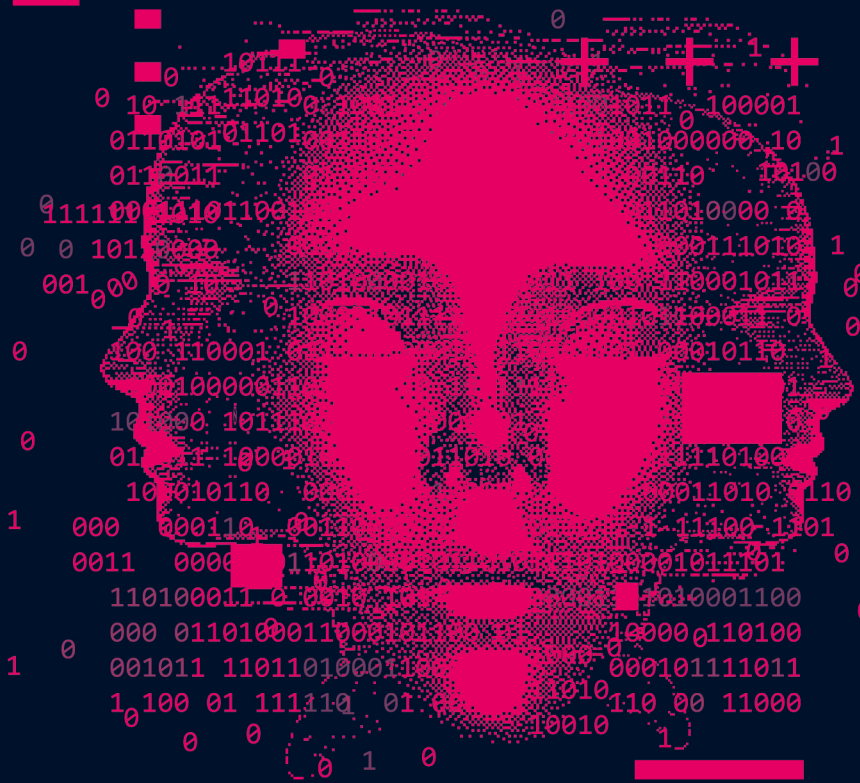

NATO

in the Era of Unpeace: Defending Against Known Unknowns

Edited by
Dominik P. Jankowski and Tomasz Stępniewski

Instytut Europy Środkowej
Institute of Central Europe

NATO

in the Era of Unpeace:
Defending Against
Known Unknowns

NATO

in the Era of Unpeace: Defending Against Known Unknowns

Edited by

Dominik P. Jankowski and Tomasz Stępniewski

Brussels – Lublin 2021

Reviewers
Major General Piotr "Zeus" Błazeusz, Ph.D., SHAPE
Professor Jakub J. Grygiel, Catholic University of America
Péter Stepper, Ph.D., National University of Public Service, Hungary

Cover design and typesetting
Amadeusz Targoński ▪ www.targonski.pl

Cover photo
© local | shutterstock.com

ISBN
978-83-66413-40-5

Published and edited
Instytut Europy Środkowej / Institute of Central Europe
ul. Niecała 5
20-080 Lublin
www.ies.lublin.pl

Print
Drukarnia Akapit
www.drukarniaakapit.pl

Contents

Ambassador Baiba Braže

Foreword

It is no exaggeration to say that the only thing we can be certain of is uncertainty itself. A few years ago, we hardly knew what "uncertainty" would look like today. COVID-19 has shown that our world is more unpredictable than ever.

During the Cold War, NATO had to focus on a single adversary: the Soviet Union. The line between war and peace was clearer. As the line becomes more blurred, however, we need to deal with multiple threats coming from state and non-state actors and from multiple directions – on land, at sea, in the air, in space, and cyberspace. Our adversaries challenge us not only using bombs and aircraft but also bots and algorithms.

In this more unpredictable world, we face a more assertive Russia, brutal terrorist groups like ISIS, and more sophisticated cyber-attacks. We see an intensifying geopolitical competition with the rise of China. We are faced with new sources of instability and

unpredictability: potentially dangerous new technologies and disruptions due to climate change.

For NATO, this means we must remain ready to tackle any known or unknown challenge, at any time, to keep our people safe. We need to be prepared for the unexpected by keeping NATO a strong military alliance, making it politically stronger, and ensuring it takes a more global approach.

To keep NATO militarily strong, our nations need to continue investing in defence so that we have the best militaries with the right capabilities. To keep our technological edge, Allies should invest even more in cutting-edge capabilities like artificial intelligence, big data, and quantum computing.

For the first time, we have deployed combat-ready forces to the east of our Alliance in response to Russia's aggressive actions. We are working together to deal with the security impact of the rise of China and new technologies. We have also designated cyberspace and space as operational domains. And our militaries are supporting civilian efforts to counter COVID-19.

We also need to use NATO even more as a platform for political consultations because this is the only place where North America and Europe meet every day to discuss, decide, and act on our shared security. When we have differences, we must bring them to the NATO table and discuss them openly so that we can work out common approaches.

And while NATO will remain a regional alliance, we must take a more global approach to deal with global challenges such as the rise of China. China is not our adversary. Its rise on the global stage brings opportunities, but it also presents challenges. China has the second biggest defence budget in the world and continues to modernize its

military at a rapid pace. At the same time, it undermines human rights and bullies other countries.

Therefore, we are working more closely with partners, notably in the Asia-Pacific region, because as a community of like-minded democracies, we have a common interest in defending our shared values, bolstering the resilience of our societies, economies, and institutions, and upholding the rules-based order.

We are also bolstering the resilience of our critical infrastructure — power grids, ports, airports, roads, railways, and telecommunication systems, including 5G. And NATO will continue to strengthen our resilience requirements, encouraging Allies to conduct thorough risk and vulnerability assessments, including mapping foreign ownership, control, or direct investment.

So, NATO is doing more. But the world is moving faster than ever before. So, we need to adapt even faster to deal with the known as well the unknown challenges. In dealing with all uncertainties, one thing is certain, though: We can only be strong if North America and Europe stand united. If we manage that, we have every reason to look into the future with confidence and optimism.

Ambassador Baiba Braže
NATO Assistant Secretary General for Public Diplomacy
Brussels, February 2021

Dominik P. Jankowski, Tomasz Stępniewski

NATO 2030 and Beyond: Editors' Introduction

The year 2014 was a watershed moment for NATO for three reasons. First, the outbreak of the Russian-Ukrainian conflict was a game-changer for European security. The entire European security architecture trembled as the eastern flank of the continent was destabilized. In fact, this conflict was yet more proof – after the first wake-up call in 2008 during the Russian-Georgian war – that Eastern Europe remains a volatile space. Second, Russia confirmed its status as a revisionist power. Its principal foreign policy goal has been to maintain Eastern Europe in Russia's sphere of influence by stopping, or at least hampering, the Euro-Atlantic aspirations of Georgia, Moldova, and Ukraine. For NATO this meant that there could not be "business as usual" with Russia. Indeed, a revisionist Russia can hardly be treated as NATO's "strategic partner" any longer. Third, Europeans rediscovered that defence still matters and that they needed to reconsider rearmament.

A new era of unpeace – defined as a mid-spectrum rivalry lying below the physically destructive threshold of interstate violence, but whose harmful effects far surpass the tolerable level of peacetime competition – has started. NATO needs to defend against the "known unknowns", including hybrid threats and emerging and disruptive technologies. Therefore, since 2014 the Alliance has undergone a substantial military adaptation process. The NATO Summits in Newport (2014), Warsaw (2016), and Brussels (2018) constitute a robust package of measures that aim, among other outcomes, to reenergize collective defence by boosting NATO's deterrence and defence posture in order to deny the state of unpeace that Russia wants to impose. In 2019, NATO leaders decided at their meeting in London that the ongoing military adaptation should be paired with more visible and active political activity by the Alliance. They agreed to launch under the auspices of the Secretary General a forward-looking reflection process – thereafter named the NATO 2030 initiative – to assess ways to strengthen the political dimension of the Alliance.

This special publication of the Institute of Central Europe (Instytut Europy Środkowej, IEŚ) in Lublin contributes to broader academic and expert NATO 2030 discussions on how to ensure that NATO remains a robust military Alliance and becomes stronger politically. In the next decade, NATO will continue to operate in the security environment marked by the era of unpeace. In fact, one should expect that more "known unknowns" will challenge NATO's political cohesion and unity as well as its deterrence and defence posture. This publication discusses some key building blocks for a future NATO strategy: enhancing collective defence, countering hybrid threats, and embracing emerging and disruptive technologies.

Dave Johnson's (International Staff, NATO) chapter emphasizes the idea that through its strategic destabilization campaign, Russia seeks to impose a state of unpeace in the Euro-Atlantic space. That state of unpeace represents a clash of values and a differing vision of a future security architecture that, in the long run, has potential implications for Alliance security as serious as Russia's military build-up. Furthermore, Michael Rühle (International Staff, NATO) argues in his piece that NATO needs to progress from what is currently an all-hazards approach to hybrid threats (i.e. any actor, any tool) to a more focussed one that looks at each hybrid actor as a unique entity. Finally, Dominik P. Jankowski (Permanent Representation of Poland to NATO) emphasizes in his chapter that the extent to which the emerging and disruptive technologies exacerbate or mitigate global security and governance challenges will remain an integral question as policymakers navigate the complex global environment, including the challenges Russia currently poses for NATO Allies.

We would like to offer our special thanks to the authors for their commitment to providing their input and analysis on the future of NATO. We hope that this special publication will be well received by readers, both academics and experts as well as practitioners and policymakers.

Dominik P. Jankowski, Tomasz Stępniewski
Brussels and Lublin, February 2021

Executive Summary

Collective defence

- NATO faces a multidimensional Russian challenge to its collective defence that is concentrated on its eastern flank, can physically threaten the Alliance from all azimuths, and penetrates to strategic depth in non-physical domains.
- Russia is implementing a multi-domain destabilization campaign (by integrated non-military and military means) intended to undermine NATO security by non-military means. Russia's military-backed destabilization campaign is intended to impose conditions of unpeace in the Euro-Atlantic space. Military power, including exercises and operations, shows of force, and nuclear sabre-rattling, is a major element of the strategic destabilization campaign.
- Moscow's destabilization campaign extends well beyond NATO's eastern flank and includes conducting long-range, hid-

den action, in particular in the information sphere, in order to translate incremental gains at the operational level into strategic gains in its long-term conflict with NATO.

- In order to uphold deterrence on NATO's eastern flank and, if necessary, to conduct a successful defence, NATO must counter Russia's ongoing destabilization campaign and contest the state of unpeace that it wishes to impose on Europe. It must also be ready to respond should Russia miscalculate that the political and military risks of aggression are manageable.
- To deter or successfully defend on its eastern flank, NATO and Allies must address the responsiveness, scalability, and multi-spectrum power of the Russian Armed Forces within the context of the ongoing Russian destabilization campaign, which would intensify in time of war.
- Military power, including exercises and operations, shows of force, and nuclear sabre-rattling, is a major element of the strategic destabilization campaign and includes military provocations to test NATO reactions and defences and carefully calibrated (so far), limited military actions intended to stay below the threshold for an Article 5 response by NATO.
- In the context of unpeace created by Russia's strategic destabilization campaign, the armed forces complement Russia's non-military levers of power by adding coercive and intimidating elements.
- The Russian Armed Forces are now structured, trained, and equipped to respond quickly and effectively in the event that Russia's vital interests are threatened, as in Ukraine, or when the political and military risks of an opportunity are assessed as manageable, as in Syria. While equipped and trained for

the most challenging scenario of large-scale conflict against a technologically advanced adversary, the Russian military is able to execute scalable options quickly in reaction to a wide range of scenarios.

- The security of NATO's eastern flank must be continuously assessed in its complete context, taking into account the factors described above. Russia today can concentrate large forces relatively quickly anywhere on its periphery, under a nuclear shadow, and with robust anti-access/area denial (A2/AD) capabilities aimed at preventing an adversary from traversing or liberating an area subjugated by Moscow. Leveraging this capability, Russia is implementing a multi-dimensional strategic destabilization campaign in the Euro-Atlantic space to achieve its foreign, security, and defence policy aims.
- This presents NATO and Allies with the dual challenges of countering Russia's destabilization campaign and rejecting the state of unpeace it tries to impose while maintaining a credible and effective deterrence and defence posture ready to respond to any contingency.
- NATO needs an alternative to President Vladimir Putin's vision of transatlantic security in five years, ten years, and beyond, and a sense of how NATO's deterrence and defence posture will support that vision.
- The current circumstances are not a passing phase. There is no reason to expect Russia's posture toward NATO to change drastically for the better in the mid-to-long term, whether President Putin remains part of the equation or not.

- Consideration of the evolving strategic environment outlined in this paper should be taken into account in a possible new Strategic Concept. Allies should:
  - Recognize that, at its core, Russia's effort to impose a state of unpeace in the Euro-Atlantic space through its strategic destabilization campaign represents a clash of values and a differing vision of the future security architecture that, in the long run, has as serious potential implications for Alliance security as Russia's military build-up;
  - Adapt NATO's strategy to respond appropriately to both elements of the Russian challenge – the customary deterrence and defence element and the broader challenge of Russia's ongoing strategic destabilization campaign. The latter will require continued enhancement of NATO's cooperation with the EU on addressing the hybrid challenge in order to deny the state of unpeace that Russia wants to impose and to deter Russia from acting with impunity below the kinetic level of aggression;
  - Continue on the basis of fulfilment of the defence spending pledge to implement the measures agreed to during the 2014 Wales Summit and afterwards to strengthen NATO's deterrence and defence posture by including more and heavier forces, continued capability enhancement across all domains, ensuring the viability of the Alliance's reinforcement strategy, and maintaining a safe, secure, and effective nuclear deterrent.

Hybrid threats

- Russia's use of hybrid tools in its assault on Ukraine in 2014 forced NATO not only to re-emphasise its core task of collective defence, but also to examine responses to hybrid threats. This is all the more urgent as hybrid campaigns could undermine NATO's collective defence preparations in a crisis, notably along NATO's eastern flank.
- Since 2014 NATO has systematically expanded its hybrid toolbox, which now encompasses, inter alia, enhanced intelligence sharing, a stronger focus on national resilience, the creation of specific tools (such as Counter Hybrid Support Teams), a more responsive public diplomacy effort, specifically tailored exercises, and closer relations with the European Union.
- Despite this progress, however, more still needs to be done. For example, more thought needs to be given to deterring hybrid threats, most notably to the specific role of the military in a predominantly non-kinetic context. NATO should also take a more actor-specific approach that takes into account a hybrid actor's strategic intent. Such steps should help to "de-mystify" hybrid challenges, as well as enhance NATO's preparedness to cope with them.

Emerging and disruptive technologies

- For NATO, the Emerging and Disruptive Technologies (EDTs) are primarily of interest due to their influence on the current and future defence capabilities as well as deterrence and defence posture. It is clear that EDTs will affect many of

the foundations of deterrence strategy. Indeed, new military technologies will play a crucial role in future warfighting and building forces that can decisively operate across domains.

- Russia has been closely monitoring the United States as well as China's technological priority areas while evaluating their long-term consequences and searching for means to counter them. The current Russian EDTs strategy has been based on two elements: first, countering the third offset strategy with the first offset strategy, which means prioritizing the development of a wide array of both strategic and tactical nuclear weapons systems; second, countering numerous U.S. and Chinese technological initiatives using similar indigenous programs, although more narrowly focused and smaller in scale.
- Disruptive technologies should not be seen in isolation from disruptive strategies. In fact, technologies enable strategies. With Russia, one needs to consider not only advances in high technology for traditional military applications but also innovations and uses below the level of declared war. Russia's premier disruptive strategy is intimidation.
- The potential EDTs implications for NATO's deterrence and defence remain of primary importance. Indeed, EDTs will provide a greater range of tools for adversaries to challenge and find weaknesses in NATO's posture. At the same time, ease of commercial access to EDTs raises the prospect of new – increasingly confident – state and non-state actors to contest NATO, particularly with increased challenges of attribution.

Dave Johnson

NATO Collective Defence in the Era of Unpeace

Dave Johnson - staff officer in the NATO International Staff Defence Policy and Planning Division. He previously served as an officer in the US Air Force, including in posts at SHAPE Headquarters, US Strategic Command, the US Defence Attaché Office Moscow, and the Pentagon. The views expressed are those of the author and do not necessarily reflect those of the North Atlantic Treaty Organization.

Executive Summary

- NATO faces a multidimensional Russian challenge to its collective defence that is concentrated on its eastern flank, can physically threaten the Alliance from all azimuths, and penetrates to strategic depth in non-physical domains.
- Russia is implementing a multi-domain destabilization campaign (by integrated non-military and military means) intended to undermine NATO security by non-military means. Russia's military-backed destabilization campaign is intended

to impose conditions of unpeace in the Euro-Atlantic space. Military power, including exercises and operations, shows of force, and nuclear sabre-rattling, is a major element of the strategic destabilization campaign.

- Moscow's destabilization campaign extends well beyond NATO's eastern flank and includes conducting long-range, hidden action, in particular in the information sphere, in order to translate incremental gains at the operational level into strategic gains in its long-term conflict with NATO.
- In order to uphold deterrence on NATO's eastern flank and, if necessary, to conduct a successful defence, NATO must counter Russia's ongoing destabilization campaign and contest the state of unpeace that it wishes to impose on Europe. It must also be ready to respond should Russia miscalculate that the political and military risks of aggression are manageable.
- To deter or successfully defend on its eastern flank, NATO and Allies must address the responsiveness, scalability, and multi-spectrum power of the Russian Armed Forces within the context of the ongoing Russian destabilization campaign, which would intensify in time of war.
- Military power, including exercises and operations, shows of force, and nuclear sabre-rattling, is a major element of the strategic destabilization campaign and includes military provocations to test NATO reactions and defences and carefully calibrated (so far), limited military actions intended to stay below the threshold for an Article 5 response by NATO.
- In the context of unpeace created by Russia's strategic destabilization campaign, the armed forces complement Russia's

non-military levers of power by adding coercive and intimidating elements.

