



One Plus Four: Charting NATO's Future in an Age of Disruption

NATO Task Force Report

Daniel S. Hamilton and Hans Binnendijk, Editors



transatlantic.org



Center for a
New American
Security

DGAP
Advancing foreign policy. Since 1951.



The Hague Centre
for Strategic Studies



Middle
East
Institute



PISM

POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS



SWP

Stiftung Wissenschaft und Politik
German Institute for International
and Security Affairs

Table of Contents

<i>About the NATO Task Force</i>	<i>iii</i>
<i>Individual Endorsements</i>	<i>iii</i>
<i>Executive Summary</i>	<i>v</i>
I. The Age of Disruption	1
II. The One: Alliance Cohesion	3
III. The Four: NATO’s Core Tasks	5
Collective Defense	5
<i>Box 1. Enhance Cybersecurity Through “Safe-to-Fail” Principles</i>	
Crisis Management	9
<i>Box 2. Address Southern Challenges Through Comprehensive Support</i>	
Cooperative Security	11
<i>Box 3. Help Ukraine and Georgia Deter Russian Aggression</i>	
Comprehensive Resilience	14
IV. Rebalancing the Transatlantic Partnership	16
V. Connecting the North Atlantic and the Indo-Pacific	18
VI. Developing an Overarching Military Concept	21
VII. Conclusion	23
<i>Notes</i>	<i>24</i>

About the NATO Task Force

This report is the result of discussions among and written contributions by independent non-government participants from across the Atlantic Alliance who participate in the NATO Task Force, hosted by the Transatlantic Leadership Network. While we also discuss issues with current government officials from many countries, this is an independent report. The Task Force initiative receives no financial or other support from any outside party.

The Transatlantic Leadership Network provides a broad umbrella enabling participants from a number of policy research institutes to cooperate and exchange views. We are pleased to acknowledge these partner institutions and thank them for their permission to feature their logos.

The Task Force participants listed on the next page, in their personal capacity, endorse the thrust of this report, though they may not support each individual recommendation. Affiliations are listed for identification purposes only; views do not necessarily reflect those of any institution or organization. We thank them and all contributors for their insights.

Daniel S. Hamilton and Hans Binnendijk, Editors

Individual Endorsements

Lisa Aronsson

Research Fellow
National Defense University

Charles Barry

Visiting Senior Research Fellow
National Defense University

Max Bergmann

Senior Fellow and Director for Europe and
Russia, Center for American Progress

Una Aleksandra Bērziņa-Čerenkova

Head, Riga Stradins University China
Studies Centre and Head, New Silk Road
Program, Latvian Institute of International
Affairs

Hans Binnendijk

Distinguished Fellow, Atlantic Council
Former Senior Director for Defense Policy,
U.S. National Security Council

Jason Blessing

Jeanne Kirkpatrick Visiting Research Fellow
American Enterprise Institute

Heinrich Brauss

Senior Associate Fellow, German Council
on Foreign Relations DGAP
Former NATO Assistant Secretary General
for Defense Policy and Planning

Sławomir Dębski

Director, Polish Institute of International
Affairs PISM

Katherine Kjellström Elgin

Fellow, Center for Strategic and Budgetary
Assessments

Nele Marianne Ewers-Peters

Lecturer and Postdoctoral Researcher
Leuphana University Lüneburg

Daniel S. Hamilton

President, Transatlantic Leadership Network
Senior nonresident Fellow, Brookings,
Senior Fellow, Foreign Policy Institute,
Johns Hopkins University SAIS; Former
U.S. Deputy Assistant Secretary of State

Ben Hodges, Lt. Gen. (ret.)

Pershing Chair in Strategic Studies
Center for European Policy Analysis CEPA
Former Commander U.S. Army Europe

Iulia-Sabina Joja

Director and Senior Fellow, Middle East
Institute

Andrea Kendall-Taylor

Senior Fellow and Director, Transatlantic
Security Program, Center for a New
American Security CNAS

Barbara Kunz

Senior Researcher, Institute for Peace
Research and Security Policy, University of
Hamburg

Claudia Major

Head of Research Division International
Security, Stiftung Wissenschaft und Politik
SWP

Rachel Rizzo

Nonresident Senior Fellow, Atlantic Council

Michael C. Ryan

Former U.S. Deputy Assistant Secretary of
Defense for European and NATO Policy

Luis Simon

Senior Analyst and Director, Brussels Office
Elcano Royal Institute

Christopher Skaluba

Director, Scowcroft Center for Strategy and
Security's Transatlantic Security Initiative,
Atlantic Council; Former Principal Director
for European and NATO Policy, Office of
the U.S. Secretary of Defense

Lauren Speranza

Director, Transatlantic Defense and Security
Center for European Policy Analysis CEPA

Tim Sweijs

Director of Research, Hague Centre for
Strategic Studies HCSS

Bruno Tertrais

Deputy Director, Fondation pour la
recherche stratégique FRS

Jim Townsend

Adjunct Senior Fellow, Center for a New
American Security CNAS; Former U.S.
Deputy Assistant Secretary of Defense for
European and NATO Policy

Alexander R. Vershbow

U.S. Ambassador (ret.); former Deputy
Secretary General of NATO; Distinguished
Fellow, the Atlantic Council

Michael J. Williams

Associate Professor and Director of
International Relations Graduate Programs,
Syracuse University

Valbona Zeneli

Professor of National Security Studies
Chair, Strategic Initiatives Department
George C. Marshall European Center for
Security Studies

Executive Summary

I. The Age of Disruption

The Atlantic Alliance stands today at an historic inflection point, between a fading era of relative stability and a volatile, dangerous Age of Disruption. *As this Task Force Report is being issued, Russian troops are poised to further invade NATO partner Ukraine. Should the deterrent efforts created by a fairly united NATO fail, this age of disruption will take a dramatic turn for the worse.*

The Age of Disruption is global in nature and broad in scope. The Alliance faces strategic competition with a revisionist Russia and a militarily powerful and technologically advanced China, each of which seeks to disrupt the international order. Terrorists threaten our people. Disruptive challenges extend to emerging technologies that are changing the nature of competition and conflict and digital transformations that are upending the foundations of diplomacy and defense. The scale and complexity of critical economic, environmental, technological and human flows, as well as the dependency of many societies on such flows, have increased dramatically. Destructive capabilities unthinkable a few decades ago are now in the hands of big powers, smaller states, and non-state actors. Climate change and energy transitions pose new security dilemmas and amplify crises. Europe's periphery has turned from a ring of friends to a ring of fire.

The Atlantic Alliance faces the most complex strategic environment in its 73-year history. North America and Europe must use the Alliance's new Strategic Concept to reaffirm their mutual bonds, recast their partnership, and retool their institutions – particularly NATO – for the Age of Disruption.

NATO's new Strategic Concept should be framed by an approach we call "One Plus Four." The One is Alliance cohesion, which must be the central strategic underpinning of a new Concept. NATO must then be repositioned for current and future challenges, many of which are unconventional and unpredictable. This will require the Alliance to update and upgrade its three core tasks -- collective defense, crisis management, and cooperative security – and to add a fourth core task: building comprehensive resilience to disruptive threats to allied societies.

II. The One: Alliance Cohesion

The foundation for NATO's next Strategic Concept must be renewed Alliance cohesion rooted in a common commitment to shared values and effective decision making. Today, those values are under assault from external and internal challengers. This is why a mutual affirmation of NATO's democratic foundation must begin with humility. Democratic deficits exacerbate mutual doubts, which can gnaw at allied commitments to collective defense and mutual security. They can be used by strategic competitors to destabilize individual allies or NATO as a whole. Deficits in internal values can become external threats. Allied cohesion, grounded in resilient democratic institutions with robust and transparent mechanisms of accountability, is the most formidable defense against these threats. This should be coupled with streamlined decision-making mechanisms allowing the Alliance to make cohesive and timely decisions.

III. The Four: NATO's Core Tasks

1. Collective Defense

a) Make It the Principal Core Task. Of NATO's core tasks, collective defense is *primus inter pares* – first among equals. It is the only core task mentioned explicitly in the North Atlantic Treaty. That priority should be made clear in the new Strategic Concept.

