berlin, April 2011 (so-called "Berlin agenda").

13 J. Appathurai, "The future of NATO's partnerships", in T. Flockhart (ed.), "Cooperative security: NATO's partnership policy in a changing world", *DIIS Report*, Danish Institute for International Studies, 2014.

cooperation, have all suffered from a lack of consensus among Allies on how to approach these partnerships, or some third states or party in particular. In some cases, it is the entire partnership process that is paralyzed as a consequence (when national priorities hinder the renewal of Individual Partnership and Cooperation Programmes (IPCPs) for example).

The negative correlation between political disunity and coherence of partnership policies can be seen in extreme cases like Syria or Libya, where NATO Allies can end up on opposing sides; or in the competitive dynamics observed between NATO and the EU on the broad crisis management spectrum in the Mediterranean Sea and potentially North Africa.

Contested multilateral order. Finally, the partnership environment is challenged at the two levels of a) the political opposition to the Western-dominated liberal world order and b) a more operational rivalry, in key areas where NATO's partnerships are supposed to be operationalized, with peer competitors, namely China and Russia. Suffice it to say that if twenty years ago, Western actors could operate more or less *alone* in large portions of the African continent, this is no longer the case. China and Russia are increasingly present in the MENA region and further south, and compete with Western powers on the "partnership market".

If one adds the cases where NATO is not necessarily welcomed locally (or where local partners are reluctant to give NATO's presence too much visibility for fear of negative public reactions) and also suffers from a negative image among a number of private actors, one sees a picture in which NATO's agenda is potentially contested at three different levels: by peer competitors, by other international organizations, and by local state- and/or non-state actors.

Interestingly enough, although these issues come as challenges to NATO's partnerships, they are also invitations for more cooperation with the types of actors that are susceptible to better position NATO on the ever more competitive market.

Policy considerations / Recommendations

The NATO 2030 process is about reflecting on the Alliance's role ten years hence, on what the challenges are, and how it should adapt to an ever more uncertain and competitive world. As stated before, partnerships are an integral part of this discussion, as they relate to making NATO more political and allow it to reach out to actors on a global scale. What follows is a series of policy considerations/recommendations that further feed the debate about the future of NATO's partnerships.

For an enhanced partnership agenda and narrative. While partnerships have become

less central in NATO's agenda over the last seven years, the changes in the security environment combined with the military nature of the Alliance plead for an enhanced partnership agenda so that NATO can maximize its military/security role. The rationale for the Comprehensive Approach – "NATO cannot do it alone" – is even more valid today given the diversity of threats and actors involved in their management.

Drivers for cooperation might seem less obvious today than when the objectives of partnership were *enlargement* or *operations*; however, there is a case for partnerships responding to the complexity of threats, or shaping the evolving and contested world order. This is what is implied by the Secretary General when linking the future political and global role of the Alliance with the need to "further strengthen partnerships".[14] Partnerships can indeed act as "political enablers" of NATO's adaptation and relevance, and any new thinking about NATO's core functions needs to factor in partnerships in relation to the multifaceted security environment and the type of needs that it creates.

This entails a narrative (and a new slogan?) on the objectives and functions of partnerships in relation to *all* NATO's core tasks (whatever they may be or become), and certainly not only in relation to a cooperative security or projecting stability agenda. Partnerships are a means to a broader end, and what partnerships do in relation to collective defence also ought to be clarified and communicated (see below). In so doing, it would also be helpful if the narrative reiterated a number of principles and objectives that guide partnerships.

The Report of the Reflection Group pleads in favour of such a new bargain. It first makes "deeper strategic connections with partners"[15] one of the six components of its vision for NATO. Then the Group suggests that NATO should "outline a global blueprint for better utilising its partnerships to advance NATO strategic interests".[16]

For non-geographical partnerships. The relevance of regional frameworks such as the PfP, the Mediterranean Dialogue and the ICI is being questioned, yet it is also acknowledged that there is little political appetite among NATO Allies to seriously revisit the existing structure.[17] In the same vein, the heterogeneity of the Partners across the Globe grouping (bringing together countries such as Australia, South Korea and Japan, together with Afghanistan, Pakistan and Mongolia), speaks against any kind of political or

14 Remarks by NATO Secretary General Jens Stoltenberg on launching #NATO2030 – "Strengthening the Alliance in an increasingly competitive world", 8 June 2020.

15 "NATO 2030: United for a new era. Analysis and recommendations of the Reflection Group appointed by the NATO Secretary General", Brussels, 25 November 2020, p.11. https://www.nato.int/cps/en/natohq/news_179840.htm

16 *Ibid*, p.15 and 57-58.