- The Russian Armed Forces are now structured, trained, and equipped to respond quickly and effectively in the event that Russia's vital interests are threatened, as in Ukraine, or when the political and military risks of an opportunity are assessed as manageable, as in Syria. While equipped and trained for the most challenging scenario of large-scale conflict against a technologically advanced adversary, the Russian military is able to execute scalable options quickly in reaction to a wide range of scenarios.
- The security of NATO's eastern flank must be continuously assessed in its complete context, taking into account the factors described above. Russia today can concentrate large forces relatively quickly anywhere on its periphery, under a nuclear shadow, and with robust anti-access/area denial (A2/AD) capabilities aimed at preventing an adversary from traversing or liberating an area subjugated by Moscow. Leveraging this capability, Russia is implementing a multi-dimensional strategic destabilization campaign in the Euro-Atlantic space to achieve its foreign, security, and defence policy aims.
- This presents NATO and Allies with the dual challenges of countering Russia's destabilization campaign and rejecting the state of unpeace it tries to impose while maintaining a credible and effective deterrence and defence posture ready to respond to any contingency.
- NATO needs an alternative to President Vladimir Putin's vision of transatlantic security in five years, ten years, and beyond,

and a sense of how NATO's deterrence and defence posture will support that vision.

- The current circumstances are not a passing phase. There is no reason to expect Russia's posture toward NATO to change drastically for the better in the mid- to-long term, whether President Putin remains part of the equation or not.
- Consideration of the evolving strategic environment outlined in this paper should be taken into account in a possible new Strategic Concept. Allies should:
  - Recognize that, at its core, Russia's effort to impose a state of unpeace in the Euro-Atlantic space through its strategic destabilization campaign represents a clash of values and a differing vision of the future security architecture that, in the long run, has as serious potential implications for Alliance security as Russia's military build-up;
  - Adapt NATO's strategy to respond appropriately to both elements of the Russian challenge – the customary deterrence and defence element and the broader challenge of Russia's ongoing strategic destabilization campaign. The latter will require continued enhancement of NATO's cooperation with the EU on addressing the hybrid challenge in order to deny the state of unpeace that Russia wants to impose and to deter Russia from acting with impunity below the kinetic level of aggression;
  - Continue on the basis of fulfilment of the defence spending pledge to implement the measures agreed to during the 2014 Wales Summit and afterwards to strengthen NATO's deterrence and defence posture by including more and heavier forces, continued capability enhancement across

all domains, ensuring the viability of the Alliance's reinforcement strategy, and maintaining a safe, secure, and effective nuclear deterrent.

Introduction

NATO faces a multidimensional Russian challenge to its collective defence that is concentrated on its eastern flank, can physically threaten the Alliance from all azimuths, and penetrates to strategic depth in non-physical domains. Because of its geography and the proximity of large Russian high-readiness military groupings, NATO's eastern flank is a sector of NATO's 360-degree approach to its security that requires particularly high vigilance. In addition to posturing its increasingly capable military forces in a menacing way, Russia is implementing a multi-domain destabilization campaign intended to undermine NATO security by non-military means. Russia's military-backed destabilization campaign is intended to impose conditions of unpeace[1] in the Euro-Atlantic space in place of the post-Cold War security architecture that Moscow finds inimical to its interests.

[1] The author has adopted the term "unpeace" from L. Kello, "The Virtual Weapon and International Order", Yale University Press, New Haven, 2017, pp. 18 and 78. Kello proposes that "the nonviolent methods of unpeace can be more potent sources of national power and influence than the overt violence of Clausewitzian war." He defines unpeace as "mid-spectrum rivalry lying below the physically destructive threshold of interstate violence, but whose harmful effects far surpass the tolerable level of peacetime competition and possibly, even, of war." Although Kello's focus is on cyber issues in defence, the notion of unpeace that he proposes is an apt description of the state of relations between Russia and NATO nations created by Russia's multi-domain destabilization campaign and its intended effects.

This all represents a decisive turn by Russia away from the mutual commitments it made with NATO nations to "work together to contribute to establishment in Europe of common and comprehensive security based on the allegiance to shared values, commitments and norms of behaviour in the interests of all states."[2] This opportunity emerged from positive trends in the security environment that allowed NATO leaders to declare at the 1990 London Summit that Europe had "entered a new, promising era."[3] Political and military tensions were declining rapidly, stability was increasing and cooperative security was the common goal, all underpinned by a developing treaty architecture. NATO leaders stated their determination "to create enduring peace on this continent." NATO invited the Soviet government to establish regular diplomatic liaison with NATO.[4]

For NATO, this all brought rapid change in the Alliance's deterrence and defence posture. NATO shifted from a Forward Defence strategy and modified its Flexible Response nuclear doctrine to reflect a reduced reliance on nuclear weapons. NATO fielded smaller and more mobile forces, scaled-back readiness, and reduced training and exercise requirements.

Europe's post-Cold War treaty-based security architecture was established. Allies pursued "a fundamentally new relationship be-

[2] "The NATO-Russia Founding Act", Section I. Principles, paragraph 1, North Atlantic Treaty Organization, 27 May 1997, https://www.nato.int/cps/en/natohq/official_texts_25468.htm? [26.09.2020].

[3] "London Declaration on a Transformed North Atlantic Alliance Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in London", North Atlantic Treaty Organization, 5-6 July 1990, paragraph 1, https://www.nato.int/cps/en/natohq/official_texts_23693.htm? [26.09.2020].

[4] As well as the governments of the Czech and Slovak Federal Republic, the Hungarian Republic, the Republic of Poland, the People's Republic of Bulgaria, and Romania.

tween NATO and Russia."[5] Russia committed to further reducing its conventional and nuclear forces. NATO reduced its conventional and nuclear forces. NATO and Russia pursued a growing roster of defence and military reform cooperation initiatives, first in the framework of the Permanent Joint Council established by the NATO-Russia Founding Act (1997), and expanded in scope and ambition in the NATO-Russia Council framework (2002).[6]

During the twenty years between the 1990 London Summit and the 2010 Lisbon Summit, NATO, in the absence of a threat on its eastern flank, shifted focus from collective defence and Article 5 scenarios to crisis response operations. Deterrence receded into the background of NATO's focus. Russia became a privileged partner.

The new, promising era declared at the London Summit in 1990, however, has now passed. In the immediate aftermath of Russia's aggression against Ukraine and in response to instability in its southern neighbourhood, NATO leaders at the 2014 Wales Summit launched the most significant strengthening of the Alliance's deterrence and defence posture since the end of the Cold War.[7] At the Brussels Summit in 2018, NATO leaders declared "Russia's aggressive actions, including the threat and use of force to attain political goals, challenge the Alliance and are undermining Euro-Atlantic security and the rules-based international order." Leaders also said, "we face

5 NATO-Russia Founding Act, chapeau text.

6 "NATO-Russia Relations, A New Quality, Declaration by Heads of State and Government of NATO Member States and the Russian Federation", North Atlantic Treaty Organization, 27 May 2002, https://www.nato.int/cps/en/natohq/official_texts_19572.htm? [26.09.2020].

7 "Wales Summit Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales", North Atlantic Treaty Organization, 5 September 2014, https://www.nato.int/cps/en/natohq/official_texts_112964.htm [26.09.2020].

a dangerous, unpredictable, and fluid security environment, with enduring challenges and threats from all strategic directions; from state and non-state actors; from military forces; and from terrorist, cyber and hybrid attacks."[8] At the 2019 London meeting, NATO leaders again declared that Russia's aggressive actions constitute a threat to Euro-Atlantic security. They reaffirmed that NATO continues to adapt its military capabilities, strategy, and plans in line with its 360-degree approach to security.[9]

The Russian approach to undermining the security of NATO nations is a coordinated employment of all elements of national power both to achieve incrementally the kind of realignment of the European security architecture previously only achievable through war and to create the most favourable conditions for war should it become opportune or necessary. This approach is supported by the looming presence of Russia's revitalized military capabilities and Moscow's demonstrated willingness to use military force to achieve political objectives.

This means that in order to uphold deterrence on NATO's eastern flank and, if necessary, to conduct a successful defence, NATO must confront both elements of Russia's approach. NATO must counter Russia's ongoing destabilization campaign and contest the state of

8 "Brussels Summit Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Brussels 11-12 July 2018", North Atlantic Treaty Organization, 11 July 2018, paragraph 2, https://www.nato.int/cps/en/natohq/official_texts_156624.htm [26.09.2020].

9 "London Declaration Issued by Heads of State and Government participating in the meeting of the North Atlantic Council in London 3-4 December 2019", North Atlantic Treaty Organization, 4 December 2019, paragraph 4, https://www.nato.int/cps/en/natohq/official_texts_171584.htm [26.09.2020].

unpeace that it wishes to impose on Europe. It must also be ready to respond should Russia miscalculate that the political and military risks of aggression are manageable. To deter or successfully defend on its eastern flank, NATO and Allies must address the responsiveness, scalability, and multi-spectrum power of the Russian Armed Forces within the context of the ongoing Russian destabilization campaign that would intensify in time of war.

Russia's Destabilization Campaign: Achieve Strategic Aims without War while Setting Favourable Conditions for War

It is now evident that Russia was reluctantly quiescent and not willingly cooperative during the immediate post-Cold War period. Moscow viewed most of the main elements of the post-Cold War Euro-Atlantic project as inimical to Russian interests. Looking back on this time, President Putin said in his 2018 speech to the Federal Assembly, in which he announced Russia's new strategic nuclear weapons, that

"Apparently, our partners got the impression that it was impossible in the foreseeable historical perspective for our country to revive its economy, industry, defence industry and armed forces to levels supporting the necessary strategic potential. And if that is the case, there is no point in reckoning with Russia's opinion, it is necessary to further pursue unilateral military advantage in order to dictate terms in every sphere in the future."

He went on to say, "No, nobody really wanted to talk to us about the core problem, and nobody wanted to listen to us. So, listen now."[10]

As soon as it was economically possible, almost entirely due to a windfall from rising oil prices, Russia began a massive military reform and modernization effort. Russia is now making itself heard in the West in many ways, including via an ongoing strategic destabilization campaign in which its revived military power is a major element.

The major milestones of Russia's destabilization campaign in Europe during 2007 to 2021 include:

- February 2007: President Putin's Munich speech
- April 2007: Mass cyberattacks against Estonia
- August 2007 Strategic bomber patrols re-started
- December 2007: Suspension of CFE compliance
- August 2008: Russia-Georgia conflict
- September 2009: ZAPAD exercise series re-started
- February 2014: Aggression against Ukraine
- October 2015 Syrian intervention
- April 2018: Salisbury nerve agent attack
- August 2019: End of INF Treaty
- August 2020: Belarus

This campaign is most often referred to in the West as "hybrid war."[11] The destabilization campaign aims to overturn the existing

[10] V. Putin, "Presidential Address to the Federal Assembly", 1 March 2018, Kremlin website, http://en.kremlin/events/president/news/56957 [26.09.2020].

[11] President Putin used the term "controlled chaos" in his published manifesto on future defence policy just prior to the 2012 presidential elections; V. Putin, "Byt' Sil'nymi: Garantii Natsional'noi Bezopasnosti Dlia Rossii", *Rossiskaya Gazeta*, No. 5708 (35), 20 February 2012, http://www.rg.ru/2012/02/20/putin-armiya.html [26.09.2020]. "Controlled chaos" is now in wide use among

global order, which Russia finds inimical to its strategic interests. It includes all the well-known elements, such as information war, political meddling, cyberattacks, energy blackmail, espionage, assassination, and more of what the Russians call "active measures."[12] Military power, including exercises and operations, shows of force, and nuclear sabre-rattling, is a major element of the strategic destabilization campaign. The strategic destabilization campaign includes military provocations to test NATO reactions and defences and carefully calibrated (so far) limited military actions intended to stay below the threshold for an Article 5 response by NATO. The entire campaign, which creates conditions of neither peace nor war – unpeace – is protected by threatened military aggression and a nuclear shadow.[13] The military threat is felt most acutely on NA-

Russia's military leadership and analysts, as in A. N. Belskii and O. V. Klimenko, "Politicheskiie Tekhnologii "Tsvetnykh Revolutsii": Puti i Sredsvta Protivodeistviia", *Voennaya Mysl'*, No. 9, September 2014, pp. 3-11. An extended analysis of the related, and somewhat interchangeable term, "strategy of attrition and destruction" is in V. I. Vorob'ev and V. A. Kitselev, "Strategii Sokrusheniia i Izmora v Novom Oblike", *Voennaya Mysl'*, No. 3, March 2014, pp. 45-57. While generally using these terms, Russian analysts recognise the western use of "hybrid" to identify similar phenomena. Russian experts tend to use "controlled chaos" and "technology of colour revolutions" to label actions directed against Russia or governments friendly to Russia, and they refer to the same means and methods as part of "new forms of armed conflict" and "new generation warfare" when discussing modifications to Russia's approach to conflict/war.

12 J. Kitfield, "NATO Ops Center Goes 24/7 To Counter Russians: Gen. Scaparrotti", *Breaking Defense*, 1 October 2018, https://breakingdefense.com/2018/10/nato-ops-center-goes-24-7-to-counter-russians-gen-scaparrotti/ [26.09.2020]. See also K. B. Payne and J. Foster, "Russian strategy – expansion, crisis and conflict", *Comparative Strategy*, Vol. 36, No. 1, 2017; pp. 1-89; Brussels Summit Declaration, para. 2.

13 The seven phases of a new generation warfare campaign are described in D. Adamsky, "From Moscow with Coercion: Russian Deterrence Theory and Strategic Culture", *Journal of Strategic Studies*, Vol. 41, Nos. 1-2, pp. 39-43 and J. Berzins, National Defence Academy of Latvia, Center for Security and Strategic Research, Policy Paper no. 2, April 2014, p. 6. The strategic destabilization campaign is arguably a protracted implementation of the first three phases involving

TO's eastern flank within range of potential strategic operations that Russia could conduct from within its own territory to contest or attempt to control large swathes of NATO territory and international waters and air space.[14]

The non-kinetic dimension of Russia's strategic destabilization campaign against the West risks serious escalation. Hybrid war became the buzz phrase after Crimea and Russian hybrid warfare has been widely misinterpreted as war-minus.[15] The actual Russian approach to hybrid war is war-plus – diplomatic, informational, subversive, and cyber-based approaches, etc. – combined with threatened or actual military force. Russia's attack on transatlantic security and stability and its growing regional presence well beyond its periphery are always backed by military power and a nuclear shadow.

The non-military and military elements of the strategic destabilization campaign are integrated conceptually and operationally. The Chief of the Russian General Staff, General Gerasimov, has clarified Russian views on the supported-versus-supporting roles of non-military and military means in non-military and direct military conflict, and how those roles shift in line with the circumstances. According to him, modern conflicts (below the level of direct military confrontation) are "conducted by the integrated employment of political, economic, informational, and other non-military means, all implemented with reliance on military force." However, when

information-psychological struggle, indirect political, economic, and informational actions to influence the mind-set of the adversary's public.

14 Western analysts refer to the capabilities aggregated in some of Russia's strategic operations concepts as A2/AD, and the contested or controlled areas they create as A2/AD "bubbles".

15 Timothy Snyder makes this astute observation in T. Snyder, "The Road to Unfreedom", Tim Duggan Books, New York, 2018, p. 193.

it comes to the preparation for and conduct of war, "non-military means, which influence the course and outcome of wars, provide and create the conditions for the effective use of military force." War is conducted "on the basis of coordinated employment of military and non-military means with the decisive role of the armed forces."

General Gerasimov has highlighted in particular the role that information confrontation can play in undermining an adversary's security. The Russian Ministry of Defence defines information confrontation as "an integral part of relations and a form of battle of the parties (state, social and political movements and organizations, armed forces, etc.), each of which seeks to inflict defeat (damage) by means of information effects on its information sphere (the totality of information, information infrastructure, entities involved in the collection, formation, distribution and use of information, as well as the regulatory system for the resulting social relations), (while) fending off or reducing such an impact on its part."[16]

On the role of information confrontation and its intended effects, General Gerasimov has said that "the information domain, not having a clearly defined international border, provides the possibility for long-range, hidden action upon not only critically important information infrastructure, but also upon the population of a country,

[16] Russian Ministry of Defence website, Military Dictionary, Information Confrontation (информационная противоборство), https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=5221@morfDictionary [26.09.2020]. As one example of how Russia uses information confrontation against NATO, an assessment of Russian information confrontation approaches against NATO and its nuclear sharing arrangements can be found in L. Kucharski, "Russian Multi-Domain Strategy Against NATO: Information Confrontation and US Forward-Deployed Nuclear Weapons in Europe", The Center for Global Security Research, Lawrence Livermore National Laboratory, 2018, https://cgsr.llnl.gov/content/assets/docs/4Feb_IPb_against_NATO_nuclear_posture.pdf [26.09.2020].

directly influencing the condition of national security of a state."[17] The Russian Minister of Defence announced the creation of Information Operations Forces in early 2017, strengthening the Russian military's already robust information operations. Russia's information operations are so extensive that the information sphere arguably constitutes Russia's virtual sixth military district – an Information Military District where deep operations against an adversary are carried out in the cognitive and psychological domains.[18] In addition to their aim to gradually erode the security of adversary states in peacetime, information operations have the potential in crises or conflict to slow or paralyze the ability of adversaries to observe, assess, decide, and act.

At the time of this writing, another scenario of destabilization and intervention is playing out on Russia's border in the vicinity of NATO, this time in Belarus. The unfolding situation after the contested 2020 presidential elections there remains fluid and unpredictable, with Russia applying calibrated pressure to ensure that the ultimate outcome favours its geopolitical position in the region. President Putin has noted that Russia has core interests in Belarus, has indicated his preparedness to intervene to restore order if nec-

17 Valerii Gerasimov, "Vektory Razvitiya Voennoi Strategii", *Krasnaya Zvezda*, 4 March 2019, http://redstar.ru/vektory-razvitiya-voennoj-strategii/ [26.09.2020].