The Alliance must be able to dissuade and deter threats to its members, from whatever source and across all domains, while being prepared to defend all parts of NATO territory and to protect the critical functions of allied societies. That means countering challenges from Russia, which is likely to remain NATO's pacing

adversary, as well as addressing pressures emanating from NATO's south and southeast. The Alliance needs to bridge gaps in its ability to better integrate its political, military and technological capacities across all five operational domains: land, sea, air, cyberspace, and outer space. NATO has been good at addressing each domain on its own. Being good at multi-domain operations is exponentially harder.

b) *Improve Conventional Deterrence and Defense.* Since the 2014 Wales Summit, NATO has approved a number of initiatives for conventional rapid response. The new Strategic Concept will need to give additional political impetus to their full implementation while advancing additional initiatives. NATO and U.S. forward presence should be further strengthened. NATO's maritime posture must be upgraded. Critical capability gaps must be filled, including those needed for rapid reinforcement of allies under threat as well as those required to deal with Russia's anti-access/area denial capabilities. NATO's Special Operations Forces should be strengthened, and NATO interoperability improved. The U.S. should take a more visible, active role in the NATO Response Force.

c) *Bolster Deterrence and Defense Against Hybrid Threats,* which requires better EU-NATO coordination and planning. The U.S. might offer to be the framework nation in the next evolution of NATO cyber operations. NATO should create a full Cyber Defense Forces Headquarters. Collective defense efforts should incorporate cyber resilience and "safe-to-fail" principles.

d) *Enhance Nuclear Deterrence.* NATO should be forthright about why nuclear deterrence remains critical to Alliance security. Modern, safe and survivable U.S. weapons and allied-dual capable delivery systems should be maintained. A clear nuclear doctrine is needed to deter Russia's "escalate to deescalate strategy." NATO should press hard for a return to nuclear and other arms control agreements.

e) *Deter and Defend in Outer Space.* NATO must follow through on its Space Policy, agreed in June 2021, by realizing the Strategic Space Situational Awareness system at NATO headquarters, and working out procedures for NATO response to incidents in outer space.

f) *Be Prepared to Engage with Moscow.* Enhanced measures of deterrence and defense should be reinforced by NATO offers to engage with Moscow. Engagement is not a favor to Putin; it is in NATO's own interests. Efforts could include minimizing escalation risks, avoiding inadvertent incidents or miscalculations in all five domains, improving transparency and confidence-building measures, and returning to nuclear and other arms control agreements.

2. Crisis Management

Europeans and North Americans must anticipate and plan for contingencies related to additional armed conflicts, further displacement, persistent terrorist threats, and security challenges arising from political, economic, and environmental instabilities. The chaotic withdrawal from Afghanistan after two decades of military engagement by NATO and its partners will be a cautionary tale that may limit future NATO engagement. The Strategic Concept will need to strike the right balance between necessary engagement in these operations and national reluctance to do so.

To strike the right balance, NATO will need to design a more comprehensive southern approach. Southern security challenges are extraordinarily complex, in both form and force. In some circumstances NATO may lead, but in most situations, it is more likely to play a supporting role. Still, these complex challenges cut across each of NATO's core tasks. Taken together, those elements should support a broad and flexible southern approach of "comprehensive support" that should include: NATO backing for lead nation and coalition operations undertaken by NATO members; collective defense incorporating missile and air defenses, maritime surveillance and counter-terrorism missions; continued implementation of NATO's Framework for the South and investment in expeditionary capabilities; encouragement of European strategic responsibility; and deterrence and defense measures, particularly along the Turkish-Syrian border.

3. Cooperative Security

Cooperative Security focuses primarily on NATO's partnerships. They consist of three categories: 1) partners who seek NATO membership, 2) partners along NATO's periphery that are not likely membership candidates; and 3) like-minded countries around the globe, including in the Indo-Pacific region. Each must be adapted to the age of disruption. Cooperative security must also address the security implications of climate change, emerging and disruptive technologies, and challenges to the global commons.

First category partners need urgent attention because of Russian threats to their security. Ukraine and Georgia in particular need a new focus. A Ukrainian Deterrence Initiative (UDI) and a Georgia Deterrence Initiative (GDI) could be created that would be extensions of the Alliance's Enhanced Opportunity Partners (EOP) program. Allies would make it a strategic objective to do everything possible, short of extending an Article 5 guarantee, to help these countries defend themselves and resist Russian destabilization.

The Alliance should prioritize mechanisms to assist Jordan and inject life in bilateral partnerships with Israel, Morocco and Tunisia. NATO can be a platform for security risk assessment, information-sharing and resilience support. NATO should forge a true strategic partnership with the EU; extend elements of the Deterrence Initiatives to Finland and Sweden if requested; strengthen its Enhanced Operational Partnership with Australia; and pursue similar arrangements with Japan and South Korea.

Cooperative Security programs can be expanded to address the security implications of climate change. The Alliance's 2021 Action Plan on Climate Change and Security must be further elaborated. Training, education, exercises and standards need to be rethought. The purchasing power of the military should be used to fuel investments in cleaner energy, infrastructure and preventive technologies. Consideration should be given to how climate and energy-related elements can be incorporated into NATO Defense Planning Process and Security Investment Program decisions. Reducing energy demand and increasing energy resilience is essential for the armed forces to ensure readiness and sustainability.

Cooperative Security should be used to address challenges to the global commons, including: 1) protecting freedom of the seas, 2) upholding the global information commons; 3) ensuring security and norms of peaceful behavior in space; and 4) protecting Alliance equities in Arctic security. In some areas, NATO will not be the lead institution, but it can offer specialized capabilities.

4. New Core Task: Comprehensive Resilience

The growing need to implement operationally the concept of resilience -- the ability to anticipate, prevent, and, if necessary, protect against and recover quickly from disruptions to critical functions of our societies -- has become a challenge on par with NATO's other core tasks. It is foundational to the other three, yet it is distinctly separate from them and equivalent to them as well. It must deal with a spectrum of challenges that are not addressed adequately by the other core tasks. NATO's efforts thus far betray a static understanding of resilience, which encompasses a wide range of dynamic interconnections. NATO must move beyond country-by-country resilience metrics and adopt a more comprehensive approach that embraces and operationalizes the mutually-reinforcing concepts of *democratic* resilience, *shared* resilience and *forward* resilience.

a) Democratic Resilience. In recent years, much strategic discussion has focused on competition among states of "great power." It is becoming clear, however, that this competition extends beyond traditional measures of power; it centers increasingly on forms of governance. Adversaries big and small are selling autocracy as "efficient." They tout their own systems and use a broad array of tools to amplify fissures and undermine confidence within democracies. When they can't do that successfully, they use diplomatic and other means of coercion. This puts democratic resilience at the heart of the new international system and international competition.

b) Shared Resilience. Resilience begins at home, but in this age of disruption, no nation is home alone. Few critical infrastructures that sustain the societal functions of an individual country are limited today to the national borders of that country. Allies must move from country-by-country baseline requirements to *shared* resilience, by establishing together metrics that can ensure their mutual security. Shared resilience efforts should include critical infrastructures but extend to many other connective elements that bind allies' critical societal functions. Enhanced NATO-EU cooperation should leverage combined resources.

c) Forward Resilience has two components, one spatial and one temporal. The spatial component essentially means projecting shared resilience forward to non-NATO partners. We see the importance of this today in Ukraine, but Ukraine is not a lone example. All across Europe's southern and eastern peripheries disruptive challenges to weak democracies can ripple back into NATO territory. The temporal component means thinking and acting forward in time – anticipating disruptive challenges, and acting to prevent, mitigate or adapt to them. This is another reason to consider a NATO Office of Net Assessment.

We recognize that there is resistance in some countries to adopting a fourth core task to complement the first three. We urge these nations to reconsider, because resilience is needed to implement the first three tasks but it is operationally very different in nature. Adding this fourth core task is critical to the success of the first three, and to allied ability to confront challenges not addressed by the other three. Failure to make resilience a new core task will only downgrade its importance.

IV. Rebalancing the Transatlantic Partnership

NATO must transform itself into a more balanced transatlantic partnership in which European allies assume greater strategic responsibility in two ways. First, they should provide half of the forces and capabilities, including the strategic enablers required for deterrence and collective defense against major-power aggression. Second, they should develop capabilities that lessen their heavy reliance on U.S. enablers so they can be the “first responders” to crises in and around Europe's periphery.

V. Connecting the North Atlantic and the Indo-Pacific

NATO's ability to address traditional and unconventional threats in Europe is becoming intertwined with related challenges to Alliance security interests posed by China. The Alliance should explore deeper coordination under Article 2 of the North Atlantic Treaty; bolster protection of defense-critical infrastructures and defense-related supply chains; create new North Atlantic-Indo-Pacific partnerships; and consider creation of a NATO-China Council to maintain diplomatic dialogue, explore potential areas of cooperation, and design crisis mitigation measures.

VI. Implementing NATO's Overarching Military Concept Informed by Innovative Technologies

NATO must maintain its technological edge. To this end, it has adopted its strategic plan to foster and protect Emerging and Disruptive Technologies (EDT). In addition, NATO's civil-military Defense Innovation Accelerator for the North Atlantic” (DIANA) is designed to help develop innovative technological solutions to address Allies military needs and promote interoperability. The Strategic Concept is an opportunity to connect these efforts with the implementation of the Alliance's Comprehensive Concept for Deterrence and Defense in the Euro-Atlantic Area (DDA) that undergirds NATO's overall strategic posture. It must be implemented in full and without any delay. This requires ongoing assessments of emerging and developing technologies and national progress and NATO standards in adopting prioritized military-technological capabilities; aligning on a set of NATO principles for the use of EDT in warfare; and establishing vibrant connections with industry partners and with EU institutions.

VII. Conclusions

One Plus Four: a NATO that is more cohesive, capable, balanced, and resilient—an Alliance prepared for the Age of Disruption.

I. The Age of Disruption

The Atlantic Alliance stands today at an historic inflection point – its fourth since World War II.