17 See *inter alia*, K.-H. Kamp and H. Reisinger, "NATO's Partnership after 2014: go West!", *Research Paper* No.92, NATO Defense College, 2013; I. Lesser *et al.*, "The future of NATO's Mediterranean Dialogue. Perspectives on security, strategy and partnership", German Marshall Fund, 2018.

even geographical rationale other than "these countries belong to no established regional framework".

This paper does not deal specifically with geographical frameworks, yet the issue of how adapted (or dysfunctional) those frameworks are today will have to be raised if the overall efficiency of partnerships is to be improved. Is the flexibility introduced by the "30+n" formula and pragmatic bilateral relations sufficient to address challenges posed by the geographical approach? While geographical frameworks may not be optimal, do they in practice impede cooperation or do the obstacles lie elsewhere? More radically, should NATO move away from geographical frameworks and opt for a more pragmatic, functional approach?

The Reflection Group poses that "NATO should make more use of thematic rather only geographic groupings for advancing work on cross-cutting challenges".[18] This begs the question of whether NATO should reach out to like-minded states (liberal democracies), in particular in the context of containing China. In an address to the NATO Parliamentary Assembly and as he was talking about Japan, South Korea, Australia and New Zealand, NATO Secretary General put that "our political response to the political challenges we see from China not sharing our core values, democracy, individual liberties, just makes that cooperation with other like-minded partners even more important".[19] In a similar vein, for the Reflection Group, in an "era of intensifying geostrategic competition and global threats", NATO should "leverage its strong partnerships […] in the Indo-Pacific"; countries mentioned are Australia, Japan, New Zealand, and the Republic of Korea, and also potentially India, in direct connection with the "strategic and political implications of China's rise".[20] In this coming debate, geography is likely to be less central to the notion of partnership than it was in the 1990s or 2000s, yet the above-mentioned countries do belong to the same geographical space – the Indo-Pacific – and share as such a relative proximity with China.

For a "security network" approach. The above-mentioned multi-actor nature of crisis management combined with multifaceted security challenges makes NATO one actor among many. Such characteristics lead to two sets of challenges: first, NATO needs to accept that the leadership position experienced in the Western Balkans or in Afghanistan is not necessarily the role model for future security governance activity. Second, NATO must continue to develop its knowledge of and level of interaction with a range of actors – including non-state actors – that are going to play an increasing role in crisis management/

18 "NATO 2030: united for a new era", p.58.

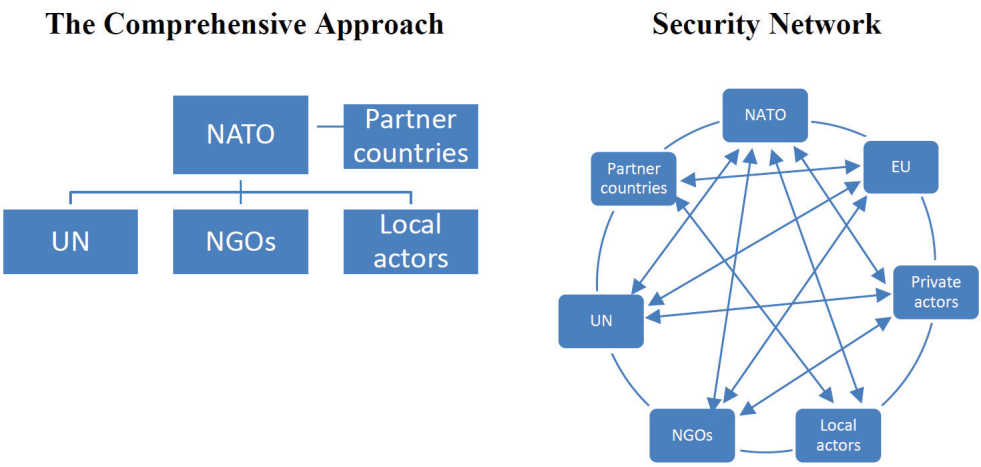
19 "Adapting NATO for 2030 and beyond", Speech by NATO Secretary General Jens Stoltenberg at the 66th Annual Session of the NATO Parliamentary Assembly, 23 November 2020.

20 "NATO 2030: united for a new era", p.57 and 60.

cooperative security, and even in collective defence.