18 See: I. Panarin, "O Sisteme Informatsionnogo Protivoborstva Rossii", *Vzglyad Delovaya Gazeta*, 28 February 2017, https://vz.ru/opinions/2017/2/28/859871.html [26.09.2020]; "Shoygu Ob'yavil o Sozdanii Voisk Informatsionnykh Operatsii", 22 April 2017, TASS; http://tass.ru/armiya-i-opk/4045814 [26.09.2020]; and "V Minoborony Sozdali Voiska Informatsionnye Operatstii", INTERFAX, http://www.interfax.ru/russia/551054 [26.09.2020]. On the information sphere as Russia's virtual sixth military district, see D. Johnson, "ZAPAD 2017 and Euro-Atlantic Security", *NATO Review*, 14 December 2017, https://www.nato.int/docu/review/articles/2017/12/14/zapad-2017-and-euro-atlantic-security/index.html [26.09.2020].

essary, and has warned against interference by others.[19] On the basis of its ongoing destabilization operations and its establishment of high readiness military forces capable of rapidly implementing operations of various scales on and beyond its borders, Russia has a wide range of options to bring to bear to prevent the "loss" of Belarus to the West.[20] Meanwhile, the struggle between popular democratic forces and Lukashenko and his Russian backers is creating another zone of instability and unpredictability on NATO's borders with potential long-term implications for the security of Allies.

In summary, Russian concepts for and implementation of conflict below the level of direct military conflict (war) are the context for NATO's current efforts to strengthen its deterrence and defence. Moscow is conducting its ongoing destabilization campaign across multiple domains that extend well beyond NATO's eastern flank including "long-range, hidden action," in particular in the information sphere, in order to translate "incremental gains at the operational level of the strategy into strategic gains"[21] in its long-term conflict with NATO. Many aspects of the destabilization campaign do not fall within NATO's collective defence task but nevertheless, have bearing on its long-term sustainability. NATO and Allies must remain vigilant against its potential effects on the political unity of

19 "Pozdravlenie Aleksandru Lukashenko c Podedoi na Vyborakh Prezidenta Belorusii", Kremlin website, 10 August 2020, http://kremlin.ru/events/president/news/63872 [26.09.2020].

20 Not all are military. See, for example, H. Liubakova, "Russia May Not Need to Invade Belarus. It's Already There", *The Washington Post*, 26 August 2020, https://www.washingtonpost.com/opinions/2020/08/26/russia-may-not-need-invade-belarus-its-already-there/ [26.09.2020].

21 On Russia's destabilization campaign or "gray zone" approach, see B. Roberts, "On Theories of Victory, Red and Blue", Livermore Papers on Global Security No. 7, Lawrence Livermore National Laboratory Center for Global Security Research, June 2020, pp. 82-90. The partial quote can be found on pages 84-85.

the Alliance and the collective resolve of Allies to sustain credible and effective deterrence and defence.

Russia's Preparations for War: Prepare to Capture and Retain the Strategic Initiative Should War Become Necessary or Opportune

Russia has invested enormous political will and finances in building an increasingly capable, full-spectrum military.[22] In the circumstances of unpeace created by Russia's strategic destabilization campaign, the armed forces complement Russia's non-military levers of power by adding coercive and intimidating elements. In keeping with its desire to achieve strategic aims without war, Russia has so far calibrated its military actions to remain carefully below the threshold for a collective response by NATO, preferring an approach that recalls Thomas Schelling's description of a "competition in risk-taking, a military-diplomatic manoeuvre with or without military engagement but with the outcome determined more by the manipulation of risk than by an actual contest of force."[23]

In support of that approach, the Russian military is ready if its leadership decides to take risks. The Russian Armed Forces are now

[22] On Russia's military revival and ongoing modernization, see, for example: G. Gressel, "Russia's Quiet Military Revolution, and What it Means for Europe", European Council on Foreign Relations, ECFR 143, October 2015, https://www.ecfr.eu/publications/summary/russias_quiet_military_revolution_and_what_it_means_for_europe4045 [26.09.2020]; K. Ven Bruusgaard, "Crimea and Russia's Strategic Overhaul", *Parameters* 44(3), Autumn 2014, pp. 81-90; and F. Westerlund and S. Oxenstierna (eds.), "Russian Military Capability in a Ten-Year Perspective" – 2019, FOI-R-4758-SE, December 2019.

[23] Thomas C. Schelling, "Arms and Influence", New Haven, Yale University Press, 2008, p. 166.

structured, trained, and equipped to respond quickly and effectively in the event that Russia's vital interests are threatened, as in Ukraine, or when the political and military risks of an opportunity are assessed as manageable, as in Syria. While equipped and trained for the most challenging scenario of large-scale conflict against a technologically advanced adversary, the Russian military is able to execute scalable options quickly in reaction to a wide range of scenarios. This ability is supported by Russia's military acquisitions, force structure and posture, exercises, and operations, which appear to be aimed at achieving maximum flexibility. This prepares the military forces to operate effectively in low-intensity special operations such as the seizure of Crimea, low-to-mid intensity operations such as in Donbas, mid-intensity operations in distant theatres such as Syria, and high-intensity operations in regional or large-scale wars such as those that Russia exercises against NATO. This spectrum of potential intensity is key to understanding Russian military preparations for future war.[24]

Readiness

As part of its efforts to ensure rapid response, Russia has maintained its armed forces and, increasingly, the government, in a state of readiness at or near a war footing since early 2014. This state of readiness corresponds to Moscow's perception of the potential for military conflict to erupt suddenly and escalate quickly. This also reflects the state of unpeace created while "the Kremlin has been

[24] See V. Gerasimov, "Sovremennye Voiny in Aktual'nye Voprosy Oborony Strany", *Vestnik Akademii Nauk*, No. 2 (59), 2017, pp. 9-13.

de facto operating in a war mode" in the conduct of its destabilization campaign against the United States and its NATO Allies.[25] In response, Moscow has put in place structures and procedures to put the government on a war footing, including a de facto revival of the wartime STAVKA (the Soviet High Command), establishment and empowerment of the National Centre for Direction of Defence, and the streamlining of military alert procedures.[26]

Russia intends to fight in higher intensity conflicts with a "whole of nation" approach. The three-pillar national security sphere unites government, military, and nation (populace) and was first enacted in the 2009 National Security Strategy and supporting strategic documents, including the updated 2014 Military Doctrine.[27]

[25] For a review of the many dimensions and the aims of the confrontation as conducted by Moscow, see D. Trenin, "A Five-Year Outlook for Russian Foreign Policy: Demands, Drivers, and Influences", Carnegie Moscow, Center Task Force White Paper, March 2016; and "Demands on Russian Foreign Policy and Its Drivers: Looking Out Five Years", Carnegie Moscow Center, October 2017. The quote may be found on page 1 of the first reference and page 2 of the second reference.

[26] D. Johnson, "Russia's Approach to Conflict – Implications for NATO's Deterrence and Defence", NATO Defense College, Research Paper 111, April 2015, http://www.ndc.nato.int/news/news.php?icode=797, pp. 4-5 and pp. 10-11 [26.09.2020]. The STAVKA was the highest organ for strategic direction of Soviet Armed Forces during World War 2, subordinate only to the State Defence Committee. See "Voenniy Entsikopedicheskiy Slovar'", Voennoye Izdatel'stvo, Moscow, 1986, p. 703; S. M. Shtemenko, "General'niy Shtab v Godiy Voiniy", Voennoe Izdatel'stvo, Moscow, 1968, p. 29 and pp. 34-35; and J. Erickson, "The Soviet High Command: A Military-Political History, 1918-1941", Frank Cass, London, 2001, pp. 597-617 and 602-603. The revived de facto STAVKA likely comprises President Putin, the Minister of Defence and the Chief of the General Staff, the Chiefs of the Services and Branches, and perhaps a few other high-ranking officers from the Defence Collegium. The STAVKA's control of operations in strategic directions would be executed through the General Staff, apparently with overall national defence enabled by the National Centre for Direction of Defence and the supporting legislation empowering the General Staff as the coordinating authority for national defence across all power ministries.

[27] S. I. Skokov, L. V. Grushka, "Vliianiye Kontseptsii Setetsentrizma na Evoliutsii i Funktsionirovaniie Sistemy Upravleniia Vooruzhenymi Silami Rossiiskoi Federatsii", *Voennaya Mysl'*, No. 12, December 2014, pp. 33-41.

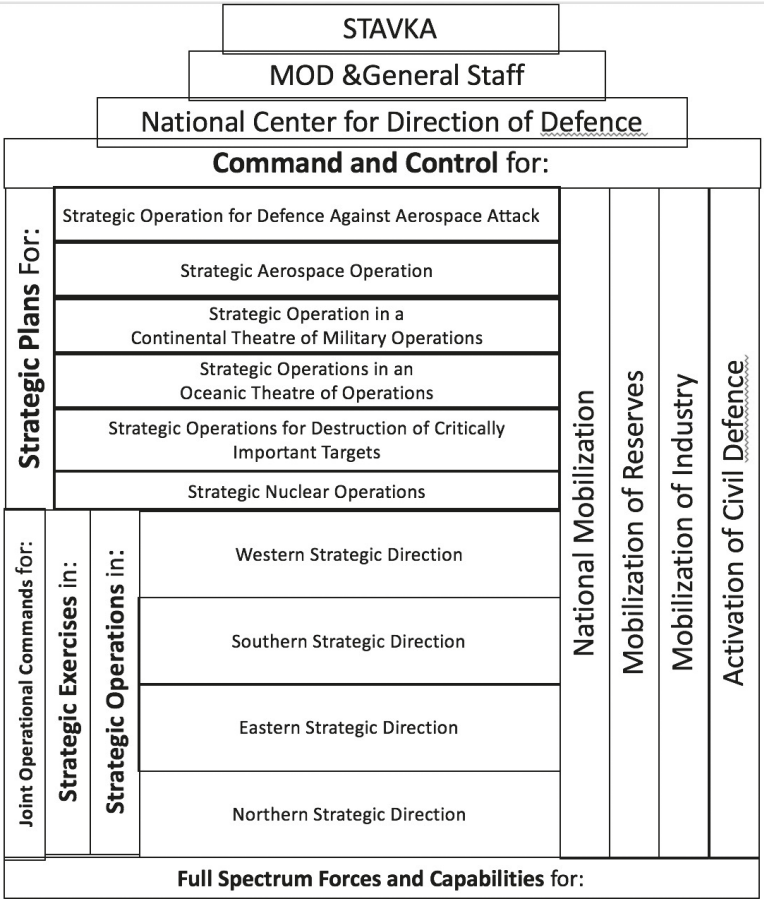

Figure 1. Russia is prepared for a rapid transition from peace to war[28]

This concept, which goes beyond the "whole of government" approach discussed in the West, is reflected in practice in the increas-

[28] The author, drawing upon official statements and Russian military writings, prepared this illustration of the various elements of Russia's military posture.

ing centralisation of decision-making; the control of media and suppression of dissent; rhetorical and practical preparations to mobilize the government, economy, military, and society for war; and the increasing militarisation of Russian society.[29] The military components of this approach to national readiness include flexible and responsive national command and control, operational command structures, high-readiness full-spectrum capability forces, plans for strategic operations, regular strategic exercises, and preparations for national and industrial mobilization (see figure 1). Lesser contingencies can be managed within the set of capabilities developed to respond to the most challenging scenario.

Command and Control

Adapted command and control, specifically, Russia's National Centre for Direction of Defence (NCDD), has an important role in supporting political-military decision-making for quick military implementation. The National Centre for Direction of the Defence of the Russian Federation (NCDD), with subordinate centres in the military districts and administrative regions, is the military element of the unified information space. It has served as the C2 hub of Russian military exercises and operations since early 2014. The NCDD began

[29] D. Johnson, "Russia's Conventional Precision Strike Capabilities, Regional Crises, and Nuclear Thresholds", Livermore Papers on Global Security No. 3, Lawrence Livermore National Laboratory Center for Global Security Research, February 2018, pp. 16-17.

24/7 combat watch on a test basis from 28 March 2014 and upgraded to full operational capability on 1 December 2014.[30]

One role of the NCDD is to maintain constant situational awareness to support routine and crisis decision-making. While the exact division of labour between the NCDD and other command posts is unclear, it would seem to play a significant role in conveying as much context as possible to Russia's NCA during the crisis. Its establishment is part of Russia's response to the demands of net-centric warfare, along with force-wide communications upgrades and heavy investment in C4ISR. The NCDD is an important enabler for Russia's close coordination and integration of forces at all levels of conflict and so an important tool for managing strategic deterrence along the conventional – non-nuclear (precision conventional strike) – nuclear spectrum.[31] General Gerasimov has said that the National Centre for Direction of Defence makes the notion of a "combat alert" order meaningless because the NCDD constantly maintains many of the steps toward readiness that, in the past, would have been necessary

[30] "Ministr Oborony Rossii General Armii Sergei Shoigu Provel Ocherednoie Selektornoie Soveschaniie", 31 March 2014, http://function.mil.ru/news_page/country/ more.htm?id=11913366@egNews [26.09.2020] and "Na Boievoie Dezhurstvo Zastupila Operativnaia Dezhurnaia Smena Natsional'nogo Tsentra Upravleniia Oboronoi Rossii", Russian Ministery of Defense Website, 1 December 2014, http://function.mil.ru/news_page/country/more.htm?id=12002205@egNews [26.09.2020].

[31] For example, according to the Chief of Staff of the Strategic Rocket Forces (SRF), the SRF Central Command Post continued to operate as usual after activation of the NCDD, though he added that the NCDD would increase the effectiveness of SRF forces on watch. "Vvod v Stroi Natsional'nogo Tsentra Upravleniya Oboronoi Rossii Povysit Effektivnost' Raboty Dezhurnykh Sil RVSN", *Krasnaya Zvezda*, 3 December 2014, http://www.redstar.ru/index.php/news-menu/vesti/tablo-dnya/item/20315-vvod-v-stroj-natsionalnogo-tsentra-upravleniya-oboronoj-rossii-povysit-effektivnost-raboty-dezhurnykh-sil-rvsn [26.09.2020].

to take after an alert order.[32] Collectively, the mission and capabilities of the NCDD represent a potentially significant enhancement to the crisis decision-making capability of Russia's National Command Authority.

Exercises

Russia regularly trains its military muscle groups for the potential main event. The Russian military reforms launched after Russia's 2008 war against Georgia initiated the current program of annual strategic exercises in 2009, beginning with ZAPAD that autumn.[33] This created the system to test combat readiness of the military districts and associated military command structures from the national to the brigade level. In 2010, Russia restructured the five military districts into four and simultaneously designated them as Joint Strategic Commands (JSCs).[34] The JSCs comprise joint combat forces at high readiness to operate in their assigned strategic direction or to deploy in support of operations in other strategic directions.

[32] "Nachal'nik Rossiiskogo Genshtaba Rasskazal Zhurnalistam o Zadachakh i Roli Natsional'nogo Tsentra po Upravleniiu Oboronoi RF", 1 November 2014, http://function.mil.ru/news_page/country/more.htm?id=11998309@egNews [26.09.2020]; N. E. Solovtsov and V. T. Nosov, "Rol' I Mesto RVSN v Vooruzhennykh Silakh Rossii", *Voennaya Mysl'*, No. 9, Nov-Dec 1994, p. 75.

[33] KAVKAZ 2008 was a cover for force movements in advance of Russian operations against Georgia in August 2008 rather than the first exercise in the cycle initiated in 2009 as part of the response to the shortfalls identified during operations against Georgian forces. Similarly, ZAPAD 1999 was conducted as a stand-alone event, partly as a show of force in the context of NATO's air campaign against the Former Republic of Yugoslavia.

[34] The Military Districts are also designated Joint Strategic Commands (JSCs). The number of Military Districts increased to five again in December 2014 when the Northern Fleet Military District was created. As of 2019, the Northern Fleet MD has not been integrated as the lead MD into the annual strategic exercise rotation. It has participated in snap exercises, exercised concurrently with ZAPAD 2017, and participated directly in VOSTOK 2018.

The scheduled strategic exercises (ZAPAD, VOSTOK, TSENTR, KAVKAZ) are the capstone events of the Russian Armed Forces' annual training cycle. The exercises have evolved over the past ten years to include strategic mobilization and deployment, larger and more complex joint military manoeuvres, reserve mobilization, industrial mobilization, and civil defence. During the several weeks of their duration, the exercises fulfil the General Staff's presidentially mandated task to organize and test the transition of the Russian Federation from peace to war. After completing the transition, the exercises test national preparedness for large-scale, high-intensity warfare against a technologically advanced peer adversary. The Russian Armed Forces also conduct snap (surprise) exercises testing the same elements as the scheduled exercises, with an increased emphasis on readiness as a key element of counter-surprise capability. In 2014, Defence Minister Shoygu said that the snap exercises are intended to demonstrate the capability to deploy 65,000 troops over a distance of 3,000 kilometres within 72 hours.[35] Some of the snap exercises have been as large as or larger than scheduled annual strategic exercises in the number of participating forces.[36] The snap exercises themselves are strategic exercises and, along with the scheduled annual strategic exercises, constitute an important part of the Russian Armed Forces' system of exercises.

The field training and live-fire phase of the exercises hones the armed forces' warfighting capabilities from the theatre or frontal

[35] "Shoygu Dlozhil Putinu, Skol'ko Voisk Mozhno Operativno Perbrosit' Na Rostoyaniye v Tri Tysiachi Kilometrov", 2 July 2014, http://palm.newsru.com/russia/02jul2014/shoigu.html [26.09.2020].

[36] J. Norberg, "Training for War, Russia's Strategic-Level Military Exercises 2009-2017", Swedish Defence Research Agency (FOI), October 2018, pp. 41-44.

level down to the brigade level. It pulls together the training conducted by the different military branches and services at various unit levels during the previous months into a large combined-arms, multi-domain exercise simulating high-intensity conflict. This exercise format tests their combat readiness against a technologically advanced peer adversary.