The first came at the end of that terrible conflict, when Europeans and North Americans responded to a new Cold War by creating the North Atlantic Treaty Organization (NATO) and a host of other mechanisms to provide for their common defense, institutionalize the transatlantic link, and provide an umbrella of reassurance under which west Europeans could focus their security concerns on common challenges rather than on each other. A second came in the late 1960s and early 1970s, when, based on the Harmel Report, allies retooled their common defense while working out arrangements with their adversaries to regulate the most dangerous aspects of Cold War competition and to render more permeable the human divisions that separated the European continent. The third moment came when the Cold War ended, peacefully and surprisingly, and as the Soviet empire, and ultimately the Soviet Union itself, dissolved.

For the next quarter century, a new paradigm took hold across much of Europe. The continent's divisions would be overcome by a magnetic, largely unchallenged, and gradually expanding democratic order, in which eastern Europe and eventually Russia could potentially find a place, the United States would continue as an affirmative European power, China was comfortably remote and would emerge as a "responsible stakeholder" in the international system, military tensions and military forces would be reduced, and growing interdependencies and open borders would lower conflict and generate greater security and prosperity.

In the 1990 Charter of Paris for a New Europe, leaders of over thirty countries announced that the "era of confrontation and division of Europe has ended." They vowed to "build, consolidate and strengthen democracy as the only system of government of our nations," and declared human rights and fundamental freedoms to be the "irrevocable...foundation of freedom, justice and peace." These extraordinary commitments gave powerful expression to Soviet President Mikhail Gorbachev's notion of a "common European home" and U.S. President George H.W. Bush's vision of a Europe that at long last could be "whole and free."

Much was achieved during this period. A Euro-Atlantic architecture of cooperative, overlapping and interlocking institutions enabled a host of countries to walk through the doors of NATO, the European Union (EU), the Council of Europe, the OECD and other organizations in ways that were not at the expense of other states or institutions. Europe was not fully whole, but it was no longer divided. It was not fully free, but vast parts of the continent were no longer under the thumb of domestic autocrats or foreign overseers. The Balkan wars were a brutal reminder that Europe was not fully at peace. Nonetheless, when those wars ended and a new millennium began, Europe seemed more secure than at any time in the previous century.

NATO's 2010 Strategic Concept -- the Alliance's guiding document still today -- was based on this paradigm and emblematic of this era. "The Euro-Atlantic area is at peace and the threat of a conventional attack against NATO territory is low," it declares.¹

1. Paradigm Lost

That era of stability is now a paradigm lost. The Atlantic Alliance is at a fourth major inflection point. Stability has given way to a more dangerous and volatile age of disruption, a world of ambiguous, asymmetric, and potentially instantaneous threats. The appealing paradigm created after the fall of the Berlin Wall is being challenged by two revisionist authoritarian major powers determined to disrupt the current international order, by disruptive and often violent non-state actors who seek to inflict damage and

terror, or gain revenge or profit, by disruptive technologies that can undercut societies, and by disruptive natural phenomena such as pandemics and climate change.

The age of disruption is dominated by strategic competition with two authoritarian powers: a revisionist Russia that seeks openly to roll back the changes in Europe since the end of the Cold War and subjugate its neighbors to a Russian sphere of influence; and a militarily powerful and technologically advanced China that poses a systemic challenge to the transatlantic community and other democratic nations. The increasingly close alignment between Russia and China adds to the strategic complexity of the threats NATO must address from each.

Russia's threatening posture is the most vivid and dangerous evidence of this new era. Russian President Vladimir Putin wants to undo the post-Cold War settlement, control his neighborhood, and disrupt the influence of open democratic societies, not because of what they do but because of who they are. It is useful to recall that the pretext for Russia's 2014 invasion of Ukraine was not NATO's open door, it was a trade agreement between Ukraine and the European Union. Putin understands the challenge a successful Ukrainian democracy would pose to authoritarianism in Russia. Through his current threats and his earlier military interventions in Georgia and Ukraine, he demonstrates both intent and ability to use military force and coercion to change Europe's map.²

Russia's coercive and subversive practices across the domains of air, sea, land, outer and cyber space employ a growing range of political, economic and military tools, including informational and psychological manipulation, cyber warfare and energy blackmail, the use of proxies and special forces, rapid mobilization, direct military intervention and the threat of nuclear use.³ They are accompanied by efforts to surprise, deceive, and disrupt, while often disguising intent and attribution. Until now, Russia's approach has sought to achieve strategic aims without war, by staying below NATO's threshold for reaction, dividing Europeans from each other as well as from their North American allies, and slowing, if not outright blocking, NATO decision-making and unity of purpose.⁴ Russia's threats to Ukraine indicate that Moscow may now be prepared to risk wider conflict, including war, to achieve its aims.

These dangers are amplified by Russia's entente with China, which includes arms cooperation and maritime exercises in the Mediterranean and Baltic Seas, as well as by Beijing's challenges to the global commons and Indo-Pacific regional order, its investments in strategic industries and ports, and its efforts to disrupt basic principles and arrangements critical to the security and prosperity of the North Atlantic region.

The age of disruption is not limited to major power competition. Emerging technologies are changing the nature of competition and conflict. Digital transformations are upending the foundations of diplomacy and defense. The scale and complexity of critical economic, environmental, technological and human flows, as well as the dependency of many societies on such flows, have increased dramatically. Destructive capabilities unthinkable a decade ago are now in the hands not only of big powers, but also smaller state and non-state actors, some of which serve as puppets and proxies in increased grey zone competition. Critical societal functions are increasingly susceptible to disturbances, interruptions, and shutdowns. Revisionists have grown their influence. Shooting wars have erupted in Europe, and borders have been changed by force. Foreign troops are in European countries without invitation. The dangers of military accidents and miscalculations have risen as confidence-building measures and arms control arrangements have fallen. Climate change and the transition to clean energies pose new security dilemmas and amplify ongoing crises. Millions have been killed by an unanticipated and unpredictable virus. Democracies are in retreat. Independent media and judicial authorities are being suppressed. Autocratic and democratic leaders alike have politicized refugees to preserve their power and disorient their opponents. Racial, religious and ethnic hatreds are alive and well. Europe's periphery has turned from a ring of friends to a ring of fire.⁵

The Atlantic Alliance faces the most complex strategic environment in its 73-year history. North America and Europe must use the Alliance's new Strategic Concept to reaffirm their mutual bonds, recast their partnership, and retool their institutions – particularly NATO – for the age of disruption.

2. NATO's Role

Seven decades after its founding, NATO's three-fold purpose remains: to provide for the collective defense of its members; to institutionalize the transatlantic link and offer a preeminent forum for allied deliberations on security and strategy; and to offer an umbrella of reassurance under which European nations can focus their security concerns on common challenges rather than on each other. There is a symbiotic relationship among these functions; allies are unlikely to be successful in any one of them without attention to the remaining two.

NATO continues to be vibrant because it has been able to adapt its mission to changing strategic circumstances. In the past, NATO has used Strategic Concepts to underwrite such adaptation.⁶ Its decision to design a new guiding Strategic Concept by June 2022 is an opportunity for allies to generate new unity, and to update NATO's tasks and tools for a complex and challenging era.

Since the end of the Cold War, the Alliance's Strategic Concepts have steadily broadened its conception of security and its geographic scope. During the fight against terror in 2010, NATO adopted crisis management and cooperative security as core tasks, and its geographic focus shifted to the Middle East. Since then, NATO has ventured into new areas like cyber security and outer space. It has taken on new responsibilities related to information warfare, the pandemic, and the security implications of climate change. The NATO 2030 Expert Report lists a full spectrum of non-traditional security challenges facing NATO and argues that they come from "every direction."⁷ And now the Alliance needs to focus as well on global challenges posed by China.

Given current Russian provocations, it is natural to wonder whether the Strategic Concept would be better focused primarily on urgent here-and-now threats than on important but longer-term ambitions. That would be a mistake. The Strategic Concept must do both. The Strategic Concept is the only Alliance document that frames Alliance needs and tasks for the coming decade. A new Strategic Concept must be more than a snapshot of the present. Allies must use a new Strategic Concept to help them future-proof their societies against coming risks and threats.

We argue that NATO's new Strategic Concept should be framed by an approach we call "One Plus Four." The One is Alliance cohesion, which must be the central strategic underpinning of a new Concept. NATO must then be repositioned for current and future challenges, many of which are unconventional and unpredictable. This will require the Alliance to update and upgrade the three core tasks that headlined the 2010 Concept -- collective defense, crisis management, and cooperative security – and to add a fourth core task: building comprehensive resilience to disruptive threats to allied societies.

II. The One: Alliance Cohesion

The foundation for NATO's next Strategic Concept must be renewed Alliance cohesion rooted in a common commitment to shared values. Today, those values are under assault from external and internal challengers. Waning attention to NATO's core values has resulted in some allies prioritizing unilateral national decisions over collective Alliance interests, or using their position to block Alliance activities as a way to gain leverage in bilateral disputes. Some allies are themselves manipulating information and distorting data, undermining democratic processes and the rule of law, even threatening each other.