While doing so, it can be useful to think about partnerships in terms of "security networks"[21] (or "security complexes" if we consider the regional frameworks) rather than in terms of, say, the comprehensive approach. Starting in the Western Balkans in the 1990s, and then in the Afghan context throughout the 2000s, NATO conceived of its partnership policy largely as being NATO- and state-centered.[22] Most of the thinking about partnerships also tends to see them as a two-player relationship, or as a relationship between one coordinator and a range of coordinated entities. This is what NATO's Comprehensive Approach was largely about (see Figure 1 below), and this made sense as long as NATO was in the lead and providing the bulk of (human) resources.

Figure 2. The Comprehensive Approach vs Security Network



This said, in the current security environment, multi-actor cooperation is likely to take the form of loosely coordinated networks of disparate and independent entities; these "security networks" are interconnected through formal or informal ties to produce an effect in the security domain that is mutually beneficial. In these networks NATO might

21 C. Whelan and B. Dupont, "Taking stock of networks across the security field: a review, typology and research agenda", *Policing and Society*, 2017.

22 See T. Tardy, "NATO and the comprehensive approach: weak conceptualisation, political divergences and implementation challenges" in G. Herd and J. Kriendler (eds.), *Understanding NATO in the 21st century*, London, Routledge, 2012, pp.102-118.

play a secondary role and be coordinated by others. The Reflection Group refers to an "informal system of overlapping organisations and bilateral/multilateral relationships"[23]; and former World Trade Organization Director-General and now President of the Paris Peace Forum Pascal Lamy talks about "polylateralism" as a method to "escape the impasse of state multilateralism" and to "widen the interstices of the *inter* and the *multi,* in order to include new actors: NGOs, businesses, cities, large academic institutions".[24]

In the response to a hybrid threat targeting a critical infrastructure on the territory of one Ally for example, actors such as NATO, the European Union, private sector companies, civil society organizations, municipalities, and police forces might be involved in a loosely coordinated "security network". If the issue is piracy-related, NATO may need to reach out to the EU and coastal states, but also to maritime powers such as China and India, as well as to shipping companies and private security companies.

This calls for some flexibility in partnerships that can be lightly institutionalized and *ad hoc* (for example to respond to a specific, time-limited issue), as well as for an openness towards diverse non-state actors (NGOs, private companies, civil society groups, etc.). Yet the flexibility of security networks would not necessarily mean an openness to whoever wants to contribute – participation would need to be subject-related.

From this it follows that partnerships are also about finding one's place in the system; it is about defining one's role in relation to, or together with, other security actors based on what one can offer and in response to the needs of the environment. This would also take partnerships one step further by looking at partners as security providers and not only as security consumers.

For more political partnerships. A critique often addressed to NATO's partnerships is that they are too technical and not sufficiently political. For example, by opening the cooperation menu to all partners for the sake of efficiency and flexibility, the 2011 "Berlin package"[25] has been portrayed as being more a managerial rather than a political agenda[26]; the critique is also often levelled at the NATO-EU relationship, confined to technical cooperation because of the political obstacles.

It is also acknowledged that partnerships can only produce a lasting and tangible effect if they are supported at the political level (the overused concept of "political will" comes into play here) – leading to the provision of resources – and if they are part of a broader

23 "NATO 2030: united for a new era", p.59.

24 "Polylateralism as the way forward, a conversation with Pascal Lamy", *Le Grand Continent*, 7 December 2020, https://geopolitique.eu/en/polylateralism-as-the-way-forward-a-conversation-with-pascal-lamy/

25 NATO, "Active engagement in cooperative security: a more efficient and flexible partnership policy", Berlin, April 2011.

26 See H. Reisinger, "Rearranging family life and a large circle of friends: reforming NATO's partnership programmes", *Research Paper* No.72, NATO Defense College, 2012.

vision. This leads to three sets of issues.

First, is the issue of prioritization of partnerships: based on how politically important (and supported) partnerships are, they must be more or less prioritized. Although no hierarchy of partnerships is officially acknowledged within NATO, in practice some partnerships or partners get more attention and resources than others. In this sense prioritization is to an extent happening. Should this become more explicit? And if yes, which partnership should be given priority? What criteria should be used for this exercise? A combination of interests and values? Would a clearer prioritization allow for a better concentration of efforts? And would it reinforce or on the contrary hinder political cohesion within the Alliance?