Within this overall context, it becomes clear that Russia's strategic exercises are not geared toward only local or regional scenarios or even operations in a single strategic direction. While they create forces that can support such contingencies, the exercises are oriented to the most challenging scenario – multi-directional, theatre-level conflict – and their capability and capacity-building effects are strategic. Practical considerations, including financial constraints, rule out force-wide and national mobilization for every exercise. But the strategic exercises effectively simulate nation-wide alerts, thereby improving the ability to take action in an actual national emergency. It is noteworthy that Russia's exercises are unique in Europe for their size and frequency.[37] In other words, they do not respond in kind to a looming NATO menace, as the Russian authorities claim.

Russia's exercises are one means by which operational lessons are adapted, tested, and integrated into military doctrine and approaches and then applied to future operations in an iterative cycle. Russian military leaders have noted how the strategic and snap exercises enabled Russia's rapid intervention in Syria and now assert

[37] D. Ruiz-Palmer, "Theatre Operations, High Commands and Large-Scale Exercises in Soviet and Russian Military Practice: Insights and Implications", Fellowship Monograph 12, NATO Defense College, May 2018, http://www.ndc.nato.int/news/news.php?icode=1172 [26.09.2020].

that lessons from Syria are factored into military exercises.[38] General Gerasimov has said that experience gained in Syrian operations provided the basis for a "strategy of limited actions" for the defence and advancement of national interests beyond the territory of Russia. This strategy, which is to be developed further, would centre on creating an independent group of forces based predominately on whichever service was best suited to the circumstances (in Syria, that was the Aerospace Forces). The strategy of limited actions would emphasize information dominance, rely upon hidden deployment of the group of forces, and aim for the creation of an integrated system of intelligence, strike means, and command and control. This integrated system would enable location, targeting, and selective strike of critically important targets in near real-time by strategic and operational-tactical non-nuclear weapons.[39]

Strategy

General Gerasimov has described a "strategy of active defence" for the employment of the Russian Armed Forces and their growing preparedness for more proactive use of military means "for the

[38] D. Johnson, "VOSTOK 2018: Ten Years of Russian Strategic Exercises and Warfare Preparation", NATO Defense College, NDC Policy Brief No. 3, February 2019, http://www.ndc.nato.int/news/news.php?icode=1264 [26.09.2020]. On the influence of Syrian operations in Russian military thinking and of related lessons in Russian exercises, see D. Adamsky, "Russian Campaign in Syria – Change and Continuity in Strategic Culture", *Journal of Strategic Studies*, 43:1, pp. 104-125 and footnote 43, https://doi.org/10.1080/01402390.2019.1668273 [26.09.2020].

[39] V. Gerasimov, "Vektory Razvitiya Voennoi Strategii", *Krasnaya Zvezda*, 4 March 2019, http://redstar.ru/vektory-razvitiya-voennoj-strategii/ [26.09.2020] quoted in D. Johnson, "General Gerasimov on the Vectors of the Development of Military Strategy", NATO Defense College Russian Studies Series 4/19, 2 March 2019, http://www.ndc.nato.int/research/research.php?icode=585 [26.09.2020].

pre-emptive neutralization of threats." The strategy comprises "integrated means for the pre-emptive neutralization of threats to the security of the state" and is guided by principles for:

- prevention of war – strategic foresight to enable timely response to emerging threats;
- preparation for war – constant high combat readiness and readiness for mobilization of the armed forces and creation of strategic reserves and stockpiles;
- the conduct of war – coordinated employment of military and non-military means acting on the basis of surprise, decisiveness, and continuity of strategic action.

Describing implementation of the active defence strategy in conflict, General Gerasimov has said that, "acting quickly, we should preempt the enemy with our preventive measures, promptly identify his vulnerabilities and create threats of unacceptable damage to him. This ensures the capture and retention of the strategic initiative."[40]

NATO's eastern flank

The security of NATO's eastern flank must be continuously assessed in its complete context, taking into account the factors described above. Russia today can concentrate large forces relatively quickly anywhere on its periphery, under a nuclear shadow and with robust anti-access/area denial (A2/AD) capabilities aimed at preventing an adversary from traversing or liberating an area subjugated by Mos-

[40] V. Gerasimov, "Vektory Razvitiya…" See also M. Garberg Bredesen and K. Friis, "Strike First and Strike Hard? Russian Military Modernisation and Strategy of Active Defence", FRIVARLD Briefing No. 10 2019, 2 December 2019, https://frivarld.se/rapporter/strike-first-and-strike-hard-russian-military-modernization-and-strategy-of-active-defence/ [26.09.2020].

cow. Leveraging this capability, Russia is implementing a multi-dimensional strategic destabilization campaign in the Euro-Atlantic space to achieve its foreign, security, and defence policy aims.

Within this broader context, the security of NATO's eastern flank is shaped, in part, by regional geography and the disposition of forces in Russia's Western Military District (WMD). Both lend themselves to the well-known fait accompli scenarios explored in various western analyses. These scenarios note the potential for Russia to achieve temporary local superiority on the basis of its time and distance advantage and revived strategic mobility which would support rapid reinforcement of the WMD from other military districts. It is generally assumed that Russia would find it challenging if not impossible to oppose NATO's full mobilization potential in a protracted conflict.[41] However, Russia's preferred course of action should direct military conflict with NATO be unavoidable, would be to secure limited gains and terminate the conflict on terms acceptable to itself by inflicting deterrent levels of damage on the adversary with conventional precision strike weapons and threatening the employment of nuclear weapons.[42]

The security of NATO's eastern flank is further complicated by the uncertainty and ambiguity that Russia has deliberately imposed on the region through its large-scale strategic and snap exercises. Russia's elastic and creative approach to exercise notification re-

[41] See, for example, C. Reach, V. Kilambi and M. Kozad, "Russian Assessments and Applications of the Correlation of Forces and Means", RAND RR4235, pp. 109-130.

[42] See B. Roberts, "On Theories of Victory, Red and Blue", pp. 42-64; D. Johnson, "Russia's Conventional Precision Strike Capabilities, Regional Crises, and Nuclear Thresholds", pp. 63-91; K. Zysk, "Escalation and Nuclear Weapons in Russia's Military Strategy", *RUSI Journal*, Vol. 163, Issue 2, 2018, pp. 4-15.

quirements, the surprise aspect of the snap exercises, and the scale of forces mobilized in proximity to NATO during exercises in the Western, Southern, and Northern Fleet Military Districts have reduced regional stability. Threat perceptions are further sharpened by Russia's pattern of using exercises to mask preparations for use of military force, as in Georgia in 2008 and Ukraine in 2014.

NATO's eastern flank consequently lies at the epicentre of the complex factors outlined above and due to Russia's destabilization campaign, its proprietary views toward the region, and Russia's military reach to and beyond its borders. This presents NATO and Allies the dual challenges of countering Russia's destabilization campaign and rejecting the state of unpeace it tries to impose while maintaining a credible and effective deterrence and defence posture ready to respond to any contingency.

Conclusions and Recommendations

> It is evident today that the line is blurred between the state of war and peace.
>
> *Valerii Gerasimov*[43]

> The distinction between war and peace is the foundation of civilized life, and its observance rests on common moral and political standards.
>
> *Martin Wight*[44]

[43] V. Gerasimov, "Sovremennye Voiny I Aktual'nye Voprosy Oborony Strany", *Vestnik Akademii Voennykh Nauk*, No. 2 (59), 2017, p. 11.

[44] M. Wight, "Power Politics", Hedley Bull and Carsten Holbraad (eds.), London, Leicester University Press for the Royal Institute of International Affairs, 1978, p. 141.

This is where NATO-Russia relations stand in the deterrence and defence dimension – NATO faces a security environment in which Russia is conducting a strategic destabilization campaign against the West while flexing its military muscles in order to impose a state of unpeace in the Euro-Atlantic space. Russia is contesting the political, informational, and operational dimensions of Euro-Atlantic security and integrates all elements of national power, including some nuclear intimidation, to do so. This is a dangerous and destabilizing mix with significant potential for escalation.

These circumstances are challenging because NATO's mission is collective defence, and it has a secondary role, if any at all, in responding to most elements of the non-military dimension of Russia's destabilization campaign. Nations and the EU are at the forefront of that struggle. However, this approach is asymmetrical to Russia's, which integrates the military and non-military elements, and Moscow may perceive an advantage here, including being able to set the conditions for Russia to seize and retain the strategic initiative at the outset of armed conflict.

Here is where the dilemma comes in – the non-military elements of the Russian strategy also set favourable conditions for employment of military force. During unpeace (before the start of direct military conflict), the non-military elements of the destabilization campaign shape the strategic environment in favour of Russia in the event that the use of military force becomes necessary or opportune. Allies need to address both aspects of Russia's approach.

The current circumstances are not a passing phase. There is no reason to expect Russia's posture toward NATO to change drastically for the better in the mid-to-long term, whether President Putin remains part of the equation or not. Under these circumstances,

deterrence and defence are a major element of NATO-Russia relations and a major subtext of NATO-Russia dialogue. In a way very similar to conclusions reached by Allies in the 1967 Harmel Report, a strengthened NATO deterrence and defence posture is necessary to set the conditions for a return to more stable relations – and will be for some time to come.

President Putin's strategic vision for the future transatlantic security architecture is fairly clear, and it is equally clear that it is inimical to the interests and values of NATO Allies. NATO, therefore, needs an alternate vision for transatlantic security in five years, ten years, and beyond, and how our deterrence and defence posture will support that vision.

When faced with a rising challenge in an earlier era, NATO defined the future tasks of the Alliance in the Harmel Report in 1967. At that time, NATO identified the resolution of the German Question as the central political issue and key to averting a crisis in Europe.[45] It took until 1990, 23 years later, for the strategic vision set out in the Harmel Report to come to fruition and for NATO leaders to be able to declare at the 1990 London Summit that NATO had "entered a new, promising era."[46] In a similar way, the considerations of the evolving strategic environment outlined here should be taken into account while developing any new Strategic Concept.

[45] "The Future Tasks of the Alliance (the Harmel Report), Annex to the Final Communique of the Ministerial Meeting", North Atlantic Treaty Organization, December 1967, paragraph 5, https://www.nato.int/cps/en/natohq/official_texts_26700.htm? [26.09.2020].

[46] "London Declaration on a Transformed North Atlantic Alliance", paragraph 1.

If Allies decide to develop a new Strategic Concept, it should:

- Recognize that, at its core, Russia's effort to impose a state of unpeace in the Euro-Atlantic space through its strategic destabilization campaign represents a clash of values and a differing vision of the future security architecture that, in the long run, has as serious potential implications for Alliance security as Russia's military build-up;
- Adapt NATO's strategy to respond appropriately to both elements of the Russian challenge – the customary deterrence and defence element and the broader challenge of Russia's ongoing strategic destabilization campaign. The latter will require continued enhancement of NATO's cooperation with the EU on addressing the hybrid challenge in order to deny the state of unpeace that Russia wants to impose and to deter Russia from acting with impunity below the kinetic level of aggression;
- Continue to implement on the basis of fulfilment of the defence spending pledge the measures agreed upon at the 2014 Wales Summit and afterwards in order to strengthen NATO's deterrence and defence posture, including more and heavier forces, continued capability enhancement across all domains, ensuring the viability of the Alliance's reinforcement strategy, and maintaining a safe, secure, and effective nuclear deterrent.

References

Adamsky, D., "Russian Campaign in Syria – Change and Continuity in Strategic Culture", *Journal of Strategic Studies*, 43:1, 2019, https://doi.org/10.1080/01402390.2019.1668273.

Adamsky, D., "From Moscow with Coercion: Russian Deterrence Theory and Strategic Culture", *Journal of Strategic Studies*, Vol. 41, Nos. 1-2, 2017, pp. 39-43.

Belskii, A. N., Klimenko, O.V., "Politicheskiie Tekhnologii "Tsvetnykh Revolutsii": Puti i Sredsvta Protivodeistviia", *Voennaya Mysl'*, No. 9, September 2014, pp. 3-11.

Berzins, J., National Defence Academy of Latvia, Center for Security and Strategic Research, Policy Paper no. 2, April 2014, p. 6.

"Brussels Summit Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Brussels 11-12 July 2018", North Atlantic Treaty Organization, 11 July 2018, https://www.nato.int/cps/en/natohq/official_texts_156624.htm.

Erickson, J., "The Soviet High Command: A Military-Political History, 1918-1941", London: Frank Cass, 2001.

"The Future Tasks of the Alliance (the Harmel Report), Annex to the Final Communique of the Ministerial Meeting, North Atlantic Treaty Organization", December 1967, https://www.nato.int/cps/en/natohq/official_texts_26700.htm?.

Garberg Bredesen, M., Friis, K., "Strike First and Strike Hard? Russian Military Modernisation and Strategy of Active Defence", *FRIVARLD Briefing No. 10 2019*, 2 December 2019, https://frivarld.se/rapporter/strike-first-and-strike-hard-russian-military-modernization-and-strategy-of-active-defence/.

Gerasimov, V., "Sovremennye Voiny I Aktual'nye Voprosy Oborony Strany", *Vestnik Akademii Voennykh Nauk*, No. 2 (59), 2017.

Gerasimov, V., "Vektory Razvitiya Voennoi Strategii", *Krasnaya Zvezda*, 4 March 2019, http://redstar.ru/vektory-razvitiya-voennoj-strategii/.

Gressel, G., "Russia's Quiet Military Revolution, and What it Means for Europe", European Council on Foreign Relations, ECFR 143, October 2015, https://www.ecfr.eu/publications/summary/russias_quiet_military_revolution_and_what_it_means_for_europe4045

Johnson, D., "ZAPAD 2017 and Euro-Atlantic Security", *NATO Review*, 14 December 2017, https://www.nato.int/docu/review/articles/2017/12/14/zapad-2017-and-euro-atlantic-security/index.html.

Johnson, D., "Russia's Approach to Conflict – Implications for NATO's Deterrence and Defence", NATO Defense College, Research Paper 111, April 2015, http://www.ndc.nato.int/news/news.php?icode=797.

Johnson, D., "General Gerasimov on the Vectors of the Development of Military Strategy", NATO Defense College Russian Studies Series 4/19, 2 March 2019, http://www.ndc.nato.int/research/research.php?icode=585.

Johnson, D., "Russia's Conventional Precision Strike Capabilities, Regional Crises, and Nuclear Thresholds", Livermore Papers on Global Security No. 3, Lawrence Livermore National Laboratory Center for Global Security Research, February 2018.

Johnson, D., "VOSTOK 2018: Ten Years of Russian Strategic Exercises and Warfare Preparation", NATO Defense College, NDC Policy Brief No. 3, February 2019, http://www.ndc.nato.int/news/news.php?icode=1264.

Kello, L., "The Virtual Weapon and International Order", New Haven: Yale University Press, 2017.

Kitfield, J., "NATO Ops Center Goes 24/7 To Counter Russians: Gen. Scaparrotti", *Breaking Defense*, 1 October 2018, https://breakingdefense.com/2018/10/nato-ops-center-goes-24-7-to-counter-russians-gen-scaparrotti/.

Kucharski, L., "Russian Multi-Domain Strategy Against NATO: Information Confrontation and US Forward-Deployed Nuclear Weapons in Europe", The Center for Global Security Research, Lawrence Livermore National Laboratory, 2018, https://cgsr.llnl.gov/content/assets/docs/4Feb_IPb_against_NATO_nuclear_posture.pdf [26.09.2020].

"London Declaration on a Transformed North Atlantic Alliance Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in London", North Atlantic Treaty Organization, 5-6 July 1990, https://www.nato.int/cps/en/natohq/official_texts_23693.htm?.

"London Declaration Issued by Heads of State and Government participating in the meeting of the North Atlantic Council in London 3-4 December 2019", North Atlantic Treaty Organization, 4 December 2019, https://www.nato.int/cps/en/natohq/official_texts_171584.htm.

Liubakova, H., "Russia May Not Need to Invade Belarus. It's Already There", *The Washington Post*, 26 August 2020, https://www.washingtonpost.com/opinions/2020/08/26/russia-may-not-need-invade-belarus-its-already-there/.

"Ministr Oborony Rossii General Armii Sergei Shoigu Provel Ocherednoie Selektornoie Soveschaniie", Russian Ministry of

Defence, 31 March 2014, http://function.mil.ru/news_page/country/ more.htm?id=11913366@egNews.

"Na Boievoie Dezhurstvo Zastupila Operativnaia Dezhurnaia Smena Natsional'nogo Tsentra Upravleniia Oboronoi Rossii", Russian Ministry of Defence, 1 December 2014, http://function.mil.ru/news_page/country/more.htm?id=12002205@egNews.

"Nachal'nik Rossiiskogo Genshtaba Rasskazal Zhurnalistam o Zadachakh i Roli Natsional'nogo Tsentra po Upravleniiu Oboronoi RF", Russian Ministry of Defence, 1 November 2014, http://function.mil.ru/news_page/ country/more.htm?id=11998309@egNews.

"The NATO-Russia Founding Act", North Atlantic Treaty Organization, 27 May 1997, https://www.nato.int/cps/en/natohq/official_texts_25468.htm?.

"NATO-Russia Relations, A New Quality, Declaration by Heads of State and Government of NATO Member States and the Russian Federation", North Atlantic Treaty Organization, 27 May 2002, https://www.nato.int/cps/en/natohq/official_texts_19572.htm?.

Norberg, J., "Training for War, Russia's Strategic-Level Military Exercises 2009-2017", Swedish Defence Research Agency (FOI), October 2018.

Panarin, I., "O Sisteme Informatsionnogo Protivoborstva Rossii", *Vzglyad Delovaya Gazeta*, 28 February 2017, https://vz.ru/opinions/2017/2/28/859871.html.

Payne, K. B., Foster, J., "Russian strategy – expansion, crisis and conflict", *Comparative Strategy*, Vol.36, No.1, 2017.

"Pozdravlenie Aleksandru Lukashenko c Podedoi na Vyborakh Prezidenta Belorusii", Kremlin website, 10 August 2020, http://kremlin.ru/events/president/news/63872.