This is why a mutual affirmation of NATO's democratic foundation must begin with humility. Our achievements do not always match our aspirations. Nonetheless, those aspirations matter – and they are enshrined in the North Atlantic Treaty. The preamble to the 1949 North Atlantic Treaty that established NATO declares that the signatories “are determined to safeguard the freedom, common heritage and civilization of their peoples, founded on the principles of democracy, individual liberty and the rule of law.”⁸ Article II states, “The Parties will contribute toward the further development of peaceful and friendly international relations by strengthening their free institutions.”⁹

Democratic deficits exacerbate mutual doubts, which can gnaw at allied commitments to collective defense and mutual security. These points of disunity can be used by strategic competitors to destabilize individual allies or NATO as a whole. Countries with weak protections for democracy, individual liberty and the rule of law are vulnerable to subversion, corruption, mis- and dis-information. Malign influences within allied states could mean that non-NATO countries could influence NATO decision-making. Regaining cohesion in decision-making is premised on reinforcing NATO's core values. Deficits in internal values can become external threats. Celeste Wallander has called democratic fragility “the alliance's Achilles' heel.” The 2020 NATO Experts Group report warns that “a drift toward NATO disunity must be seen as a strategic rather than merely a tactical or optical problem.”¹⁰

In recent years, much strategic discussion has focused on competition among states of “great power.” It is becoming clear, however, that this competition extends beyond traditional measures of power; it centers increasingly on forms of governance. Adversaries big and small are selling autocracy as “efficient.” They tout their own systems and use a broad array of tools to amplify fissures and undermine confidence within democracies. When they can't do that successfully, they use diplomatic and other means of coercion. They support illiberal democracies. Others are beginning to follow their model. This puts democratic resilience at the heart of the new international system and international competition.

Resilient democracies have historically been less likely to experience intra- and interstate conflict, generate refugees, and harbor violent extremists. They are better at maintaining transparent institutions, civilian control of the military and intelligence services, and building trust and confidence with each other and with additional countries, all of which are core features of NATO's ability to collectively defend its members, manage crises, and cooperate with partners.¹¹

Ensuring cohesion can be difficult in an alliance that acts by consensus among 30 different democracies. Allies should review their decision-making procedures to ensure that the consensus rule does not hamper timely and effective responses to threats that can appear suddenly and unexpectedly. In this context, we endorse the proposal made by the NATO 2030 Experts Group to create a NATO net assessment office, composed of both military and civilian staff and reporting directly to the Secretary General, with the mission of examining NATO's strategic environment on the basis of agreed threats and challenges across the whole spectrum of military and non-military tools.¹² A common assessment of the strategic environment and its various challenges will help to provide greater alliance cohesion.

Affirmation of NATO as an alliance of democracies, and a commitment to ensure sound decision-making among those democracies, are foundational to NATO's ongoing missions. They must be enshrined in a new Strategic Concept.

III. The Four: NATO's Core Tasks

1. Collective Defense

a. Make It the Principal Core Task

Collective defense and deterrence remain central to NATO's purpose. Of NATO's core tasks, collective defense is *primus inter pares* – first among equals. It is the only core task mentioned explicitly in the North Atlantic Treaty. That priority should be made clear in the new Strategic Concept.¹³

What NATO Secretary General Jens Stoltenberg has called “full spectrum deterrence” means the Alliance must be able to dissuade and deter threats to its members, from whatever source and across all domains, while being prepared to defend all parts of NATO territory and to protect the critical functions of allied societies. NATO must provide collective defense against the full panoply of provocations, from low-level hybrid tactics and conventional military harassment on to nuclear blackmail. In a disruptive era, these threats can come from just around the corner or from far around the world. They can be persistent, simultaneous, and dynamic. The first core task will also need to be expanded in the new Strategic Concept to account for this full spectrum of threats.

Russia is likely to remain NATO's pacing adversary to 2030. Its persistent use of digital tools to disorient, and to disrupt and degrade critical functions of allied societies, its military interventions in neighboring countries, its recent positioning of more than 130,000 troops and logistical stocks on its border with NATO partner Ukraine, and its demands for unacceptable concessions from the Alliance, are all matters of great concern. Russia's actions have exposed gaps in NATO deterrence and highlighted potential new gaps to come. Crimea-style tactics, which are localized, low-intensity and quick, are designed to be just below the threshold of triggering Allies' commitment to mutual defense in response to armed attack. Currently, NATO is neither structured militarily nor disposed politically to handle such challenges properly. Moreover, Moscow's military doctrine, paired with its military-technological advances, could further impair NATO's ability to defend allies under attack, or it could present the Alliance with *fait accomplis* that may be hard to reverse. Russia's vast nuclear capability, in combination with repeated references by Russian leaders that they would willingly use nuclear weapons in the context of the doctrine of “escalate to de-escalate,” are more causes for grave concern.¹⁴

Deterrence to NATO's south and southeast is in many ways even more complicated when it comes to threats posed by terrorist attacks and Iranian missiles, assaults on Turkey, and instabilities that flow from sectarian violence, failing states, and mass migration. Knowing what tools may be effective against which threats can be difficult. Terrorists and religious extremist groups may not be susceptible to deterrence. They need to be defended against by a combination of prevention, protection, resilience, denial and punishment, plus disaster and humanitarian response measures. Many of these challenges are not NATO's alone, but they are NATO's as well. NATO is more likely to be one of many actors rather than the dominant player, and the forces required must be more agile, adaptable and synchronized with non-military instruments of power.

Projecting ahead, the Alliance needs to bridge current and future gaps in its ability to better integrate its political, military and technological capacities across all five operational domains: land, sea, air (including missile defense), cyberspace, and outer space. This is particularly important to counter Russia's overall strategy of cross-domain coercion, which seamlessly integrates conventional, nuclear, and hybrid elements, as well as to address other potential threats, whether from terrorists, digital disruptors, or countries like Iran or China.

NATO has been good at addressing each domain on its own. Being good at multi-domain operations is exponentially harder. Such operations extend far beyond the military dimension, incorporating political, economic, technological, social, and psychological considerations. They require the Alliance to better relate

deterrence and defense to resilience and to crisis management, to work more effectively with other partners, and to become more nimble, flexible, mobile, and innovative – qualities that have challenged NATO in the past. And they mean national security agencies and the Alliance as a whole will need to change their organizational cultures – perhaps the toughest challenge of all.¹⁵

The sections below expand on specific items related to collective defense including conventional defense, dealing with hybrid and cyber-attacks, nuclear deterrence, and operations in space. A major Task Force recommendation is that the Strategic Concept contain a separate part on “Guidelines for the Alliance future force posture,” which would detail steps needed for NATO’s future defense capabilities, with a special focus on multi-domain operations. A possible text for such a section is available as a separate Task Force product.¹⁶

b. Improve Conventional Deterrence and Defense

Now and over the coming decade, NATO conventional forces must be able to defend against major military forces from at least Russia in all five operational domains. Smaller-scale operations, generally to NATO’s south, while less demanding, may be more likely, and must also be anticipated and exercised. Both should be stressed in the new Strategic Concept.

The adequacy of NATO military capacity to meet these tasks is hard to assess and assure. Allied military commanders must be confident not only in the number of conventional formations allies will provide, but in their readiness, protection, sustainment, and interoperability, and in the capacity of allies’ infrastructure to bring adequate capability to bear -- at any time, at any point of defense, and across all domains. No ally can maintain these requirements without continuous investment; force modernization is a constant imperative. Allies can enhance their deterrent through regular exercises, better military mobility, greater pre-positioning, and forward in-place forces. The size, readiness and other details of forward forces should be adjusted as warranted by military risk assessments.

Since the 2014 Wales Summit, NATO has approved at least six initiatives for conventional rapid response, including:

- the enhanced NATO Response Force (eNRF),
- the Very High Readiness Force (VJTF),
- enhanced Forward Presence (eFP) battle groups on a rotational basis in the Baltic states and Poland, and tailored Forward Presence in the Black Sea region (Romania and Bulgaria),
- strengthening the NATO Command Structure with Joint Force Command (JFC) Norfolk and Joint support and Enabling Command (JSEC) Ulm,
- a broader reservoir of high readiness land, sea, and air forces to be created by full implementation of the NATO Readiness Initiative,¹⁷ and,
- NATO/EU cooperation to create the legal, transport infrastructure, command and control, and logistic conditions to enable rapid movement of military forces across Europe, on land and in the air, and to sustain them in theatre.

The new Strategic Concept will need to give additional political impetus to full implementation of these important ongoing initiatives. In addition, several others might be championed:

- *Strengthen NATO and U.S. forward presence in the east of NATO’s territory.* The current eFP and U.S. forward presence have each been judged adequate, given earlier circumstances. However, in light of Russia’s explicit strategic objectives, its aggressive posture and significant regional military superiority, as well as its time-distance advantage in the Baltic region, the eFP battlegroups must be enhanced significantly. Also, an additional permanent U.S. ground presence would be needed, particularly in the Baltic states.