Second, the plea for more political partnerships needs to be nuanced by the fact that quite a few partnerships remain technical precisely because there are political obstacles to their full implementation. This is the case of the NATO-EU relationship that is unlikely to move much further given the political context. Intra-Alliance politics and the lack of consensus among Allies on certain aspects of partnerships (the Mediterranean Dialogue in relation to Israel for example) are also cases in point. In such situations, calling for more politics may sound futile at least in the short term, and rather opting for the development of de-politicized activities might be the way forward. As a matter of fact, back in 2011, the logic behind the Berlin package was partly to leave those political issues aside and still move forward in reforming partnerships.

Third, this being said, partnerships cannot in the long run be disconnected from the political context, and must, as much as possible, be part of a broader vision or policy. For NATO this implies:

- the development of such a vision (through a Projecting Stability Strategy for example) that would include:
  - identifying objectives of partnerships, short- vs longer term, political vs more operational, etc.
  - identifying needs, for example more on capacity or more on governance;
  - considering country specificity (the needs of Afghanistan are different from the needs of Egypt);
  - examining the match between a particular partnership and the regional context (in the MENA region, in Central Asia, etc.);
- weighing carefully the demand-driven approach of partner countries (assessing the added-value of the NATO contribution in comparison to other cooperation programmes) and the need for a NATO strategic approach[27];

27 The Report of the Reflection Group advocates a "shift from the current demand-driven approach to an interest-driven approach" for NATO's partnerships (p.15.)

– coordinating NATO and bilateral programmes run in parallel by Allies;
– when possible, the design of incentives (in coordination with Allies present in the region or country) that serve NATO's long-term objectives; and
– thinking creatively in terms of security networks that could bring together different types of actors or institutions (like the NATO-Jordan-UN counter-terrorism initiative for example).

In the same vein, partnerships being more strategic also implies that they are considered in the broader context of NATO's collective defence mandate (and not only NATO's cooperative security agenda). In other words, how can partnerships help NATO to better deter and defend? Hybrid threats provide a good example of where the collective defence agenda requires that NATO co-operate with a wide range of actors, ranging from the EU to private actors. And if great power competition is on NATO's agenda, then any thinking about future partnerships must deal with how such partnerships can play to NATO's advantage in great power politics. This leads, *inter alia*, to issues such as:

- what China's emergence and potential confrontation with the US means for NATO's partnerships;
- whether and how NATO should interact with India to counterbalance China;
- what kind of dialogue or partnerships NATO should develop with democratic or like-minded states worldwide, or, conversely, with authoritarian regimes that may play an important role in NATO's broad Projecting Stability Strategy;
- how partnerships can help NATO build its own resilience in the face of the Russian threat.

For more strategic thinking. Finally, insofar as partnerships imply two or more security actors co-operating on a particular aspect of security governance, they relate to the notions of core and peripheral tasks, comparative advantages, complementarity vs overlap, but also market positioning, hierarchy, competition.

In order to minimize the negative effect of possible duplication among various security actors, some strategic thinking about a sound division of tasks is required. This is to say that, for NATO, partnership is a lot about finding one's place in the broader security architecture. Based on what NATO's core tasks are to become, NATO will have to define the type of partnerships it requires, those it wants to prioritize, and those that become secondary.

As examples, for NATO to embrace a more civilian agenda (in light of the COVID crisis) or to clearly renounce it, will impact NATO's relationship with the EU or other civilian actors; moving towards total defence and resilience-building would also and fundamentally shape NATO's partnerships. In the same vein, identifying (or not) China as a threat to

tackle will have an impact on the type of partnerships (with India? with Indonesia?) that are required. Re-concentrating on NATO's core military role would equally determine the type of partnership that is needed.

This means that partnerships are an integral part of NATO's identity and adaptation. May the current NATO 2030 process – and possibility a subsequent Strategic Concept – bring clarity on the latter so that the former can produce a strategic effect.

NDC Publications (2018-2021)

NDC Policy Briefs

2018

The internal nature of the Alliance's cohesion
Thierry Tardy
NDC Policy Brief 1, October 2018

Projecting stability in practice? NATO's new training mission in Iraq
Kevin Koehler
NDC Policy Brief 2, October 2018

Challenges and potential for NATO-Egypt partnership
Adel El-Adawy
NDC Policy Brief 3, November 2018

The Great War legacy for NATO
Ian Hope
NDC Policy Brief 4, November 2018

European defence: what impact for NATO?
Thierry Tardy
NDC Policy Brief 5, December 2018

Will artificial intelligence challenge NATO interoperability?
Martin Dufour
NDC Policy Brief 6, December 2018

NATO-EU maritime cooperation: for what strategic effect?
Stefano Marcuzzi
NDC Policy Brief 7, December 2018