Putin, V., "Presidential Address to the Federal Assembly", 1 March 2018, Kremlin website, http://en.kremlin/events/president/news/56957.

Putin, V., "Byt' Sil'nymi: Garantii Natsional'noi Bezopasnosti Dlia Rossii", Rossiskaya Gazeta, No. 5708 (35), 20 February 2012, http://www.rg.ru/2012/02/20/putin-armiya.html.

Roberts, B., "On Theories of Victory, Red and Blue", Livermore Papers on Global Security No. 7, Lawrence Livermore National Laboratory Center for Global Security Research, June 2020.

Reach C., Kilambi, V., Kozad, M., "Russian Assessments and Applications of the Correlation of Forces and Means", RAND RR4235.

Ruiz-Palmer, D., "Theatre Operations, High Commands and Large-Scale Exercises in Soviet and Russian Military Practice: Insights and Implications", Fellowship Monograph 12, NATO Defense College, May 2018, http://www.ndc.nato.int/news/news.php?icode=1172.

Russian Ministry of Defense website, Military Dictionary, Information Confrontation (*информационная противоборство*), https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=5221@morfDictionary.

Schelling, T. C., "Arms and Influence", New Haven: Yale University Press, 2008.

"Shoygu Dlozhil Putinu, Skol'ko Voisk Mozhno Operativno Perbrosit' Na Rostoyaniye v Tri Tysiachi Kilometrov", 2 July 2014, http://palm.newsru.com/russia/02jul2014/shoigu.html.

"Shoygu Ob'yavil o Sozdanii Voisk Informatsionnykh Operatsii", 22 April 2017, TASS, http://tass.ru/armiya-i-opk/4045814.

Shtemenko, S. M., *General'niy Shtab v Godiy Voiniy*, Moscow: Voennoe Izdatel'stvo, 1968.

Skokov, S. I., Grushka, L. V., "Vliianiye Kontseptsii Setetsentrizma na Evoliutsii i Funktsionirovaniie Sistemy Upravleniia Vooruzhenymi Silami Rossiiskoi Federatsii", *Voennaya Mysl'*, No. 12, December 2014.

Snyder, T., "The Road to Unfreedom", New York: Tim Duggan Books, 2018.

Solovtsov, N. E., Nosov, V. T., "Rol' I Mesto RVSN v Vooruzhennykh Silakh Rossii", *Voennaya Mysl'*, No. 9, Nov-Dec 1994.

Trenin, D., "A Five-Year Outlook for Russian Foreign Policy: Demands, Drivers, and Influences", Carnegie Moscow, Center Task Force White Paper, March 2016.

Trenin, D., "Demands on Russian Foreign Policy and Its Drivers: Looking Out Five Years", Carnegie Moscow Center, October 2017.

Ven Bruusgaard, K., "Crimea and Russia's Strategic Overhaul", *Parameters* 44(3), Autumn 2014, pp. 81-90.

"Voenniy Entsikopedicheskiy Slovar'", Moscow: Voennoye Izdatel'stvo, 1986.

"Vvod v Stroi Natsional'nogo Tsentra Upravleniya Oboronoi Rossii Povysit Effektivnost' Raboty Dezhurnykh Sil RVSN", *Krasnaya Zvezda*, 3 December 2014, http://www.redstar.ru/index.php/news-menu/vesti/tablo-dnya/item/20315-vvod-v-stroj-natsionalnogo-tsentra-upravleniya-oboronoj-rossii-povysit-effektivnost-raboty-dezhurnykh-sil-rvsn.

Vorob'ev, V. I., Kitselev, V. A., "Strategii Sokrusheniia i Izmora v Novom Oblike", *Voennaya Mysl'*, No. 3, March 2014, pp. 45-57.

"V Minoborony Sozdali Voiska Informatsionnye Operatstii", INTERFAX, http://www.interfax.ru/russia/551054.

"Wales Summit Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council

in Wales", North Atlantic Treaty Organization, 5 September 2014, https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

Westerlund, F., Oxenstierna, S. (eds.), "Russian Military Capability in a Ten-Year Perspective – 2019", FOI-R-4758-SE, December 2019.

Wight, M., "Power Politics", Bull H., Holbraad C. (eds.), London: Leicester University Press for the Royal Institute of International Affairs, 1978.

Zysk, K., "Escalation and Nuclear Weapons in Russia's Military Strategy", *RUSI Journal*, Vol. 163, Issue 2, 2018.

Michael Rühle

NATO's Response to Hybrid Threats

Michael Rühle – Head of the Hybrid Challenges and Energy Security Section in the NATO International Staff Emerging Security Challenges Division. The author expresses solely his personal views. He would like to thank Clare Roberts and Katie Westwood for many helpful comments and suggestions.

Executive Summary

- Russia's use of hybrid tools in its assault on Ukraine in 2014 forced NATO not only to re-emphasise its core task of collective defence, but also to examine responses to hybrid threats. This is all the more urgent as hybrid campaigns could undermine NATO's collective defence preparations in a crisis, notably along NATO's eastern flank.
- Since 2014 NATO has systematically expanded its hybrid toolbox, which now encompasses, inter alia, enhanced intelligence sharing, a stronger focus on national resilience, the

creation of specific tools (such as Counter Hybrid Support Teams), a more responsive public diplomacy effort, specifically tailored exercises, and closer relations with the European Union.

- Despite this progress, however, more still needs to be done. For example, more thought needs to be given to deterring hybrid threats, most notably to the specific role of the military in a predominantly non-kinetic context. NATO should also take a more actor-specific approach that takes into account a hybrid actor's strategic intent. Such steps should help to "de-mystify" hybrid challenges, as well as enhance NATO's preparedness to cope with them.

Introduction: A Paradigm Shift

The year 2014 was a true watershed year in NATO's history. Within a few months, all three major assumptions that had guided NATO's post-Cold War evolution collapsed. The assumption that Russia would remain essentially benign – an assumption that had already been shattered by the Russia-Georgia war of 2008 – was finally buried with Moscow's annexation of Crimea and its support for the separatists in Eastern Ukraine. Russia's blatant aggression against Ukraine, which was clearly intended to undermine Ukraine's westward orientation, also buried a second assumption: that a new, undivided Europe could be built on the gradual eastward enlargement of NATO and the EU. With Russia's intervention in Ukraine, many observers saw the enlargement process in Europe's east come to a halt, leaving only a handful of smaller countries in the Western Balkans as plausible short-term candidates for NATO membership.

The year 2014 also saw the end of NATO's large-scale operation in Afghanistan, with the International Security Assistance Force (ISAF) turning into a much smaller training mission. The ambivalent results of the Afghanistan engagement shattered yet a third assumption: that NATO would draw its future legitimacy mostly from missions and operations outside Europe. Although the rise of the "Islamic State" (ISIL), which also unfolded over the course of 2014, was a strong reminder that NATO had to remain vigilant for security challenges emanating from outside Europe, the Ukraine-Russia crisis constituted a paradigm shift that leads NATO to the most significant strengthening of its collective defence capacities since the end of the Cold War.

However, there was yet another challenge NATO had to meet: the emergence of hybrid warfare as a new threat to the security of Allies and partner countries. Elements of hybrid warfare had been visible during the 2008 Russia-Georgia war, when Russia combined military and non-military means to weaken its opponent. However, Russia's use of hybrid tactics against Ukraine in early 2014 was different both in terms of intensity and effectiveness. By overtly and covertly employing military and paramilitary forces, supplying separatist groups in Eastern Ukraine, staging cyberattacks, withholding energy supplies, and waging a massive propaganda campaign, Russia provided a textbook example of how non-traditional warfare could be employed effectively to achieve political objectives. Against this background, the references in Russia's military doctrine to the

"integrated use"[1] of military and non-military measures appeared to be much more than a mere description of the characteristics of modern warfare — they accurately described Russia's actions.

Russia's Approach to Hybrid Warfare

Military historians were quick to point out that this approach to warfare was nothing new and that all wars included hybrid elements.[2] Scholars of Soviet history have argued that many of the hallmarks of hybrid warfare, including subversion, disinformation, and economic coercion were central elements of Soviet intelligence operations and were known as "active measures."[3] However, the case of Ukraine showed that new technologies, such as cyber and social media, have enabled these tried and tested subversion strategies to turn into something far more powerful. They provided Russia with a broader range of destabilisation tools, which can be deployed with far greater reach and impact than those used by its Soviet predecessor. Hence, Russia has been using disinformation, political subversion in neighbouring countries, cyberattacks, and hostile operations by intelligence services. In Ukraine, energy was part and parcel of Russia's hybrid toolbox, just as deniable proxy forces, such

1 "Military Doctrine of the Russian Federation", approved by the President of the Russian Federation on December 25, 2014, No. Pr.-2976, https://rusemb.org.uk/press/2029 [04.07.2020].

2 See R. Johnson, "Hybrid War and Its Countermeasures: A Critique of the Literature", *Small Wars & Insurgencies*, Vol. 29, No. 1, 2018, pp. 141-163.

3 See T. Kuzio and P. D'Anieri, "The Sources of Russia's Great Power Politics: Ukraine and the Challenge to the European Order", *E-International Relations Publishing*, Bristol, UK, 2018, https://www.e-ir.info/publication/the-sources-of-russias-great-power-politics-ukraine-and-the-challenge-to-the-european-order/ [05.07.2020].

as the so-called "Wagner Group," were advancing Russian interest in Libya and elsewhere.[4]

The key motivations for Russia's use of hybrid means are not difficult to fathom. Russia sees NATO as a hostile Alliance, all the more so because NATO's enlargement process has gradually reduced Russia's influence in parts of its erstwhile "near abroad." Russia's approach to security, which aims at keeping its neighbours' militaries weak and in a state of limited sovereignty, inevitably clashes with Western approaches, which aim at allowing nations to choose their security alignments without any veto right of a third party. While Russia has formally underwritten all the key documents in this regard, it de facto does not grant countries such as Ukraine or Georgia full sovereignty.

Moreover, with NATO's enhanced Forward Presence (eFP) close to Russia's borders, Russia feels even more compelled to seek ways to undermine NATO's political cohesion. Although NATO's military presence on its eastern flank is modest and can hardly be perceived as a major threat to Russia, Moscow's own worst case logic assumes that NATO Allies could increase their force levels (or those of key military installations, such as Ballistic Missile Defence sites) at any time. In short, Moscow's own siege mentality demands that it stops any further Western "encroachment" into its "zone of privileged

[4] See M. Rühle and J. Grubliauskas, "Energy as a Tool of Hybrid Warfare", *NATO Defense College Research Report* No. 113, April 2015, http://www.ndc.nato.int/download/downloads.php?icode=451 [05.07.2020]; M. Klein, "Private military companies – a growing instrument in Russia's foreign and security policy toolbox", *Hybrid CoE Strategic Analysis* No. 17, June 2019, https://www.hybridcoe.fi/wp-content/uploads/2020/06/Strategic-Analysis-3_2019.pdf [05.07.2020]; "Wagner, shadowy Russian military group, 'fighting in Libya'", BBC News, 7 May 2020, https://www.bbc.com/news/world-africa-52571777 [05.07.2020].

interest" (Medvedev), either by influencing Western policy or disrupting Western unity. While this is to be achieved without risking a direct kinetic conflict, it is obvious that all non-kinetic activity inevitably takes place under the shadow of conventional and nuclear military means.[5]

Another reason that hybrid means are an attractive option for Russia is that, unlike democracies, authoritarian regimes – or "managed democracies" (V. Putin) – command all levers of state power. This does not suggest that each and every hybrid activity is part of a comprehensive strategy, centrally masterminded by the Kremlin.[6] On the contrary, much of what Russia does in the hybrid domain appears opportunistic – a trial-and-error approach that may fail as often as it may succeed. However, Russia's government structure allows it not only to apply an impressive array of diverse hybrid tools but also to do so with a remarkable degree of persistence. When it comes to looking for ever new ways of exploiting Allies' vulnerabilities, Russia shows considerable imagination, as well as the strategic patience to persist even in the face of failure.

5 See J. Durkalec, "Nuclear-backed 'Little Green Men': Nuclear Messaging in the Ukraine Crisis", *Report*, The Polish Institute of International Affairs (PISM), Warsaw, July 2015, https://www.pism.pl/publikacje/Raport_PISM__Nuclear_Backed__Little_Green_Men___Nuclear_Messaging_in_the_Ukraine_Crisis [21.08.2020].

6 See M. Galeotti, "We need to talk about Putin: How the West Gets Him Wrong", London: Ebury Press, 2019; also see H. Klijn and E. Yüksel, "Russia's Hybrid Doctrine: Is the West Barking Up the Wrong Tree?", *Clingendael Op Ed*, 28 November 2019, https://www.clingendael.org/publication/russias-hybrid-doctrine-west-barking-wrong-tree [04.07.2020].

NATO's Counter Hybrid Strategy[7]

Even if Ukraine, due to its internal weakness and its historic, cultural, and geopolitical entanglement with Russia, represented a *sui generis* case of hybrid warfare that was unlikely to be replicated elsewhere, NATO Allies were forced to realise that a new era of competition was dawning. Since NATO's success as a military security provider depended on the political cohesion of its Allies, an opponent could undermine NATO's military preparations by targeting civil society (e.g. through propaganda) and civilian infrastructure (e.g. through cyberattacks). Consequently, at NATO's September 2014 Wales Summit, its first Summit after Russia's illegal annexation of Crimea, the Allies vowed to ensure that NATO was able to effectively address the specific challenges posed by hybrid threats. They also considered it essential that the Alliance possessed "the necessary tools and procedures required to deter and respond effectively to hybrid warfare threats, and the capabilities to reinforce national forces." This would include "enhancing strategic communications, developing exercise scenarios in light of hybrid threats, and strengthening coordination between NATO and other organisations, ... with a view to improving information sharing, political consultations, and staff-to-staff coordination."[8]

[7] Parts of the following segments are based on C. Roberts and M. Rühle, "NATO's Response to Hybrid Threats", *The Alliance Five Years after Crimea: Implementing the Wales Summit Pledges*, M. Ozawa (ed.), *NATO Defense College Research Paper* No. 7, December 2019, pp. 61-69, http://www.ndc.nato.int/download/downloads.php?icode=621 [04.07.2020].

[8] "Wales Summit Declaration", paragraph 13, 5 September 2014, https://www.nato.int/cps/en/natohq/official_texts_112964.htm?mode=pressrelease [04.07.2020]; The Warsaw Summit Declaration, issued on 9 July 2016, contained no less than 13 references to the term "hybrid", https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en [04.07.2020].

At the same time, work began on a "Strategy on NATO's Role in Countering Hybrid Warfare." By defining NATO's responses in three categories – prepare, deter, defend – the classified document provided a robust framework for the development of NATO's counter-hybrid toolkit. The strategy, which was finalised in late 2015, acknowledged the primacy of nations in countering hybrid actions, as well as the role of the broader international community.[9]

Prepare

The Strategy proceeded from the assumption that preparing to counter threats as part of hybrid scenarios would become NATO's regular business. Accordingly, the constant gathering, sharing, and assessment of information and intelligence were going to be major elements of NATO's approach. The challenge was to link seemingly unconnected events, identify them as a potential hybrid campaign, and to support NATO's decision-making accordingly. NATO was also going to support individual Allies' efforts to identify national vulnerabilities and strengthen their own resilience if requested. The Strategy emphasized NATO's role as a hub for expertise, providing support to Allies in areas such as civil preparedness and chemical, biological, radiological, and nuclear (CBRN) incident response, critical infrastructure protection, strategic communications, protection of civilians, cyber defence, energy security, and counterterrorism. The Strategy also underlined the significant role of training, exercises, and education in preparing to counter hybrid threats. This would

[9] For an unclassified summary see "NATO's response to hybrid threats", https://www.nato.int/cps/en/natohq/topics_156338.htm [04.07.2020].

include exercising of decision-making processes and joint military and non-military responses in cooperation with other actors.

Deter

To deter hybrid threats, the Strategy emphasized the need to convince potential adversaries that the consequences of pursuing their aims, in whatever domain, would outweigh the potential gains. While this could include measures taken by the wider international community (e.g. sanctions), NATO itself would continue to increase the readiness and preparedness of its forces as well as strengthen its decision-making process and its command structure as part of its deterrence and defence posture. This would send a strong signal that the Alliance was improving both its political and military responsiveness and its ability to deploy appropriate forces to the right place at the right time.

Defend

In defending against a hybrid attack, NATO's aim would be to contain and limit an adversary's freedom of action and defeat the threat, either alone or as part of an international response. NATO would also assist individual Allies and help mitigate the effects of an attack on civilian populations or critical infrastructure. If an opponent used military force, so would NATO, including in areas other than where the initial hybrid attacks had taken place. However, the overriding goal was to prevent a hybrid conflict from escalating into a military conflagration.

Enlarging NATO's Counter Hybrid Toolbox

While the 2015 Strategy provided a systematic framework for making progress, it had been written in response to the events in Ukraine in 2014 and, inevitably, was somewhat abstract and aspirational. However, the years that followed would lead to a better understanding of hybrid threats, as well as a clearer idea about NATO's responses.

One major step was enhancing intelligence-sharing. The creation of the Joint Intelligence and Security Division (JSID) in 2016, which included a unit dealing specifically with hybrid threats, marked a major step forward in providing Allies with a better capability to "connect the dots." Realising that hybrid threats were both internal and external in nature, nations were increasingly willing to share intelligence about domestic developments. Intelligence assessments were also increasingly used to support committee discussions among Allies on hybrid threats. These developments vindicated what some in NATO had predicted quite some time ago: in an ever more complex security environment, intelligence had to be regarded as a genuine "capability" alongside tanks, drones, or missiles.