- *Upgrade NATO's maritime posture to reflect the increased Russian threat.* The Alliance's maritime strategy, which was set in 2011, is out of date. In 2016, for instance, the Alliance replaced its 15-year-old Article 5 Operation Allied Endeavor in the Mediterranean with the much broader non-Article 5 mission set of Operation Sea Guardian. In 2022 Operation Neptune Strike conducted vigilance operations in the eastern Mediterranean in response to heightened tensions with Russia.¹⁸ NATO maritime forces have increased operations in the Black Sea within the limits of the 1936 Montreux Convention. NATO's Maritime Strategy must be updated, and its maritime posture upgraded, to address current and likely future contingencies.
- *Fill critical capability gaps to deal with Russia's anti-access/area denial (A2/AD) capabilities.* This would include counter A2/AD capabilities such as suppression of adversarial air defenses, availability of long-range precision strike conventional missiles, improved Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR), and additional electromagnetic warfare assets.¹⁹
- *Strengthen NATO's Special Operations Forces (SOF).* These forces will be of increasing value in a more turbulent and disruptive era. Like all forces, SOF must be backed by resilient infrastructure, combat enablers, and sustainment capacity kept at the same readiness levels as the forces they support.
- *Improve NATO interoperability.* Allied forces should also be better integrated and interoperable. Adoption of approved standards for interoperability across all forces and domains has become critical to NATO's effectiveness. The pace of systems technology, and the greater number of allies providing capabilities, demand constant standardization oversight and rigor.
- *Boost U.S. participation in the NATO Response Force (NRF).* The United States should take a more visible, active role in the NATO Response Force. Doing so will make a major statement of U.S. commitment to the Alliance where it counts most, the conduct of rapid response operations.

c. Bolster Deterrence and Defense Against Hybrid Threats

Advancing the Alliance's ability to deter and defend also means prioritizing ways to deal with unconventional conflicts that might hover below the Alliance's Article 5 mutual defense threshold. These include some types of cyberattacks, energy intimidation, financial destabilization, election interference, and dis- and misinformation campaigns. NATO's Strategic Communications Center of Excellence Command (CoE STRATCOM) needs creative new steps to detect and counter false information, including real time alerts to Allies on emerging threats and recommended countermeasures. Many relevant competences in Europe fall to national civilian authorities, to the private sector, or to the EU. While NATO can lead in developing and adapting cyber-deterrence and counter-disinformation guidelines and capabilities, better EU-NATO coordination and planning, will be needed. There is greater need to align and intensify action via the Helsinki-based European Center for Countering Hybrid Threats, ensuring there are operational feed-in loops to NATO and EU decision-making.

NATO and the defense establishments of its members are under constant attack from cyber hackers seeking to penetrate their information systems, extract data and plant viruses that could be used against allies. Digital disruptors target NATO systems, the operational cyber networks needed to execute military missions, and an extensive number of civilian networks that are essential to critical societal functions. Allies have determined that some types of cyber attacks could trigger Article 5 of the North Atlantic Treaty. In the 2016 Cyber Defense Pledge, allies affirmed their individual responsibilities under Article 3 of the Treaty to enhance their cyber defenses. The 2030 Reflection Group highlighted the need to develop both greater collective defense capacity in cyberspace and a more robust consultation framework to facilitate collective

defense, crisis management, and cooperative security in the cyber domain.²⁰ These concerns were largely echoed by allies in the 2021 Brussels Summit Communiqué.²¹

Nonetheless, allies have been reluctant to organize operational capabilities via NATO, and only five member states have announced that they will make sovereign cyber effects available to the Alliance.²² Limited measures thus far undertaken include deployment of cyber defense elements with NATO response forces, where continuous coordination and planning of cyber operations is essential. NATO has also gained initial experience through the SHAPE Cyber Operations Center (CyOC).

Box 1. Enhance Cybersecurity Through “Safe-to-Fail” Principles

If NATO is to effectively address the broad range of security challenges emanating from the cyber domain, the Alliance could complement its current collective defense efforts by incorporating cyber resilience and “safe-to-fail” principles into the new Strategic Concept.²³

Until now, NATO efforts to operationalize collective defense have relied primarily on ‘fail-deadly’ and ‘fail-safe’ logics in cyberspace. Should deterrence fail, ‘fail-deadly’ means the Alliance responds with the use of deadly force, whereas ‘fail-safe’ efforts are intended to ensure that the Alliance and its members can continue to operate safely and securely in the cyber domain.²⁴

While these two approaches are important, they only apply to a limited band of the full spectrum of threats presented by the cyber domain. Fail-deadly deterrence is only likely to succeed in preventing adversarial states from cyber operations that reach the threshold of armed conflict with destructive physical effects that are quickly attributable.²⁵ It is likely to be ineffective with state or non-state actors inflicting lower threshold attacks for which attribution is difficult. These considerations are further complicated by the differing legal restraints individual allies place on offensive cyber operations. Fail-safe measures also face several challenges. Given the sheer quantity of daily network probes experienced by NATO and individual member states, it is unlikely that every intrusion can be successfully countered or even identified. Highly sophisticated cyber operations are also likely to evade most defensive measures. Moreover, computers and systems increasingly rely on commercially available products and non-NATO-based manufacturers. Defensive strategies will have limited utility if hardware or software components have been preloaded with malware.²⁶

The Alliance and its members need to account for a variety of threats and scenarios for which fail-deadly and fail-safe strategies prove ineffective—such as ransomware attacks, distributed denials of service, exploitation of digital supply chains, or operations conducted by non-state actors. To withstand and bounce forward from such disruptions, NATO should ensure that military cyber functions and capabilities are ‘safe-to-fail’ -- that is, they can fail in ways that do not remove their ability to recover at or above original operating capacity. Incorporating safe-to-fail principles would require the Alliance to fill out the full meaning of Article 3, which is not limited to “self-help” but also includes “mutual aid.” It would mean coordinating with the private sector and de-conflicting economic priorities, as provided under Article 2. It would include developing metrics for assessing Allied operational success in cyberspace, and horizon-scanning for emerging cyber technologies that could affect Alliance security.²⁷

The Strategic Concept should take NATO efforts further. The United States might offer to be the framework nation in the next evolution of NATO cyber operations planning and coordination. A full NATO Cyber Defense Forces Headquarters (NCHQ) should be agreed, based on the proven NATO Special Operations Forces Headquarters (NSHQ) model. An NCHQ would improve cooperation among allies and protect NATO’s freedom of action in cyberspace, strengthening deterrence. Such a headquarters should generate the necessary arrangements and readiness to allow nations to plug their capabilities and produce cyber effects should there be a collective decision to do so. It should act to achieve consensus on issues of cyber

deterrence, particularly whether individual Alliance cyber defense capabilities alone are adequate or whether capabilities are needed to effectively deter major strikes against NATO networks, the networks of individual nations, or against the critical infrastructures of allied societies (Box 1). It should be linked to the EU's broader cyber toolbox.²⁸

d. Enhance Nuclear Deterrence

NATO should continue to be forthright about why nuclear deterrence remains critical to Alliance security. It should acknowledge that the world without nuclear weapons that NATO seeks is not today's world, and highlight the risks and dangers of Russia's nuclear saber-rattling, at a time when demise of the Intermediate-Range Nuclear Forces (INF) Treaty allows Russia to continue its deployments of nuclear INF systems within striking range of European allies.

The Strategic Concept should advance NATO's nuclear forces agenda in three ways. First, the Alliance must clearly restate its shared responsibility for NATO's nuclear forces by maintaining modern, safe and survivable U.S. weapons and survivable allied-dual capable delivery systems in Europe. Second, NATO needs to state a clear nuclear doctrine to more effectively deter Russia's "escalate to deescalate strategy."²⁹ Finally, while maintaining current weapons deployment posture, NATO should press hard for a return to nuclear and other arms control agreements, including a revival of the now defunct INF Treaty.

e. Deter and Defend in Outer Space

NATO deterrence and defense rely on assured access to outer space for communications, intelligence and warning, navigation, and many other functions. Space assets are essential to the stability of allied economies and societies. Without them, military powers are 'blind, deaf and mute.'³⁰ More than half of the approximately 3,000 government and commercial satellites in space operate from allied territory. Both kinetic and non-kinetic threats from, to, and within space could disrupt the space operations of the Alliance and its members, potentially leading to an Article 5 contingency. NATO has added a Space Operations Center to its Air Command (AIRCOM) and a Space Operations Center of Excellence in France. These agencies must articulate Alliance interests in space and assist members in coordinating their space resources via the NATO Defense Planning Process (NDPP) to meet NATO as well as national requirements. NATO must follow through on its Space Policy, agreed in June 2021, by realizing the Strategic Space Situational Awareness system at NATO headquarters, and working out procedures for NATO response to incidents in outer space, just as it has for other domains, including potential military measures and political consultations.

f. Be Prepared to Engage with Moscow

Enhanced measures of deterrence and defense should be reinforced by clear NATO offers to engage with Moscow. Engagement is not a favor to Putin; it is in NATO's own interests. As the Alliance suggested in the January 2022 NATO-Russia Council meeting, efforts could include minimizing escalation risks, avoiding inadvertent incidents or miscalculations at sea, on land, in the air, and in cyber and outer space, improving transparency and confidence-building measures, returning to nuclear and other arms control agreements and considering additional ones.