2019

Energy security in the Baltic Region: between markets and politics
Marc Ozawa
NDC Policy Brief 1, January 2019

NATO's nuclear deterrence: more important, yet more contested
Michael Rühle
NDC Policy Brief 2, January 2019

Vostok 2018: ten years of Russian strategic exercises and warfare preparation
Dave Johnson
NDC Policy Brief 3, February 2019 (8 pages)

Preparing for "NATO-mation": the Atlantic Alliance toward the age of artificial intelligence
Andrea Gilli
NDC Policy Brief 4, February 2019

NATO at 70: modernising for the future
Rose Gottemoeller
NDC Policy Brief 5, March 2019

NATO's coming existential challenge
Karl-Heinz Kamp
NDC Policy Brief 6, March 2019

"NATO@70": still adapting after all these years
Julian Lindley-French
NDC Policy Brief 7, March 2019

NATO is doing fine, but the Atlantic Alliance is in trouble
Bruno Tertrais
NDC Policy Brief 8, April 2019

70 years of NATO: the strength of the past, looking into the future
Kori Schake, with *Erica Pepe*
NDC Policy Brief 9, April 2019

NATO at 70: enter the technological age
Tomáš Valášek
NDC Policy Brief 10, April 2019

Building the airplane while flying: adapting NATO's force structure in an era of uncertainty
Sara Bjerg Moller
NDC Policy Brief 11, May 2019 (8 pages)

What NATO's counter-terrorism strategy?
Kris Quanten
NDC Policy Brief 12, May 2019

Why the Baltics matter. Defending NATO's North-Eastern border
Sven Sakkov
NDC Policy Brief 13, June 2019

The necessary adaptation of NATO's military instrument of power
Jan Broeks
NDC Policy Brief 14, June 2019

Deterring hybrid threats: the need for a more rational debate
Michael Rühle
NDC Policy Brief 15, July 2019

Russia and China: "axis of convenience" or a "stable strategic partnership"?
Marc Ozawa
NDC Policy Brief 16, July 2019

NATO and EU training missions in Iraq – an opportunity to enhance cooperation
Niels Schafranek
NDC Policy Brief 17, August 2019

Fighting "Men in Jeans" in the grey zone between peace and war
Peter Braun
NDC Policy Brief 18, August 2019

From hybrid warfare to "cybrid" campaigns: the new normal?
Antonio Missiroli
NDC Policy Brief 19, September 2019

The role of democracy and human rights adherence in NATO enlargement decisions
Eyal Rubinson
NDC Policy Brief 20, September 2019 (8 pages)

What NATO contribution to the security architecture of the Indo-Pacific?
Jean-Loup Samaan
NDC Policy Brief 21, October 2019

The enhanced Forward Presence: innovating NATO's deployment model for collective defence
Christian Leuprecht
NDC Policy Brief 22, October 2019 (8 pages)

NATO at 70: what defence policy and planning priorities?
Patrick Turner
NDC Policy Brief 23, October 2019

Calibrating the scope of NATO's mandate
Thierry Tardy
NDC Policy Brief 24, November 2019

Imitation, innovation, disruption: challenges to NATO's superiority in military technology
Andrea Gilli and Mauro Gilli
NDC Policy Brief 25, December 2019

2020

Alliance capabilities at 70: achieving agility for an uncertain future
Camille Grand and Matthew Gillis
NDC Policy Brief 1, January 2020

It's that time of the decade again: some considerations for NATO's eighth Strategic Concept
Jeffrey H. Michaels
NDC Policy Brief 2, January 2020

The case for NATO's global partnership with India
Abdurrahman Utku HacIoğlu
NDC Policy Brief 3, February 2020

Turkey's military policy in Syria: implications for NATO
Can Kasapoglu
NDC Policy Brief 4, February 2020

No time to hedge? Articulating a European pillar within the Alliance
Jens Ringsmose and Mark Webber
NDC Policy Brief 5, March 2020

Scoping NATO's environmental security agenda
Michael Rühle
NDC Policy Brief 6, March 2020

Time for a NATO strategy on North Korea?
Tina J. Park
NDC Policy Brief 7, April 2020

The NATO Pipeline System: a forgotten defence asset
Dominik P. Jankowski
NDC Policy Brief 8, April 2020

Projeter la stabilité au Sud : l'autre défi de l'OTAN
Projecting Stability to the South: NATO's other challenge
Chloé Berger
NDC Policy Brief 9, May 2020

NATO's needed offensive cyber capabilities
Ion A. Iftimie
NDC Policy Brief 10, May 2020