Another step was the deepening of NATO-EU relations. As targets of hybrid activities, both institutions quickly grasped the importance of working together on the hybrid dossier. Largely through informal cooperation at a staff-to-staff level, NATO and the EU developed so-called "playbooks" and "operational protocols" to help align their responses to hybrid threats. Mutual briefings on the hybrid landscape, as well as on the specific threat picture (for example, in the cyber domain) led to a closer relationship between the organisations. This cooperation was supported by the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), created by Finland in 2016 specifically to work for NATO and the EU. The Hybrid CoE pro-

vides analyses on hybrid threats, but it also acts as a "safe space" for informal discussions between NATO and EU staff.

NATO also injected more and more hybrid elements into its exercises, thus forcing political and military decision-makers to grapple with the possible tensions between hybrid attacks on individual Allies, the desire to respond collectively, and to do so in an ambiguous information environment. These exercises, some of them conducted parallel to and in coordination with the EU, highlighted the difficulties of military alliances responding to non-kinetic attacks, suggesting that NATO had to re-visit the very notion of "thresholds." They also highlighted the differences between NATO and the EU both in terms of their organisational structure and their working methods. As a consequence, NATO agreed on an even more ambitious exercise regime, including shorter exercises that would also include top-level civilian decision-makers.

Another major element of NATO's approach to countering hybrid threats is the emphasis on allied resilience. As the security of NATO's eastern flank relies on the combination of a rather modest rotational military presence in-theatre and a complex reinforcement effort, a well-orchestrated hybrid campaign against core elements of that reinforcement strategy (e.g. command and control, energy supplies) could achieve a significant degree of disruption. In light of this risk, as well as the fact that most hybrid attacks would target individual nations, NATO has to ensure that each member country is resilient enough to continue playing its role. For example, individual nations must be ready in the event of NATO's preparations to reinforce the Eastern Allies in a crisis. At the 2016 Warsaw Summit, Allies committed to enhancing their resilience "against the full

spectrum of threats, including hybrid threats, from any direction."[10] Resilience was highlighted as essential for deterrence and defence and effective fulfilment of the Alliance's core tasks. Acknowledging that enhancing resiliency was largely a national responsibility, NATO focused on advising Allies and identified seven "baseline requirements"[11] to serve as yardsticks for national self-assessments. These baseline requirements would be updated over time in light of new challenges, such as technical progress in communications or other areas.

NATO's counter hybrid toolbox has been extended further with the introduction of "Counter-Hybrid Support Teams" (CHST). Modelled on already existing advisory teams for resilience or critical infrastructure protection, a CHST consists of civilian experts, drawn from a pool of specialists nominated by allied nations and with appropriate security clearances, who could be deployed on short notice to an ally who requested NATO's support, either in an acute hybrid crisis or in order to assist in building national counter-hybrid capacities. In November 2019 the first CHST deployed to Montenegro, then a new and vulnerable ally. NATO is also contemplating the creation of Military Advisory Teams, which follow a similar logic as their civilian counterparts. These steps demonstrate that NATO

10 "Commitment to enhance resilience", Warsaw, 9 July 2016, https://www.nato.int/cps/en/natohq/official_texts_133180.htm [04.07.2020].

11 See H. Thankey and W. Roepke, "Resilience: The First Line of Defence", *NATO Review*, 27 March 2019, https://www.nato.int/docu/review/2019/Also-in-2019/resilience-the-first-line-of-defence/EN/index.htm [04.07.2020]. The baseline requirements are 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 civil communications systems; 7) resilient civil transportation systems.

is building response options below the threshold of Article 5 of the Washington Treaty.

The question of how to deter hybrid threats is also receiving increasing attention. While resilience would be a major element of a "deterrence by denial" approach, Allies are aware that elements of "deterrence by punishment" have to be explored as well. At the 2016 Warsaw Summit,[12] Allies stated that hybrid attacks could trigger Article 5 of the Washington Treaty. Collective attribution – arguably one of the strongest means of punishing a hybrid actor – remained a delicate issue, as it touched on national sovereignty. However, when Russian agents used a nerve agent to try to kill a former double agent in the British city of Salisbury in March 2018, a joint statement was quickly released condemning the attack and expressing solidarity with the UK. Most NATO and EU member states named Russia as the culprit and NATO Allies and partners expelled more than 140 Russian officials. While it is impossible to know for sure whether such collective attribution ("name and shame") will deter future such acts, Allies have sent the message that hybrid activities come at a price that not all attackers may be willing to pay.

The multifaceted character of hybrid threats also led NATO's leadership to try out new meeting formats, deliberately seeking to go beyond the established formats of Summits of Heads of State and Government as well as Foreign and Defence Ministerials. In May 2019 an informal meeting of the North Atlantic Council brought together for the first time national security advisers and senior national leads for hybrid threats to discuss ways to deal with these

[12] "2016 Warsaw Summit Declaration" (op. cit.), para. 72.

new types of challenges. The meeting underscored the value of a full spectrum approach, requiring expertise of both civil and military threats confronting Allies. It also testified to NATO's willingness to approach hybrid threats in new and innovative ways: unconventional threats required an unconventional approach.

NATO has also started to take a closer look at potential technological game changers, such as artificial intelligence (AI) and "big data" analysis. Although not exclusively related to hybrid threats, the Allies realised that, as in the case of cyberspace (which NATO has recognised as a distinct military domain), new technologies could offer a potential aggressor effective means for disruption or diversion as part of a hybrid campaign. Conversely, developments like AI could also be employed to quickly detect and counter fake news campaigns on the Internet. Accordingly, NATO has adjusted the structure of its International Staff by standing up new units dedicated to innovation and data policy. After having elevated cyber defence and intelligence a few years earlier, these additional changes underscored NATO's determination not to allow an aggressor the opportunity to orchestrate smarter and stealthier attacks.

Spreading disinformation is among the most frequently used tools in Russia's hybrid toolbox. Since the party that launches a disinformation campaign will always have the advantage of the initiative, disinformation campaigns, such as those directed at NATO's eFP, are easy to orchestrate, put NATO on the defensive (at least initially), and, should they fail to create sufficient interest, can quickly be replaced with another false narrative. Hence, NATO aims to detect disinformation campaigns earlier and to detect certain patterns within these campaigns, which helps in determining the next potential target. This also includes sharing analyses with the EU, as well cooperating

closely with the two NATO Centres of Excellence that have particular expertise in this area: the Centre of Excellence on Strategic Communications in Riga and the aforementioned Helsinki-based Centre of Excellence for Countering Hybrid Threats. Moreover, a NATO website called "Setting the Record Straight" serves as a "one-stop shop" for myth-busting factsheets, speeches, interviews, rebuttal statements, videos, and imagery, and is published in several languages, including Russian. Finally, NATO engages media continuously – online, on air, and in print, and also persistently asks media to correct false stories. All of these activities will not stop hostile propaganda, yet they demonstrate that such propaganda will be identified and exposed. And, just as importantly, they also demonstrate that NATO's own narrative ultimately is much more accurate and plausible than that of Russia or other hybrid actors.

NATO is also seeking to draw the military and civilian instruments of power closer together. Although hybrid methods can be applied in crisis and conflict, most hybrid actions are designed to remain below those levels (e.g. NATO Rules of Engagement or Article 5), seeking instead to accrue advantage over time by targeting the victim's systemic vulnerabilities. To deter or counter such actions, NATO needs to change an adversary's decision calculus. This requires a comprehensive set of response options that brings together military and non-military instruments. Such an array of different levers would not only allow for a broader range of responses, but also provide more flexibility in creating operational and strategic dilemmas: if the aim of an attack is to create a dilemma for the defender by forcing him to choose which objective to defend, a Western counter hybrid strategy will be most effective if it confronts the hybrid aggressor with a similarly difficult choice. Accordingly, NATO has

started work on so-called comprehensive preventive and response options. By examining a large spectrum of potential hybrid actions, and by relating the most appropriate civil-military response tools to each of them, a set of measures will be created that should allow for faster decision-making and more tailored responses. Some of these measures might well be asymmetric, i.e. NATO should not only think of responding in kind. While the response to some threats, such as covert or clandestine military attacks, are likely to have a military dimension, others, such as influence campaigns, may require exclusively non-military responses (e.g. legal, financial, or strategic communications). The challenges that this work entails should not be underestimated, however. Making such a comprehensive approach work will require not only political agreement of Allies to trigger the necessary action(s), but also the seamless coordination between NATO's political and military entities in implementing them.

The Challenges Ahead

NATO's approach to hybrid threats since 2014 has seen the consistent expansion of its counter hybrid toolbox, including its relationship with other actors, notably the European Union. However, the complexity of hybrid activities is likely to continue to challenge NATO on various levels.

The Role of the Military

NATO's major tools are military, yet hybrid attacks are intended to remain below the level of a kinetic response. This not only makes deterring such attacks very difficult but also creates a dilemma for NATO that will not be easy to resolve. If hybrid actions, such as cy-

berattacks, fake news campaigns, or electoral interference, are going to become permanent features of interstate competition, the role of military deterrence will be reserved for the "high end" of the deterrence spectrum. In essence, military deterrence will ensure that a hybrid campaign does not escalate into a military conflagration. By contrast, if non-kinetic hybrid attacks are essentially a precursor to a military attack, as events in Ukraine in 2014 suggest, the defender might have to resort to force even in mere anticipation of a pending military attack. But how likely is an early pre-emptive (collective) kinetic response to a hybrid, non-kinetic attack if the hybrid aggressor has sizeable forces of its own? In short, when addressing the security of NATO's eastern flank, the Allies need to give much more thought to the links between non-kinetic campaigns and military instruments. The above-mentioned work on comprehensive preventive response options should go a long way in clarifying the specific role of the military in deterring and countering hybrid threats.

Cooperation with other Actors

NATO alone does not possess all the tools necessary to counter hybrid threats. Therefore, cooperation with other actors, such as the EU and the private sector, is essential. NATO has made considerable progress in this area, as hybrid threats have proven to be a common concern and thus a helpful catalyst for cooperation. However, such cooperation has natural limits owing to different objectives, memberships, and working methods. While formal constraints can be overcome in part by informal cooperation on the working level, certain steps, such as the exchange of classified information, will remain a perennial challenge. By the same token, intelligence sharing, a major tool in countering hybrid threats, will remain limited,

even among close Allies. Despite these constraints, it will be crucial for NATO to become a trusted part of these evolving networks, including public-private partnerships, to address hybrid threats. The goal must be to establish "communities of trust" in which different stakeholders can share confidential information on such attacks and possible countermeasures. In short, while NATO's cooperation with other actors will remain a work in progress, with much improvisation and trial-and-error, the need for a networked approach to hybrid threats is now widely accepted.

The Fuzzy Hybrid Debate

A final challenge remains the fuzzy nature of the Western hybrid debate itself. This debate is characterized by the use of imprecise terminology, sweeping generalisations, and much alarmism.[13] For example, if terms like "hybrid warfare" are used to describe non-military activity, even non-military strategic competition between states becomes a "war." Leaving aside the implications of such a broad-brush approach for international law, this tendency to characterise almost every unwelcome behaviour as a "hybrid threat" or even as "warfare" creates an unduly alarmist outlook that hinders rather than helps a rational debate.[14] It overestimates the success of many hybrid activities, and it risks to underselling NATO's deterrent, as it measures the organization's performance against an illusionary

[13] See M. Rühle, "Deterring Hybrid Threats: The Need for a More Rational Debate", *NATO Defense College Policy Brief* No. 15, July 2019, http://www.ndc.nato.int/download/downloads.php?icode=600 [04.07.2020].

[14] See J. Raitasalo, "America's Constant State of Hybrid War", *The National Interest Online*, 21 March 2019, https://nationalinterest.org/feature/americas-constant-state-hybrid-war-48482 [04.07.2020].

perfectionist yardstick. At NATO's eastern flank in particular, where NATO seeks to signal to Russia that Moscow's eventual use of force will not achieve any viable political objective, an overly nervous debate on Russia's hybrid activities could be self-defeating by making NATO's military deterrence look weaker than it actually is while simultaneously giving Russia a false sense of confidence in probing NATO's defence arrangements via non-kinetic means.

Conclusions

NATO's re-focus on collective defence since 2014 centres on military capabilities and defence expenditures, yet it also sets the stage for a more systematic examination of hybrid challenges and NATO's role in countering them. The way in which progress has been made testifies to the flexibility of NATO: Allies realised early on that hybrid threats required different, sometimes unorthodox approaches and developed their policies accordingly, notably by partnering with the EU.

However, countering hybrid threats is a long-term strategic challenge for NATO and its Allies. Management of these threats needs to become an ongoing endeavour and will require a change in mindset. Allies must move from the deliberate, sequential planning and decision-making processes that have applied to NATO crisis response operations in the post-Cold War era towards a more dynamic approach of continuously updated situational awareness that drives political discussion, option development, decision-making, and political control. To do this effectively, NATO needs to progress from what is currently an all-hazards approach to hybrid threats (i.e. any actor, any tool) to a more focused one that looks at each hybrid ac-

tor as a unique entity. Moreover, the Allies should not only analyse each distinct actor's hybrid tools but also the strategic motivation that lies behind their use. Based on the resulting better understanding of the opponent's strategic intent, packages of measures should be tailored to each specific actor. This will also help the military to better engage in the debate and to develop tools to support Allies in countering non-military threats, whether through the use of special operations, information operations, psychological operations, or others. Such a more focused approach will improve NATO's effectiveness in influencing the cost-benefit analysis of potential hybrid aggressors and better contest the "grey zone" in what has become the modern theatre of operations. In short, if opponents increasingly act in the grey area, NATO can no longer afford to think solely in black and white.

References

"Commitment to enhance resilience. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8-9 July 2016", https://www.nato.int/cps/en/natohq/official_texts_133180.htm.

Durkalec, J., "Nuclear-backed 'Little Green Men': Nuclear Messaging in the Ukraine Crisis", *Report*, Polish Institute of International Affairs (PISM), Warsaw, July 2015, https://www.pism.pl/publikacje/Raport_PISM__Nuclear_Backed__Little_Green_Men___Nuclear_Messaging_in_the_Ukraine_Crisis.

Galeotti, M., "We need to talk about Putin: How the West Gets Him Wrong", London: Ebury Press, 2019.

Johnson, R., "Hybrid War and Its Countermeasures: A Critique of the Literature", *Small Wars & Insurgencies*, Vol. 29, No. 1, 2018, pp. 141-163.

Klein, M., "Private military companies – a growing instrument in Russia's foreign and security policy toolbox", *Hybrid CoE Strategic Analysis* No. 17, June 2019, https://www.hybridcoe.fi/wp-content/uploads/2020/06/Strategic-Analysis-3_2019.pdf.

Klijn, H., Yüksel, E., "Russia's Hybrid Doctrine: Is the West Barking Up the Wrong Tree?", *Clingendael Op Ed*, 28 November 2019, https://www.clingendael.org/publication/russias-hybrid-doctrine-west-barking-wrong-tree.

Kuzio, T., D'Anieri, P., "The Sources of Russia's Great Power Politics: Ukraine and the Challenge to the European Order", *E-International Relations Publishing,* Bristol, UK, 2018, https://www.e-ir.info/publication/the-sources-of-russias-great-power-politics-ukraine-and-the-challenge-to-the-european-order/.

"Military Doctrine of the Russian Federation, approved by the President of the Russian Federation on December 25, 2014, No. Pr.-2976", https://rusemb.org.uk/press/2029.

"NATO's response to hybrid threats", https://www.nato.int/cps/en/natohq/topics_156338.htm.

Ozawa, M. (ed.), "The Alliance Five Years after Crimea: Implementing the Wales Summit Pledges", *NATO Defense College Research Paper* No. 7, December 2019.

Raitasalo, J., "America's Constant State of Hybrid War", *The National Interest Online*, 21 March 2019, https://nationalinterest.org/feature/americas-constant-state-hybrid-war-48482.

Roberts, C., Rühle, M., "NATO's Response to Hybrid Threats", *The Alliance Five Years after Crimea: Implementing the Wales Summit*

Pledges, Ozawa, M. (ed.), *NATO Defense College Research Paper* No. 7, December 2019.

Rühle, M., Grubliauskas, J., "Energy as a Tool of Hybrid Warfare", *NATO Defense College Research Report* No. 113, April 2015, http://www.ndc.nato.int/download/downloads.php?icode=451.

Rühle, M., "Deterring Hybrid Threats: The Need for a More Rational Debate", *NATO Defense College Policy Brief* No. 15, July 2019, http://www.ndc.nato.int/download/downloads.php?icode=600.

Thankey, H., Roepke, W., "Resilience: The First Line of Defence", *NATO Review*, 27 March 2019, https://www.nato.int/docu/review/2019/Also-in-2019/resilience-the-first-line-of-defence/EN/index.htm.

"Wagner, shadowy Russian military group, 'fighting in Libya'", *BBC News*, 7 May 2020, https://www.bbc.com/news/world-africa-52571777.

"Wales Summit Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales", North Atlantic Treaty Organization, 5 September 2014, https://www.nato.int/cps/en/natohq/official_texts_112964.htm?mode=pressrelease.

Dominik P. Jankowski

NATO and the Emerging and Disruptive Technologies Challenge

Dominik P. Jankowski – Political Adviser and Head of the Political Section at the Permanent Delegation of the Republic of Poland to NATO. The views expressed are those of the author and do not necessarily reflect those of the institution he represents.

Executive Summary

- For NATO, the Emerging and Disruptive Technologies (EDTs) are primarily of interest due to their influence on current and future defence capabilities as well as deterrence and defence posture. It is clear that EDTs will affect many of the foundations of deterrence strategy. Indeed, new military technolo-

gies will play a crucial role in future warfighting and building forces that can decisively operate across domains.

- Russia has been closely monitoring the United States as well as China's technological priority areas, while evaluating their long-term consequences, and searching for means to counter them. The current Russian EDTs strategy has been based on two elements: first, countering the third offset strategy with the first offset strategy, which means prioritizing the development of a wide array of both strategic and tactical nuclear weapons systems; second, countering numerous U.S. and Chinese technological initiatives using similar indigenous programs, although more narrowly focused and smaller in scale.
- Disruptive technologies should not be seen in isolation from disruptive strategies. In fact, technologies enable strategies. With Russia, one needs to consider not only advances in high technology for traditional military applications, but also innovations and uses below the level of declared war. Russia's premier disruptive strategy is intimidation.
- The potential EDTs implications for NATO's deterrence and defence remain of primary importance. Indeed, EDTs will provide a greater range of tools for adversaries to challenge and find weaknesses in NATO's posture. At the same time, ease of commercial access to EDTs raises the prospect of new – increasingly confident – state and non-state actors to contest NATO, particularly with increased challenges of attribution.