2. Crisis Management

While NATO needs to prioritize its collective defense core task, it cannot afford to neglect crisis management. Syria, Iraq, Northern Africa and the Mediterranean, Ukraine, Georgia, Bosnia and Kosovo are all active crises of varying intensity with significant implications for Alliance members. NATO and the EU have each launched crisis management initiatives, but most have suffered from partial participation and inadequate support.³¹ The chaotic withdrawal from Afghanistan after two decades of NATO military engagement will be a cautionary tale that may limit future NATO engagement. The Strategic Concept will

need to strike the right balance between necessary engagement in these operations and national reluctance to do so.

Box 2. Address Southern Challenges Through Comprehensive Support

NATO's southern security challenges are extraordinarily complex, in both form and force. Poverty, political instabilities and wars continue to inflict staggering human costs across the entire region, pushing millions to seek refuge on European shores. The wars in Syria, Libya and Yemen have become proxy conflicts that have devastated those countries and provided fertile grounds for terrorists, mercenaries, and other armed groups. Escalating armed conflict, displacement, hunger and widespread poverty are turning the Sahel into a hotbed of instability for terrorists and traffickers in drugs, weapons and human beings.³² Civil war in Ethiopia, Africa's second most-populous country, could destabilize the entire Horn of Africa. Foreign fighters returning to Europe and European-based extremists constitute a dire intelligence and security challenge for NATO member states. Horrific terrorist attacks are tragic evidence of clear and direct threats to the Euro-Atlantic community. Alliance concerns have been amplified by China's economic and military presence in Africa and Russia's enhanced military footprint across the region.

These ongoing crises have overburdened NATO allies and overwhelmed key NATO partners in the region. They have created fissures across Europe as countries struggle to cope and as their priorities collide. Addressing them requires integrated operations involving a multitude of countries and institutions. In some circumstances NATO may lead, but in most situations the Alliance is more likely to play a supporting role. Still, these complex challenges cut across each of NATO's core tasks: collective defense and deterrence, crisis management, and cooperative security. They are a vivid reminder that resilience has become a priority task for the Alliance. Throughout this report, we have suggested how upgrades to each of these tasks should apply to NATO's south. Taken together, as part of the implementation NATO's Concept for the Deterrence and Defence of the Euro-Atlantic Area (DDA), those elements should support a broad and flexible southern approach of "comprehensive support" that should include:

- Backing from NATO for lead nation and coalition operations undertaken by NATO members;
- Incorporating missile and air defenses, maritime surveillance, and counter-terrorism missions into exercises such as Sea Guardian;
- Implementing fully NATO's Framework for the South and investment in allies' expeditionary capabilities, as well as exercising southern contingencies in the Middle East-North Africa region;
- Strengthening crisis management capabilities such as Special Operations Forces, counter insurgency and aircraft designed for no-fly zones;
- Encouraging European strategic responsibility and closer NATO-EU ties
- Strengthening regional partners such as Israel, Jordan, Iraq, Morocco and Tunisia, and partnerships with the Gulf Cooperation Council and the African Union;
- Reinforcing NATO's political elements, including serving as a platform of dialogue among like-minded countries; and
- Focusing on deterrence and defense measures, particularly along the Turkish-Syrian border.

While NATO must do its part to encourage security in the south, allies must also recognize that many of the region's challenges are not readily amenable to Alliance solutions. NATO may be hard-pressed to shield allies from their consequences. Revitalizing the Alliance's resiliency through the measures suggested above, and others recommended below, would be important steps.

Over the next decade, Europeans and North Americans must anticipate and plan for contingencies related to additional armed conflicts, further displacement, persistent terrorist threats, and security challenges arising from political, economic, and environmental instabilities. They must improve their capacity to conduct scalable counter insurgency and stabilization operations, build partner capacity through training of defense and police forces, promote security sector assistance and reform, generate better situational

awareness, integrate civilian and military operations, and cooperate with private sector actors and civil society. Crisis management needs to be part of a comprehensive NATO Southern Approach (Box 2).

NATO's Special Operations Forces (SOF) capabilities are particularly important to crisis management missions in the south as well as to managing hybrid threats from Russia in the east. Nations should be encouraged to sustain their investment in SOF capabilities as a priority, even with tight budgets. This has to include the funding of participation in NATO as well as in bilateral and multilateral SOF exercises. NATO should continue to facilitate multinational SOF development through training, education, exercises and networking, and, if called upon, to deploy operational command and control of SOF from NATO's Special Operations Headquarters. SOF forces need to be more fully integrated into NATO's command structure. The evolution of hybrid warfare and disruptive challenges also means SOF must develop and maintain additional capacity to work with civilian authorities, including law enforcement and other security agencies.

To integrate the civilian and military aspects of crisis management missions, NATO should seek maximum benefit from its investment in the Comprehensive Crisis Operations and Management Center (CCOMC) at SHAPE. The CCOMC includes ready spaces for representatives of non-NATO organizations cooperating with the Alliance on crisis management. Lessons learned in Afghanistan need to be further assessed by NATO's Civil-Military Cooperation Center of Excellence in The Hague together with NATO's Joint Analysis and Lessons Learned Center in Lisbon.

Crisis management operations can be reinforced by more effective Alliance efforts at cooperative security, as addressed in the next section. Crisis management challenges demand more effective synergies between NATO and the EU, particularly Alliance support for greater European strategic responsibility that could enable Europe to be the "first responder" in crisis management operations in and along its periphery, as discussed in section IV.

3. Cooperative Security

The Alliance has defined its third core task of cooperative security primarily in terms of working on common security challenges together with other partners. This task remains important. Until now, however, NATO's approach to partnership has been demand-driven and largely voluntary. Particular initiatives advance because partners express interest and a number of allies commit attention and resources. It is time for the Alliance to use its partnerships more strategically and to prioritize those that may best advance Alliance interests. In addition, cooperative security must expand beyond bilateral or regional partnerships, to incorporate initiatives that address the security implications of challenges to the global commons.

NATO has more partners than members. Partners provide significant political support to the Alliance and can also contribute substantial military forces. NATO's partners can enhance the capabilities of the Alliance at low cost. The Alliance can make best use of its partnerships by considering three different groupings. One consists of partners that are aspirants to NATO membership. A second comprises partners along NATO's periphery that are not likely membership candidates. A third consists of other like-minded countries that either already contribute significantly to the common good or have the potential to do so.

When it comes to the first category, NATO's partnerships with Ukraine, Georgia, and Bosnia and Herzegovina are in flux, with each partner seeking NATO membership, but without allied consensus to take such a step. Allies should be careful not to close their door to the people of wider Europe, while at the same time working to deepen practical security cooperation and create conditions under which the question of accession, while controversial and difficult today, can be posed more positively in the future.

Box 3. Help Ukraine and Georgia Deter Russian Aggression

Seven years after illegally annexing Ukraine's Crimean Peninsula and launching a semi-covert proxy war in eastern Ukraine, Russia continues to hold Ukraine's security hostage. Further military provocations are likely. The best solution for Ukraine, fast-tracking its membership in NATO and giving it the added protection of an Article 5 guarantee, is not in the cards for the foreseeable future. Most NATO allies are not even prepared to take the preliminary, procedural step of granting Ukraine a Membership Action Plan (MAP). Under these circumstances, the Alliance risks eroding its own credibility by maintaining its current ambivalent stance: Indeed, by repeating NATO's 2008 declaration in Bucharest at every NATO summit – that Ukraine (and Georgia) “will become members” one day – but keeping the door shut in practice, NATO risks not only demoralizing the Ukrainians and Georgians, but signaling weakness to Moscow.

Given the stakes, allies should use NATO's new Strategic Concept to adopt a Ukrainian Deterrence Initiative (UDI) that would be an extension of the Alliance's Enhanced Opportunity Partner (EOP) program. Under this approach, allies would make it a strategic objective to do everything possible, short of extending an Article 5 guarantee, to help Ukraine defend itself and resist Russian destabilization. By maximizing Ukraine's capacity to impose significant costs on Russia for future aggression, NATO would bolster Ukraine's deterrence and increase its leverage for achieving a political settlement.

The initiative would encompass not only military equipment and training, but measures to increase Ukraine's resilience against cyber-attacks, financial disruption, disinformation, economic warfare and political subversion. The Ukraine-NATO Commission could provide for ad-hoc consultations whenever Ukraine or allies believe the territorial integrity, political independence or security of any of the parties is threatened. Ukraine should gain more access to the Alliance's Centers of Excellence. Additional possibilities should be generated for Ukraine to benefit from NATO Trust Funds, which provide resources to help partner countries implement practical projects in the areas of demilitarization, defense transformation and capacity building. A new Trust Fund should be added, dedicated to capability development and focused on defensive weapons acquisitions.

A similar Georgian Deterrence Initiative (GDI) could be offered to Georgia. If requested, elements could also extend to Sweden and Finland. All of these countries already have EOP status and face constant Russian military and political pressure. They could build on the example of the 2021 U.S.-Georgian Defense and Deterrence Enhancement Initiative.