NATO and CSDP: party and public positioning in Germany and France
Konstantin Gavras, Thomas J. Scotto, Jason Reifler, Stephanie Hofmann, Catarina Thomson, Matthias Mader, Harald Schoen
NDC Policy Brief 11, June 2020

NATO's strategic redirection to the South
Stephen J. Mariano
NDC Policy Brief 12, June 2020

NATO and 5G: what strategic lessons?
Andrea Gilli
NDC Policy Brief 13, July 2020

Revitalizing NATO's once robust standardization programme
Paul Beckley
NDC Policy Brief 14, July 2020

NATO and the COVID-19 emergency: actions and lessons
LtGen Olivier Rittimann
NDC Policy Brief 15, September 2020

A renewed collective defense bargain? NATO in COVID's shadow
Sten Rynning
NDC Policy Brief 16, September 2020

Catalyst or crisis? COVID-19 and European Security
Claudia Major
NDC Policy Brief 17, October 2020

COVID-19 and the defence policies of European states
Alice Billon-Galland
NDC Policy Brief 18, October 2020

The interstate conflict potential of the information domain
Dumitru Minzarari
NDC Policy Brief 19, November 2020

China in the COVID world: continued challenges for a rising power
Bates Gill
NDC Policy Brief 20, November 2020

The pandemic and the military: towards total defense?
Antonio Missiroli and Michael Rühle
NDC Policy Brief 21, November 2020

Russian Grand Strategy and the COVID-19 crisis
Andrew Monaghan
NDC Policy Brief 22, December 2020

"NATO 2030. United for a new era": a Digest
Thierry Tardy
NDC Policy Brief 23, December 2020

2021

Deterrence by detection: using surveillance to pre-empt opportunistic aggression
Thomas G. Mahnken and Grace B. Kim
NDC Policy Brief 1, January 2021

Operation Althea and the virtues of the Berlin Plus Agreement
LGen. Olivier Rittimann
NDC Policy Brief 2, January 2021

NATO's eastern flank: retooling the US-Baltic security link
Andris Banka
NDC Policy Brief 3, February 2021

NDC Research Papers

Projecting stability: elixir or snake oil?
Edited by Ian Hope
NDC Research Paper 1, December 2018

NATO's futures: the Atlantic Alliance between power and purpose
Sten Rynning
NDC Research Paper 2, March 2019

A strategic odyssey: constancy of purpose and strategy-making in NATO, 1949-2019
Diego A. Ruiz Palmer
NDC Research Paper 3, June 2019

Russia's military posture in the Arctic - managing hard power in a "low tension" environment
Mathieu Boulègue
NDC Research Paper 4, July 2019

NATO and the EU. The essential partners
Edited by Gustav Lindstrom and Thierry Tardy
NDC Research Paper 5, September 2019

The brain and the processor: unpacking the challenges of human-machine interaction
Edited by Andrea Gilli
NDC Research Paper 6, December 2019

The Alliance five years after Crimea: implementing the Wales Summit pledges
Edited by Marc Ozawa
NDC Research Paper 7, December 2019

NATO at 70: no time to retire
Edited by Thierry Tardy
NDC Research Paper 8, January 2020

COVID-19: NATO in the age of pandemics
Edited by Thierry Tardy
NDC Research Paper 9, May 2020

Recalibrating NATO nuclear policy
Edited by Andrea Gilli
NDC Research Paper 10, June 2020

Russia's emerging global ambitions
Marcin Kaczmarski, Wojciech Michnik, Andrew Monaghan, Marc Ozawa, Vasile Rotaru
NDC Research Paper 11, July 2020

NATO's strategic foundations: values, deterrence, and arms control
Edited by Stephen J. Mariano
NDC Research Paper 12, September 2020

Russia's energy policy. Dependence, networks and special relationships
Marc Ozawa and Ion Alexandru Iftimie
NDC Research Paper 13, October 2020

Lessons from the Enhanced Forward Presence, 2017-2020
Edited by Alexander Lanoszka, Christian Leuprecht, and Alexander Moens
NDC Research Paper 14, November 2020

"NATO-Mation": strategies for leading in the age of artificial intelligence
Andrea Gilli with Mauro Gilli, Ann-Sophie Leonard and Zoe Stanley-Lockman
NDC Research Paper 15, December 2020

Russia in NATO's South: Expansionist Strategy or Defensive Posture?
Edited by Chloé Berger and Cynthia Salloum
NDC Research Paper 16, January 2021


NATO
OTAN