Introduction

Emerging and disruptive technologies (EDTs) seem simultaneously trendy, powerful, and mysterious. They are often perceived as carrying the potential to revolutionize governmental structures, economies, and life as one knows it. At the same time, scholars and policymakers emphasize that "these technologies may also promote international instability: for instance, by leading to a swift redistribution of wealth around the world; a rapid diffusion of military capabilities or by heightening the risks of military escalation and conflict."[1]

For past decades, NATO and its Allies have enjoyed a technological edge, which has underpinned their collective military security – an advantage resulting from their collective economic, industrial, and academic strengths. NATO's technological edge has always been an essential enabler of its ability to deter and defend against actual and potential adversaries. In October 2019, NATO Defence Ministers expressed concern that this advantage can no longer be taken for granted. In fact, NATO was in danger of losing its technological edge due to a combination of factors, among them a growing determination from peer competitors, especially Russia and China, to drive the future of advanced technologies, including military applications. Availability and knowledge of EDTs, enhanced by rising defence budgets, have provided NATO's adversaries with capabilities to challenge the Alliance politically, militarily, and technologically. Allowing adversaries to gain competitive advantage in the EDTs area

[1] A. Gilli, "Preparing for "NATO-mation": the Atlantic Alliance Toward the Age of Artificial Intelligence", *NATO Defense College Pocy Brief,* No. 4, February 2019, p. 1, http://www.ndc.nato.int/news/news.php?icode=1270 [11.10.2020].

would impede NATO's ability to win on the battlefield, challenge strategic stability, and change the fundamentals of deterrence.

For NATO, EDTs are primarily of interest through their influence on current and future defence capabilities, as well as on deterrence and defence posture. It is clear that EDTs will affect many of the foundations of deterrence strategy. Indeed, new military technologies will play a crucial role in future warfighting and building forces that can decisively operate across domains. At the same time, deeply strategic and practical understanding of the significance of EDTs and their diffusion, as well as extending thinking concerning how science, technology, and international social relations interact to shape and facilitate management of the changing global security landscape, is a pressing need for NATO in the upcoming decade.[2]

Emerging and Disruptive Technologies – the Historical and Theoretical Context

From a historical perspective, technology has driven the changing nature of conflict, but not conflict itself. Technology, as Krazberg's First Law on Technology underscores, is neither good nor bad; nor is it neutral.[3] The offset strategy remains a key concept applied to

[2] P. Breedlove, M. E. Kosal, "Emerging Technologies and National Security: Russia, NATO, & the European Theater", *Governance in an Emerging New World*, G. P. Shultz, J. Cunningham, D. Fedor, J. Timbie (eds.), Hoover Institution, 2019, p. 28, https://www.hoover.org/sites/default/files/issues/resources/emerging_technology_and_americas_national_security_web.pdf [11.10.2020].

[3] "Science & Technology Trends 2020-2040. Exploring the S&T Edge", NATO Science & Technology Organization, March 2020, p. 4, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf [11.10.2020].

national security involving technological capabilities. Offset strategies have used technical innovation to counter the strength of adversaries and deter them. Since World War II one has witnessed three offset strategies.

As articulated by Philip Breedlove and Margaret E. Kosal, "the first offset strategy used a nuclear-based deterrence strategy to offset Soviet land forces, proximity to Europe, and conventional superiority in Europe."[4] The United States strategy relied on massive retaliation and use of nuclear weapons. The second offset strategy began in the 1970s and was needed to counter and deter the Soviet's superior conventional forces and to address Soviet advances in strategic nuclear arsenal and delivery systems. The second offset strategy "invested in the development of stealth aircraft, precision guided munitions, and space-based reconnaissance and navigation capabilities."[5] In the 2000s a third offset strategy was needed to address the narrowing technological gap between the United States and specific near-peers adversaries. Technologically, the third offset strategy "focused on autonomous learning systems, human-machine collaborative decision-making, assisted human operations, advanced manned-unmanned system operations, and network-enabled autonomous weapons and high-speed projectiles."[6] It also emphasized operational and organizational innovation, as well as

[4] P. Breedlove, M. E. Kosal, "Emerging Technologies and National Security: Russia, NATO, & the European Theater", *Governance in an Emerging New World*, G. P. Shultz, J. Cunningham, D. Fedor, J. Timbie (eds.), Hoover Institution, 2019, p. 10-11, https://www.hoover.org/sites/default/files/issues/resources/emerging_technology_and_americas_national_security_web.pdf [11.10.2020].

[5] Ibidem, p. 11 [11.10.2020].

[6] Ibidem, p. 11 [11.10.2020].

innovative military and civilian talent management. Table 1 offers a comparison of the three U.S. offset strategies with the Soviet/Russian military technological revolutions.

Table 1: Russian/Soviet Military Technological Revolutions and U.S. Offset Strategies

Years	Critical elements
1950s-1960s	Nuclear weapons Satellites Ballistic missiles Ground-based early warning Anti-submarine warfare
1970s-1980s	Airborne early warning Intelligence, surveillance, target acquisition, reconnaissance (ISTAR) Precision-guided munition Netted command and control
2000s-2010s	Big data Robotics Artificial intelligence Biotechnologies Network-enabled autonomous weapons High-speed projectiles Network-centric warfare

Source: table prepared based on a lecture by Diego A. Ruiz Palmer at the seminar on EDTs organized by the Permanent Delegation of the Republic of Poland to NATO on January 15, 2020.

Discussions about a possible fourth offset strategy have already started, especially as the third offset strategy has been influenced in recent years by the insufficient resilience of systems and organizations, but also by changes to industry culture, investment sources, and protection across the innovation base, including the security of supply chains.

Looking into the future, Andrea Gilli has identified three main technological trends underway which will have an impact on geo-economic transition, military transformation, and crisis escalation. “First, accelerating growth in the power of processors will add more computing power, over the next few years, than in all of

human history combined. Second, software is not only eating the world, it is also progressively re-designing it thanks to recent developments in computer science and, in particular, in the field of deep neural networks. Finally, due to the growing availability of portable devices, electronic content has been doubling every 24 months in the recent past, to the extent that 90 percent of existing digital data was created in the past two years."[7]

Moreover, according to Jim Thomas, four broad inter-related trends will impact our understanding of EDTs in the coming years:

- The continued adoption of precision-strike warfare;
- The intensification of the battle network competitions;
- The expansion of military activities in frontier domains (e.g. space or cyberspace);
- The supplanting of human forces by highly autonomous machines.[8]

To properly understand the impact of EDTs, one also needs a solid theoretical framework. The NATO Science and Technology Organization defines technologies as emerging, disruptive, or convergent. Emerging technologies are expected to reach maturity in the period 2020-2040. They are currently not in wide use, and their effects on defence and security are not entirely clear.[9] Disruptive technologies

[7] A. Gilli, "Preparing for "NATO-mation": the Atlantic Alliance Toward the Age of Artificial Intelligence", *NATO Defense College Policy Brief,* No. 4, February 2019, p. 2, http://www.ndc.nato.int/news/news.php?icode=1270 [11.10.2020].

[8] Based on a lecture by Jim Thomas at the seminar on EDTs organized by the Permanent Delegation of the Republic of Poland to NATO on January 15, 2020.

[9] "Science & Technology Trends 2020-2040. Exploring the S&T Edge", NATO Science & Technology Organization, March 2020, p. 6, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf [11.10.2020].

are expected to have a major effect on defence and security in the period 2020-2040.[10] Finally, convergent technologies are based on novel combinations to create a disruptive effect.[11] For Philip Breedlove and Margaret E. Kosal, "to be disruptive, technologies do need not be radical or novel from an engineering or technical perspective. In fact, another class of disruptive technology is important to acknowledge – innovative use of existing technology. Using a combination of existing technologies in ways that are novel can result in a capability that is disruptive."[12]

Not all emerging technologies will be disruptive and not all disruptive technologies are emergent. In fact, technological development is distinctly cyclical. As the NATO Science and Technology Organization suggests, "the most well-known of these cycles is the Gartner Hype Cycle."[13] Yet, technologies do not always follow the sequence of such a cycle. In fact, most technologies fail. Numerous technologies disappear from public or even expert consciousness after initial hype when they prove unproductive. At the same time, when the limitations of technology become clear and one has a better understanding of what is practical and where such a technology can be best applied, the next generation of products starts to occur.

10 "Science & Technology Trends 2020-2040…" p. 6 [11.10.2020].

11 Ibidem, p. 6 [11.10.2020].

12 P. Breedlove, M. E. Kosal, "Emerging Technologies and National Security: Russia, NATO, & the European Theater", *Governance in an Emerging New World*, G. P. Shultz, J. Cunningham, D. Fedor, J. Timbie (eds.), Hoover Institution, 2019, p. 11, https://www.hoover.org/sites/default/files/issues/resources/emerging_technology_and_americas_national_security_web.pdf [11.10.2020].

13 "Science & Technology Trends 2020-2040. Exploring the S&T Edge", NATO Science & Technology Organization, March 2020, p. 11, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf [11.10.2020].

The Alliance currently concentrates on eight EDTs that are considered to be major disruptors until 2040:

- Data
- Artificial intelligence
- Autonomy
- Space
- Hypersonics
- Quantum technologies
- Biotechnology and human enhancement
- Novel material and manufacturing

They are all in some shape or form intelligent, interconnected, distributed, and digital (I2D2) in nature. What is important for NATO is that each of the above identified technology characteristics combine to drive a specific military trend:

- Intelligent + distributed = autonomous system and agents
- Interconnected + digital = battle networks
- Interconnected + distributed = expending domains
- Intelligent + digital = precision warfare[14]

Preparing for the future security of NATO requires anticipating the types of threats that may emerge as technology advances, the potential consequences of those threats, the probability that new and more disperse types of enemies will obtain or pursue them, and the impact they will have on the future of armed conflict.

[14] See more: "Science & Technology Trends 2020-2040. Exploring the S&T Edge", NATO Science & Technology Organization, March 2020, p. 9, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf [11.10.2020].

Russian EDTs Development

Russia has been closely monitoring the United States as well as China's technological priority areas while evaluating their long-term consequences and searching for means to counter them. According to Michael Raska, the current Russian EDTs strategy has been based on two elements. First, the strategy must counter the third offset strategy with the first offset strategy, which means prioritizing the development of a wide array of both strategic and tactical nuclear weapons systems: "In Russian strategic thought, maintaining a variety of sophisticated nuclear weapons can invalidate any conventional advantages of the United States, NATO, and China. Ensuring that Russia remains a nuclear superpower is the basis of all Russian security policies. Moscow has never ceased the development of strategic and tactical weapon systems even during the darkest days of 1990s, and indeed accelerated research and development during the period of swift economic growth in the 2000s."[15] Indeed, for Russia nuclear weapons are the most cost-effective pillar of strategic deterrence.

Second, Russia began to counter numerous U.S. and Chinese technological initiatives using similar indigenous programs, although more narrowly focused and smaller in scale. In October 2012, Russia established the Advanced Research Foundation (ARF).[16] As emphasized by Michael Raska, "the ARF focuses on R&D of high-risk, high-pay-off technologies in areas that include hypersonic vehicles,

[15] M. Raska, "Strategic Competition for Emerging Military Technologies: Comparative Paths and Patterns", *PRISM* 8, No. 3, January 2020, p. 73, https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3_Raska_64-81.pdf [06.12.2020].

[16] The Advanced Research Foundation is a counterpart to the U.S. DARPA (Defense Advanced Research Projects Agency).

artificial intelligence, additive technologies, unmanned underwater vehicles, cognitive technologies, directed energy weapons, and others. While Russian technologies are at the early stages in some areas, in key areas such as directed energy weapons, rail gun, hypersonic vehicles, and unmanned underwater vehicles, programs are progressing into advanced stages, backed by considerable financing for many years prior to the ARF."[17] However, the challenge for Russia remains sustained resource allocation to transform these disruptive technologies into actual military capabilities. Due to its current relationship with the West, one should expect that Russia will try to establish new industrial partnerships with major non-Western countries, primarily India and China. The goal of the potential cooperation will be to secure financing and technological cooperation on these projects. In fact, "Russia has already had a positive experience with India (BrahMos cruise missile joint production venture), and has embarked on two major joint programs with the Chinese – a wide-body passenger aircraft and advanced heavy helicopter programs. The interest in establishing the new joint programs with the Chinese is especially strong in the Russian space industry. The purchase of Chinese space-grade microchip production technology in exchange for RD-180 liquid-fuel rocket engine technology is under negotiation and may start a new stage in Sino-Russian cooperation."[18]

[17] M. Raska, "Strategic Competition for Emerging Military Technologies: Comparative Paths and Patterns", *PRISM* 8, No. 3, January 2020, p. 74, https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3_Raska_64-81.pdf [06.12.2020].

[18] Ibidem, p. 74 [06.12.2020].

The results of the Russian Science and Technology Foresight – a full-fledged study targeted at the identification of the most promising areas of science and technology development in Russia as it nears 2030 – revealed that in numerous areas Russia is lagging behind the world leaders. Foresight 2030 covered seven priority areas:

- Information and communication technologies
- Biotechnology
- Medicine and health
- New material and nanotechnologies
- Rational use of nature
- Transportation and space systems
- Energy efficiency and energy saving[19]

In information and communication technologies, Russia occupies advanced positions in areas like "New data transfer, networking, and content distribution technologies." However, it lags behind global leaders in most fields, in particular "Computer-aided element base design technologies" or "New data transfer technologies."[20] With regard to biotechnology, the most advanced areas of applied research in Russia identified in the study include "High-performance techniques for genome, transcriptome, proteome, and metabolome analysis," as well as "Systematic and structural biology."[21] When it comes to medicine and health, Russia has as yet made only modest progress in human organs regeneration. Nevertheless, according

[19] See more: L. Gokhberg, A. Sokolov, A. Chulok, "Russian S&T Foresight 2030: Identifying New Drivers of Growth", *Foresight*, Vol. 19, No. 5, 2017, pp. 441-456, https://doi.org/10.1108/FS-07-2017-0029 [11.10.2020].

[20] Ibidem, p. 447 [11.10.2020].

[21] Ibidem, p. 448 [11.10.2020].

to Gokhberg, et al., Russia's best chances to achieve sound practical results are in such fields as "Biocompatible biopolymeric materials" and "Techniques for fast identification of toxic substances and pathogens."[22] Unlike most of the other priority areas, the level of research and development in new material and nanotechnology in Russia is assessed as high, particularly in such fields as "Nano-size catalysts for deep processing of raw materials" and "Nano-structured membrane materials."[23] Finally, in transportation and space systems, the research and development fields with the highest domestic competitive advantage include "Development of research models to study transport situation in the Arctic and subarctic areas" and "Development of air- and spacecraft to launch suborbital small-size space satellites."[24]

At the same time, Russia is speeding up its work on artificial intelligence. President Vladimir Putin has said on numerous occasions that the leader in the field of AI would become "the master of the world." In October 2019, Russia adopted a National Strategy for the Development of Artificial Intelligence Through 2030. According to Elena Chernenko and Nikolai Markotkin, Sberbank president German Gref was the driving force behind the strategy, and the state-owned bank prepared a roadmap for developing AI in Russia.[25] In November 2019, the internet giants Yandex and Mail.ru Group, along with Gazprom Neft energy company, MTS, and the Russian Direct In-

[22] L. Gokhberg, A. Sokolov, A. Chulok, "Russian S&T Foresight 2030…", p. 448 [11.10.2020].
[23] Ibidem, p. 449 [11.10.2020].
[24] Ibidem, p. 451 [11.10.2020].
[25] E. Chernenko, N. Markotkin, "Developing Artificial Intelligence in Russia: Objectives and Reality", Carnegie Moscow Center, 5 August 2020, https://carnegie.ru/commentary/82422 [06.12.2020].

vestment Fund, formed a structure known as the AI Russia Alliance which is tasked with promoting Russia's AI-based technologies. The alliance is expected to coordinate the efforts of the business and scientific communities to achieve the objectives set forth in the national AI strategy. Therefore, as Elena Chernenko and Nikolai Markotkin emphasize, in the near future the driving force behind Russian AI technologies will be commercial investment, with large IT companies – rather than start-ups – being in the driver's seat.

Still, the military sector is one of the strongest in terms of developing Russian AI. Increasingly, Russian military specialists in the field of AI applications are making advances in the use of such technologies, primarily in the maritime context. As Roger McDermott underscores, "Moscow's interests in the use of AI to further develop maritime military capabilities relates to the future development of surface and sub-surface platforms that will be fully roboticized. Alongside this longer-term ambition is the use of situational analysis technology to ensure that naval commanders gain an advantage in time and space over a potential adversary by using the AI system to foresee the development of any situation within an operational environment, thus helping to gain the initiative. However, this is taking place within a much wider context of Moscow's increasingly proactive interest in using AI technologies, which is changing the face of its conventional military capability and will do so for years to come."[26] The extent to which Moscow has prioritized, developed, and continued to plan future advances in applying AI within the mil-

[26] R. McDermott, "Moscow's Pursuit of Artificial Intelligence for Military Purposes", *Eurasia Daily Monitor*, Vol. 17, No. 95, July 2020, https://jamestown.org/program/moscows-pursuit-of-artificial-intelligence-for-military-purposes/ [06.12.2020].

itary has to a large degree been underestimated by the West. With the introduction of AI in the fields of maritime security, engine production, or in enhancing command and control, there is no doubt that AI is finding expanding roles in the Russian Armed Forces.