Rather than adhering to the standard formula that NATO partnerships are demand-driven and funded largely by voluntary national contributions, under the UDI and GDI NATO would be proactive in assisting Ukraine (and other EOP partners) by making it a formal NATO responsibility, backed by common funding, to help train Ukrainian armed forces and to facilitate their acquisition of modern defensive weapons that would raise the cost to Russia for any new aggression – such as anti-armor capabilities, counter-artillery systems, air and missile defense, anti-ship missiles and combat drones. This would be of far greater benefit to Ukraine and Georgia than a MAP, which is largely symbolic.

The strategy could be further reinforced by steps to increase NATO's military presence in Ukraine and establish an enhanced rhythm of rotational deployments by allies' forces to Ukraine and the region. This could include establishing a joint army training and evaluation center like the one established in Georgia in 2014, a joint naval training and servicing facility in the Black Sea, and more frequent exercises with Ukrainian and other Black Sea partners to defend freedom of navigation. As part of this effort, allies could help Ukraine finance the construction of NATO-compatible military infrastructure, such as airfields, railheads, and port facilities.

The stakes go beyond Ukraine. They relate to the future of a rules-based international order based on the sovereignty of all independent states, inviolability of borders and peaceful settlement of disputes. If Putin were to succeed in re-subjugating Ukraine, it would be a major blow to NATO's vision of the liberal international order, and a recipe for long-term instability in the heart of Europe.

Russia intervened militarily in Georgia in 2008 and in Ukraine in 2014. Both countries remain primary targets of Russian aggression, with Russian forces on their soil. The Alliance should consider deeper deterrent and resilience initiatives that make those partnerships more meaningful operationally (Box 3).

Strengthening category two partners in the south will be critical. Jordan has been a key source of stability in a sea of tumult. Yet it is poised precariously on the front lines of conflict. This has led to severe security concerns for Jordan's government and has made Jordan a key host for refugees. Prioritizing mechanisms for assisting Jordan should be integral to NATO's southern strategy. The Alliance should also inject life in bilateral partnerships, for instance with Israel, Morocco and Tunisia. This should include reinvigorated intelligence-sharing and capacity-building.

In terms of category three (very capable like-minded partners), relationships with Sweden and Finland can evolve further to the point where they are virtual members just short of having an Article 5 commitment. NATO should also supplement its Enhanced Operational Partnership with Australia and pursue similar arrangements with Japan and South Korea, as outlined in more detail in Section V.

Perhaps most importantly, a new Strategic Concept can anchor a true NATO-EU strategic partnership to promote European strategic responsibility, leverage synergies and resources, address a range of civil-military and unconventional challenges, and shore up democratic standards and shared resilience. Given the imperative of rapid mobility and reinforcement in the event of danger to the Alliance, NATO-EU partnership is essential to creating a "military Schengen"³³ to ease cross-border movements, mirroring the EU's own civilian Schengen zone.

Beyond these specific categories of partnership, cooperative security must evolve to encompass challenges to the global commons. The Alliance is an important actor in at least four dimensions of the global commons, including: 1) protecting freedom of the seas, 2) upholding the global information commons; 3) ensuring security and norms of peaceful behavior in space; and 4) protecting Alliance equities in Arctic security. As outlined in chapter V, China's activities pose challenges in all four areas. Such challenges only can be addressed cooperatively with a range of non-NATO state and non-state actors. In some areas, NATO will not be the lead institution, but it can offer specialized capabilities. In other areas, for instance, in protecting freedom of navigation, it needs to be equipped to play a leading role. The Strategic Concept should highlight NATO's interest in the global commons and suggest partnerships as one important tool to manage those interests.

NATO has already noted that climate change is a threat multiplier that can exacerbate political and societal tensions, limit the availability of food and water, undermine human health, affect global maritime security, displace people, degrade infrastructure and economies, compromise biodiversity, and exacerbate extreme weather. It is challenging military missions, operational plans and installations. Moreover, the carbon footprints of North American and European militaries are massive. The U.S. military alone releases more greenhouse gas than 140 countries, emitting more than 25,000 kilotons of carbon dioxide a year. Most military infrastructure is not energy efficient; heating accounts for a third of EU armed forces' energy consumption.³⁴

The Alliance's initial effort to address the security implications of climate change is encapsulated in its 2021 Action Plan on Climate Change and Security. The plan's four cornerstones of awareness, adaptation, mitigation and outreach are all solid beginnings, but each must be further elaborated, especially regarding operational challenges. Training, education, exercises and standards will need to be rethought and renovated. The purchasing power of the military should be used to fuel investments in cleaner energy, infrastructure and preventive technologies to mitigate the effects of climate change.³⁵ Consideration should be given to incorporate the possible capability-related elements of climate and related energy transitions into the NATO Defense Planning Process and in NATO Security Investment Program decisions on future infrastructure spending. Allied Command Operations should consider climate-induced contingencies to which the NRF may need to respond, given that it was already deployed in response to Hurricane Katrina and to an earthquake in Pakistan. ACT should work with individual allied nations to assess training areas and other readiness infrastructure that might need investment to protect from climate-induced damage.

Reducing energy demand and increasing energy resilience is essential for the armed forces to ensure a high level of readiness and sustainability. Canada, and a number of other NATO allies that are also EU members, have adopted environmental sustainability policies for their armed forces that could offer good practice. Various initiatives are under way within NATO and the EU, yet efforts are scattered and sometimes duplicative. NATO and EU forces should accelerate their efforts. EU-NATO staff-to-staff dialogues can explore potential areas of cooperation linked to climate and defense, including means through which military establishments can assess and manage climate-change-related vulnerabilities to acquisition and supply. These issues should also be part of the U.S.-EU Dialogue on Security and Defense.

Canada has offered to host a Center of Excellence on Climate and Security to enhance situational awareness that would enable allies to anticipate, adapt, and act to meet security challenges posed by climate change. Optimally, it would be an independent center, similar to the model established by the Center of Excellence for Countering Hybrid Threats in Helsinki, which would offer greater synergies and facilitate NATO-EU cooperation.

Beyond these initiatives, NATO can be a platform for security risk assessment, information-sharing and resilience support among partners. NATO's Centers of Excellence and its structures for education and training are useful vehicles through which allies and partners can share good practices in a wide range of areas, including energy security, terrorism, cyber and hybrid threats, strategic communications and resilience. Additional Centers on the security implications of economic and technological interdependencies should be considered with Indo-Pacific partners.

4. A New Core Task: Comprehensive Resilience

The growing need to implement operationally the concept of resilience—the ability to anticipate, prevent, and, if necessary, protect against and bounce forward from disruptions to critical functions of our societies—has become a challenge on par with NATO's other core tasks. It is essential to the other three, yet it has not been integrated adequately into allied planning or operational activities beyond narrow country-by-country baseline requirements. It must deal with a spectrum of challenges that are not addressed adequately by the other core tasks. And NATO's efforts thus far betray a static understanding of resilience, which encompasses a wide range of dynamic interconnections. We understand the reluctance of some to create a fourth core task, but given the importance of resilience in a world of disruption and the inability to merge it adequately with the other three core tasks, we urge Alliance leaders to reconsider and create such a new fourth core task.

NATO must move beyond country-by-country metrics and adapt a more comprehensive approach that embraces and operationalizes the mutually-reinforcing concepts of democratic resilience, shared resilience and forward resilience. The foundational importance of democratic resilience was discussed in chapter II. Shared and forward resilience are equally essential.³⁶

In Article 3 allies commit to build resilience against armed attack through “continuous and effective self-help and mutual aid.” Until now, NATO's resilience efforts through country-by-country baseline requirements have focused on the first part of that phrase: “self-help.” Adopting comprehensive resilience would give meaning to the second part of that phrase: “mutual aid.” Article 3 also provides the basis for NATO's cooperation on resilience with partner governments and the private sector.

Each NATO member state bears primary responsibility for ensuring the resilience of its own democratic society. Resilience begins at home. However, in an age potentially catastrophic terrorism, networked threats and disruptive cyber-attacks, no nation is home alone. Few critical infrastructures that sustain the societal functions of an individual country are limited today to the national borders of that country. Strong efforts

in one country may mean little if a neighboring ally is weak. The upshot: governments accustomed to protecting their territories must also be able to protect their connectedness — the vital arteries that are the lifeblood of open societies. Resilience will never be achieved on a country-by-country basis; Allies dependent on mutual flows of people, power, goods and services must move from country-by-country baseline requirements to *shared* resilience, by establishing together metrics that can ensure their mutual security. This needs to include but go beyond critical infrastructures to encompass key industries, financial flows, strategic ports and transportation/reception nodes, supply chains, communications and information networks, and other elements of the connective tissue that binds allies' critical societal functions.

This leads to the concept of *forward* resilience, which has two components, one spatial and one temporal.