In this context, one should stress that Russia is a technologically advanced country in the design and development of armaments, even if its manufacturing and budgetary capacity has seldom matched its strategic ambition. Indeed, it is important not to underestimate the strength and resilience of Russia's scientific community and innovation potential. Russian advantage is its ability to match technology with the applicable operational concepts and force and command structures. In fact, Russia has been able to use both symmetrical and asymmetrical means and methods of warfare. As Katarzyna Zysk emphasizes, "the objective has been to undermine or circumvent the opponent's military-technological superiority and exploit its vulnerabilities, preferably in a cost-effective manner politically and economically."[27]

Therefore, disruptive technologies should not be seen in isolation from disruptive strategies. In fact, technologies enable strategies. With Russia, one needs to consider not only advances in high technology for traditional military applications, but also innovations and uses below the level of declared war. Russia's premier disruptive strategy is intimidation – to instil the awe and terror of war in adversaries in order to weaken and fracture them, all while using technology as an enabler. In peacetime, they intimidate opponents

[27] K. Zysk, "Defence Innovation and the 4th Industrial Revolution in Russia", *Journal of Strategic Studies*, December 2020, https://www.tandfonline.com/doi/full/10.1080/01402390.2020.1856090 [20.12.2020].

through various psychological methods, from disinformation to targeted nuclear exercises. In wartime, they use surprise and deception and are prepared to undertake asymmetric operations to destabilize, overwhelm, and fracture the adversary. Indeed, Philip Breedlove and Margaret E. Kosal insist that "understanding Russian approaches to technology development would not be complete without acknowledging the role that dezinformatsiya, disinformation, and maskirovka, military deception, play in interactions with external actors."[28]

NATO's Approach to EDTs

NATO's approach to EDTs should be based on three key objectives:

- Retain the technological edge
- Maintain the core values of the Alliance
- Ensure that no potential adversary gains a strategic, asymmetric advantage over NATO that could undermine the deterrence and defence posture

The potential EDTs implications for NATO's deterrence and defence remain of primary importance. Indeed, EDTs will provide a greater range of tools for adversaries to challenge and find weaknesses in NATO's posture. At the same time, ease of commercial access to EDTs raises the prospect of new – increasingly confident – state and non-state actors to contest NATO, particularly with increased challenges of attribution. Table 2 presents an overview of

[28] P. Breedlove, M. E. Kosal, "Emerging Technologies and National Security: Russia, NATO, & the European Theater", *Governance in an Emerging New World*, G. P. Shultz, J. Cunningham, D. Fedor, J. Timbie (eds.), Hoover Institution, 2019, p. 12, https://www.hoover.org/sites/default/files/issues/resources/emerging_technology_and_americas_national_security_web.pdf [11.10.2020].

the EDTs impact on NATO's posture, including both challenges and opportunities.

Table 2: EDTs Impact on NATO's Deterrence and Defence Posture

Deterrence and defence pillar	**Challenges**	**Opportunities**
Readiness	Reduced warning time Attribution	Early warning Decision support
Capability development	Assessment of asymmetry Ethical constrains Private sector dominance	Shorter timescales to implement capabilities Potential cost savings
Posture management	Assessment of response thresholds Strategic miscalculations risks	Enhanced deterrence messaging
Resilience	Over-reliance on technologies Supply chains	Improved interconnectivity across network infrastructure

Source: table prepared based on author's interviews with NATO and Allied officials.

Moreover, based on the four broad inter-related trends presented earlier in this study, one can identify the most critical implications for NATO's deterrence and defence. First, the maturation of the precision-strike regime appears to favour the denial of most domains relative to the ability to gain control over them. The dominant force elements of the Allied armed forces can be held at risk with precision-guided missiles for a fraction of those platforms' costs. Yet, Allies could exploit cross-domain precision weapons to deny an opponent the ability to project power intra-regionally. By developing the "anti-access/area denial" (A2/AD) capabilities, frontline states –

including on NATO's eastern flank – could considerably strengthen NATO's conventional deterrence. In this context, one should note that trends in precision-strike warfare call into question NATO's preference for expeditionary defence whereby forces are dispatched reactively to reinforce frontline states.

Second, disrupting an adversary's battle network should be treated as a major warfighting mission. In doing so, the Allied armed forces will need to reduce their vulnerabilities to network attacks while improving their abilities to operate in environments where radio-frequency interference will be a likely condition. Moreover, the security of Allied military supply chains – especially with regards to semiconductor production and 5G networks – will demand greater attention as a consequence of the competition between battle networks. Finally, the struggle between opposing battle networks will hinge on the contests for control of space and cyberspace – both crucial for military surveillance, warning, battle management, and communications.

Third, the contestation of space and cyberspace will require new missions for protecting assets and holding hostile systems at risk within those domains. Allies will also observe a growing use of space to deny operations in other domains. This will entail closer space cooperation between Allies in order to enhance strategic solidarity and complicate efforts by an aggressor to target the space capabilities.

Fourth, the supplanting of human forces by highly autonomous machines could offer NATO a path to significantly reduce the cost of training forces to the point where they are able to achieve "first battle competence." Autonomous systems may also offer Allies affordable means of regaining forward combat power in conflicts on the periphery of great power rivals through more distributed,

swarming, and expandable forces. Table 3 offers an overview of the military implications on NATO of selected EDTs.

Table 3: Military Implications of Selected EDTs

EDT	Military Implications
Data	Excelling at data would support a more refined understanding of tactical, operational, and strategic environments/courses of actions. Most affected areas: ISR, situational awareness, training and readiness, logistics, support to operations.
Artificial intelligence	AI's impact will occur predominantly through the use of embedded AI in other associated technologies. Over-reliance on AI systems will introduce new vulnerabilities and lead to a potential adversarial AI arms race. Most affected areas: C4ISR, capability planning, CBRN, medical, training, cyber and info-space.
Autonomy	Autonomous systems are expected to lead changes in, among others, force structure, effectiveness, countermeasures, swarming, logistics, situational awareness, lethality, cyber.
Quantum technologies	Quantum technologies are expected to offer improvements in, among others, computing, sensing, communication, cryptography.
Space	The following developments will, among others, impact space capabilities: smallsats, microwave photonics, quantum.
Hypersonics	The following elements will be impacted by hypersonics: strike, defensive countermeasures, aircraft, ISR.
Biotechnology and human enhancement	Biotechnology and human enhancement are expected to create disruption in, among others, readiness, operations, medical countermeasures, social networks.

Source: table prepared based on "Science & Technology Trends 2020-2040. Exploring the S&T Edge", NATO Science & Technology Organization, March 2020, pp. 41-111, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf [11.10.2020].

Conclusions and Recommendations

While the suggestion that EDTs will enable a new class of weapons that will modify the strategic landscape remains to be realised, a number of unresolved security puzzles underlying the emergence of these new technology areas have implications for NATO. As one

looks to the future, new adversaries and new science and technology will emerge. The extent to which these EDTs may exacerbate or mitigate the global security and governance challenges that Russia currently poses to NATO Allies will remain an integral question as policy-makers navigate the complex global environment.

NATO is a natural forum for deliberations about EDTs, especially in a transatlantic context. It also has vast experience, going back to the Cold War, in working towards standardisation and interoperability among Allies. However, the results achieved have been mixed, which underscores the challenges the Alliance now faces – there are not only 30 Allies with disparate levels of capability, but also a backdrop of rapid technological advances where some of its competitors and adversaries may hold significant advantages.

In this context, NATO should concentrate on four core issues with regard to EDTs. First, as Andrea Gilli emphasizes, the Alliance should start a process on "NATO-mation."[29] In fact, the Alliance should serve as a primary transatlantic coordinating institution for information-sharing and cooperation between Allies on the security dimension of EDTs. NATO has an important role to play in the development of a common strategy based on an Alliance-wide EDTs threat assessment and an analysis of opportunities. Therefore, EDTs can serve as a unifying element for NATO's work on future policies.

[29] See more: A. Gilli, "Preparing for "NATO-mation": the Atlantic Alliance Toward the Age of Artificial Intelligence", *NATO Defense College Policy Brief,* No. 4, February 2019, http://www.ndc.nato.int/news/news.php?icode=1270 [11.10.2020] and A. Gilli, ""NATO-Mation": Strategies for Leading in the Age of Artificial Intelligence", *NATO Defense College Research Paper,* No. 15, December 2020, https://www.ndc.nato.int/news/news.php?icode=1514 [21.12.2020].

Second, NATO will need partners on its path towards achieving a comprehensive implementation strategy on EDTs. This will require connection with the private sector early and often, clearly communicating NATO's priorities and requirements while providing accessible opportunities for industry, including non-traditional ones. Much of the innovative work being undertaken in the commercial sector is being carried out by companies that have never worked in the defence realm or have no wish to do so. Therefore, building new partnerships at NATO with the private sector will enable the Alliance to increase awareness, share data, and creatively tap into experiences and knowledge. Moreover, NATO and the EU should initiate a strategic dialogue to address fundamental issues of tech governance and data sharing in order to overcome the transatlantic tech policy divide.

Third, Allies should manage expectations and not overestimate the role of EDTs. EDTs are not a panacea to all of NATO's problems, including the existing gaps in the still-needed conventional capabilities. Indeed, EDTs will not be a silver bullet to address NATO's shortfalls. Therefore, Allies should first and foremost concentrate on two elements: overcoming the interoperability gap[30] and revitalizing NATO's once robust standardization programme.[31]

Fourth, Allies should consider using NATO as a body to coordinate efforts to find innovative ways to finance EDTs, including through an

[30] See more: M. Dufour, "Will Artificial Intelligence Challenge NATO Interoperability?", *NATO Defense College Policy Brief,* No. 6, December 2018, http://www.ndc.nato.int/news/news.php?icode=1239 [11.10. 2020].

[31] See more: P. Beckley, "Revitalizing NATO's Once Robust Standardization Programme", *NATO Defense College Policy Brief,* No. 14, July 2020, http://www.ndc.nato.int/news/news.php?icode=1456 [11.10. 2020].

establishment of a NATO venture capital fund. A potential deep-tech investment in technologies with security and defence applications through a dedicated NATO structure could help Allies maintain their technological edge.

References

Albrycht, I., Rekowski, M., Mikulski, K. (eds.), "Geopolitics of Emerging and Disruptive Technologies", The Kosciuszko Institute, October 2020, https://ik.org.pl/wp-content/uploads/geopolitics-of-emerging-and-disruptive-technologies-2020.pdf.

Barberini, P., "Military Technology: Risks and Opportunities for the Atlantic Alliance", *Documenti IAI,* No. 20/10, May 2020, https://www.iai.it/en/pubblicazioni/military-technology-risks-and-opportunities-atlantic-alliance.

Beckley, P., "Revitalizing NATO's Once Robust Standardization Programme", *NATO Defense College Policy Brief,* No. 14, July 2020, http://www.ndc.nato.int/news/news.php?icode=1456.

Breedlove, P., Kosal, M. E., "Emerging Technologies and National Security: Russia, NATO, & the European Theater", *Governance in an Emerging New World*, Shultz, G. P., Cunningham, J., Fedor, D., Timbie, J. (eds.), Hoover Institution, 2019, pp. 8-39, https://www.hoover.org/sites/default/files/issues/resources/emerging_technology_and_americas_national_security_web.pdf.

Buchanan, B., "The AI Triad and What It Means for National Security Strategy", Center for Security and Emerging Technology, Georgetown University's Walsh School of Foreign Service, August 2020, https://cset.georgetown.edu/wp-content/uploads/CSET-AI-Triad-Report.pdf.

Chernenko, E., Markotkin, N., "Developing Artificial Intelligence in Russia: Objectives and Reality", Carnegie Moscow Center, 5 August 2020, https://carnegie.ru/commentary/82422.

Dufour, M., "Will Artificial Intelligence Challenge NATO Interoperability?", *NATO Defense College Policy Brief,* No. 6, December 2018, http://www.ndc.nato.int/news/news.php?icode=1239.

Gilli, A., ""NATO-Mation": Strategies for Leading in the Age of Artificial Intelligence", *NATO Defense College Research Paper,* No. 15, December 2020, https://www.ndc.nato.int/news/news.php?icode=1514.

Gilli, A., "NATO and 5G: What Strategic Lessons?", *NATO Defense College Policy Brief,* No. 13, July 2020, http://www.ndc.nato.int/news/news.php?icode=1453.

Gilli, A., "Preparing for "NATO-mation": the Atlantic Alliance Toward the Age of Artificial Intelligence", *NATO Defense College Policy Brief,* No. 4, February 2019, http://www.ndc.nato.int/news/news.php?icode=1270.

Gilli, A., Gilli, M., "Imitation, Innovation, Disruption: Challenges to NATO's Superiority in Military Technology", *NATO Defense College Policy Brief,* No. 25, December 2019,http://www.ndc.nato.int/news/news.php?icode=1404.

Gokhberg, L., Sokolov, A., Chulok, A., "Russian S&T Foresight 2030: Identifying New Drivers of Growth", *Foresight*, Vol. 19, No. 5, 2017, pp. 441-456, https://doi.org/10.1108/FS-07-2017-0029.

Iftimie, I. A., "NATO's Needed Offensive Cyber Capabilities", *NATO Defense College Policy Brief* No. 10, May 2020, http://www.ndc.nato.int/news/news.php?icode=1453.

Kluge, J., "Russia's Transition to 5G: Stuck in a Regulatory Tug of War", Foreign Policy Research Institute, August 2020, https://

www.fpri.org/article/2020/08/russias-transition-to-5g-stuck-in-a-regulatory-tug-of-war/.

Konaev, M., Dunham, J., "Russian AI Research 2010-2018", *CSET Issue Brief*, Center for Security and Emerging Technology, Georgetown University's Walsh School of Foreign Service, October 2020, https://cset.georgetown.edu/research/russian-ai-research-2010-2018/.

McDermott, R., "Moscow's Pursuit of Artificial Intelligence for Military Purposes", *Eurasia Daily Monitor*, Vol. 17, No. 95, July 2020, https://jamestown.org/program/moscows-pursuit-of-artificial-intelligence-for-military-purposes/.

Missiroli, A., "From Hybrid Warfare to "Cybrid" Campaigns: the New Normal?", *NATO Defense College Policy Brief* No. 19, September 2019, http://www.ndc.nato.int/news/news.php?icode=1350.

Raska, M., "Strategic Competition for Emerging Military Technologies: Comparative Paths and Patterns", *PRISM* 8, No. 3, January 2020, pp. 64-81, https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3_Raska_64-81.pdf.

"Science & Technology Trends 2020-2040. Exploring the S&T Edge", NATO Science & Technology Organization, March 2020, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf.

Valášek, T., "NATO at 70: Enter the Technological Age", *NATO Defense College Policy Brief*, No. 10, April 2019, http://www.ndc.nato.int/news/news.php?icode=1305.

Zysk, K., "Defence Innovation and the 4th Industrial Revolution in Russia", *Journal of Strategic Studies*, December 2020, https://www.tandfonline.com/doi/full/10.1080/01402390.2020.1856090.

Authors

Dominik P. Jankowski, Political Adviser and Head of the Political Section at the Permanent Delegation of the Republic of Poland to NATO.

Dave Johnson, a staff officer in the North Atlantic Treaty Organization International Staff Defence Policy and Planning Division. He previously served as an officer in the US Air Force, including in posts at SHAPE Headquarters, US Strategic Command, the US Defence Attaché Office Moscow, and the Pentagon.

Michael Rühle, Head of the Hybrid Challenges and Energy Security Section in the NATO International Staff Emerging Security Challenges Division.

Tomasz Stępniewski, Doctor Habilitatus (Polish Academy of Sciences, Warsaw, Poland), Research Director at the Institute of Central Europe and Associated Professor and Head of the Department of Political Theory and Eastern Studies at the Institute of Political Science and Public Administration, Faculty of Social Sciences, The John Paul II Catholic University of Lublin, Poland.

NATO is in peacetime competition with Russia, which is capable and willing to seize any opportunity to intimidate Allies and to challenge our values and security architecture. This publication underlines the need to update the NATO Strategic Concept to properly reflect the new, changed strategic environment, while providing sound recommendations for the mid- to long-term. The authors skillfully argue that the Alliance must develop its own toolbox to effectively counter Russian employment of its instruments of power to continuously assure NATO's superiority and ability to pose strategic dilemmas and risks unacceptable to Russia's calculus, through the exploration of any identified weaknesses in their "destabilization campaign." The interrelated, non-exhaustive list of this campaign elements includes nuclear, conventional, special forces, cyber, space, non-kinetic, hybrid, disinformation, emerging and disruptive technologies, which Russia is ready to use in different combinations, scale, domains, directions in a non-traditional and non-Western way. We should be prepared and properly equipped to demask and counter Russian real intentions and act proactively, instead of reactive only mode.

Major General Piotr "Zeus" Błazeusz , Ph.D.,
Deputy Chief of Staff for Strategic Development and Preparation, SHAPE

Russia will pose a threat to European security in the long run and in a whole spectrum of domains. This book is a welcome analysis of the long-term dangers presented by Russia, even in a post-Putin era. And it provides a much needed study of the disruption that new technologies will play in NATO's deterrence posture. Highly recommended!

Professor Jakub J. Grygiel, Catholic University of America;
Senior Advisor at The Marathon Initiative

"NATO in the Era of Unpeace: Defending Against Known Unknowns" helps us to understand contemporary security environment. It broadens our knowledge on the adaptation to emerging challenges, from traditional military affairs to various non-kinetic threats. We live in a time which can be called the era of "unpeace"– neither peace nor war – and the book argues how blurry the line is between war and peace. Even if the conflict in and around Ukraine might be a sui generis case, and will not be repeated soon, NATO still needs to understand all the efforts by our adversaries which aim to disrupt Western unity. Hybrid warfare, biotechnologies, AI and big data are with us already, and our foes are more than ready to exploit them for their own sake. If you would like to understand these tendencies and their implications for NATO, this book is a must-have on your bookshelf.

Péter Stepper, Ph.D., Adjunct Professor, Faculty of Military Science and Officer Training, National University of Public Service, Hungary

ISBN 978-83-66413-40-5
9 788366 413405

Instytut Europy Środkowej
Institute of Central Europe

www.ies.lublin.pl