The spatial component essentially means projecting shared resilience forward to non-NATO partners. We see the importance of this today in Ukraine, which is being used by Russia as an experimental laboratory for hybrid threats and disruptive attacks on critical societal functions. Since Russia's 2014 military intervention in Ukraine, its digital disruptors have engaged in a relentless effort to weaken Ukraine and stymie its efforts to align more closely with the West by attacking the country's critical infrastructure, incapacitating electricity grids, subway systems and airports. Because Kyiv is largely unable to retaliate, Russia has also found Ukraine to be a useful testing ground for its cyberwarfare capabilities.

In the current crisis, NATO has acted to help Kyiv become more resilient to such attacks. That is good — but allies should not think of such help as a “one-off” in the middle of a passing crisis, they should think of it as an ongoing, integral part of NATO' mission going forward.

Ukraine is not a lone example. All across Europe's southern and eastern peripheries disruptive challenges to weak democracies can ripple back into NATO territory. These examples underscore NATO's interest in projecting resilience capacities forward to vulnerable democratic partners. Allies should share societal resilience approaches and operational procedures with partners to improve democratic resilience to corruption, psychological and information warfare, interference with elections or democratic institutions, and disruptions to cyber, financial and energy networks and other critical infrastructures. Shared resilience efforts among allies in the areas outlined above should be extended as possible to critical NATO and EU partners. Creating a higher degree of resilience in vulnerable societies makes it more difficult for malign state or non-state actors alike to disrupt and create the instability they need for their success.

Forward resilience also has a temporal connotation, as in thinking and acting forward in time — anticipating disruptive challenges coming our way, and acting to prevent, mitigate or adapt to them. This is another reason to consider a NATO Office of Net Assessment. It can inform NATO's efforts to mitigate and adapt to the security consequences of climate change and disruptive technologies.

Corrosive cyber operations, disruptions to defense-relevant supply chains, and the COVID-19 pandemic have each underscored the need for the Alliance to address more effectively unconventional challenges to human security. Comprehensive resilience would also include efforts to withstand hybrid attacks on NATO societies and political will. NATO will also be impacted by global warming. Efforts to deal with it eventually may require the capabilities of NATO militaries for issues like emergency rescue and logistics support.

Resilience is a job for NATO, but it need not be a job for NATO alone. Enhanced NATO-EU cooperation offers a means to leverage the combined resources of both organizations in common cause. Most NATO member states are also EU member states. Much of the resilience challenge has to do with civilian institutions and privately-owned infrastructures, many of which are integrated into EU structures and processes. Fortunately, NATO and the EU already work closely on resilience issues related to critical

infrastructure protection; they should extend that cooperation to issues of democratic, shared, and forward resilience.

During the Cold War, allies knew where the front line was. After the Cold War, they hoped that there would be no more front lines. Today, allies are focused on front-line challenges to their east and to their south. In this age of disruption, however, the front line could be anywhere – the Polish-Russian border, Istanbul’s Grand Bazaar, Frankfurt’s airport, Italy’s food supply, transatlantic subsea cable links, the Internet, the Washington DC metro, or the Hoover Dam. Building resilience to disruptive threats is a major common task for North America and Europe. For a quarter-century, NATO’s mantra was “out of area or out of business.” Today, it must be “in area or in trouble.”

Agreeing on a new core task of comprehensive resilience promises to be the most innovative, forward-looking feature of a new Strategic Concept. It and the other core tasks are also mutually reinforcing. Collective defense and deterrence remain central to NATO’s purpose; they will be more credible if our democracies are more resilient. Many crises along NATO’s borders cannot be prevented or managed through military means alone; operationalizing the concepts of shared and forward resilience will improve the Alliance’s core task of crisis management. And NATO can do more to bring its unparalleled experience as an alliance of resilient democracies to its third core task of cooperative security.

IV. Rebalancing the Transatlantic Partnership

As NATO grapples with new and complex strategic realities, it can no longer afford its excessive reliance on the United States, either for collective defense or for crisis management and cooperative security missions beyond Europe’s borders. The United States will have to pay increasing attention to China and limit its involvement in the Middle East and South Asia. The United States will therefore increasingly look to the European allies to shoulder more of the common burden, and encourage greater contributions to security by the European Union and non-NATO partners like Finland and Sweden.³⁷

Over the next decade, NATO must transform itself into a more balanced transatlantic partnership in which Europe assumes greater strategic responsibility while reinforcing the transatlantic link. Setting the goal of a rebalanced Alliance in the new Strategic Concept would move allies beyond contentious arguments over burden-sharing and embrace Europe’s longstanding ambition to play a larger role in its own defense, while sidestepping semantic sideshows over the meaning of “European strategic autonomy,” which has become politically toxic in some allied nations.

Advancing greater European strategic responsibility starts by defining the concept in a way designed to strengthen the Alliance. It should focus on two military goals:

- The first should be to enhance the European allies’ conventional military capabilities to a level that would provide half of the forces and capabilities, including the strategic enablers, required for deterrence and collective defense against major-power aggression. Should a conflict simultaneously break out with China in Asia and Russia in Europe, the United States may not be able to deploy adequate reinforcements to Europe. European allies need to be able to pick up the slack.
- The second goal should be to develop European capabilities to conduct crisis management operations in Europe’s neighborhood without today’s heavy reliance on American enablers such as strategic lift, refueling, command, control and reconnaissance. The withdrawal from Afghanistan was just the latest demonstration of Europe’s continued dependence on U.S. enablers.

Meeting these two goals would allow Europe to become the first responder to most crises in its neighborhood, acting through NATO, through the EU, or through ad hoc coalitions of the willing. It would

permit the United States to shift some of its forces and strategic focus to the Indo-Pacific region without any significant reduction in the capabilities needed to deter Russia.

To achieve these goals, allies could agree within the NATO Defense Planning Process to a military level of ambition for European strategic responsibility. European allies and Canada could commit to investing sufficient resources to ensure that, by the end of the decade, they can meet 50% of NATO's Minimum Capability Requirements. This would mean fully usable forces required to cover the whole spectrum of operations and missions, as well as the strategic enablers needed to conduct multiple large- and small-scale missions – if necessary, without U.S. support.

Meeting this standard will take time, given Europe's current lack of enablers, its relatively low readiness rates, and its fragmented military industrial complex. Building European strategic responsibility will be a process, not a one-time event. The new Strategic Concept should launch that process, reinforced by complementary efforts via the EU's Strategic Compass.

Greater European strategic responsibility will require more, not less, transatlantic consultation on political-military matters. When Europe acquires the military capabilities needed to exercise real strategic responsibility, its political voice will be amplified. Diplomatic differences may still arise, but a dialogue among equals is more likely to overcome areas of disagreement. That said, new mechanisms for NATO-EU coordination will be needed.

Greater European strategic responsibility could clarify who would lead certain missions and what they need to do to succeed. European nations could become the first responders to future crises in neighboring North Africa and the Middle East. They might take the lead for cooperative security missions such as training with NATO partners around the Black Sea or in the Western Balkans. The United States would continue to lead collective defense operations against a major adversary in Europe in combination with more robust European forces. To reassure allies that there would be no diminution in the U.S. commitment to deter Russia, the United States could move additional ground forces to Europe.

Institutional and command arrangements need to be refined to make it easier for the Europeans to conduct autonomous operations. The EU or individual European nations might lead smaller crisis response operations, modeled on French-led operations in North Africa. Most larger operations would continue to be conducted by NATO, because its integrated military command structure has unique experience in doing so. Efforts could be animated by the so-called Berlin Plus command arrangements, yet generate a more effective framework so that NATO's command structure could be used for EU-led operations, with a European general in charge.

Greater strategic responsibility for Europe also requires improved defense industrial cooperation and efficiencies across Europe. The European Defense Agency (EDA), European Defense Fund (EDF), and Permanent Structured Cooperation (PESCO) have aimed to make Europe's defense industry more efficient and effective. A transatlantic understanding on European strategic responsibility could encourage streamlining of Europe's defense industry without excluding U.S. technologies that could improve their output and ensure interoperability.

The United States has resisted EU calls for a greater European defense role since the idea was first promoted in the early 1990s. U.S. concerns centered on the danger of competition and duplication with NATO structures and planning processes, along with doubts about the capacity of European militaries to conduct even small-scale operations without U.S. support. Given today's security environment, it is past time for the United States to shed its ambivalence and work with its European allies and the EU to make strategic autonomy – defined as greater strategic responsibility – a win-win for both sides of the Atlantic. Agreeing to greater European strategic responsibility will be much more effective at rebalancing transatlantic military

responsibilities than continued American harping about burden-sharing. Europeans will be more effectively animated to invest more in their defense by understanding what they are expected to contribute and why.

NATO's goal that every ally spends 2% of its GDP on defense has become an important political metric of allied commitment, and there is good reason for allies to invest more in their security following decades of neglect and in the face of the serious threats and complex challenges outlined in this report. In many ways, however, the 2% benchmark is an arbitrary measure. It ties a static target (2%) to a moveable value (GDP). It is not tied to any element of Allied strategy. It is a measure of input (money) rather than output (capabilities). Even though NATO's adversaries persistently deploy cyber assaults and seek to disrupt critical societal functions within the Alliance, allied investments in cyber protection and related resilience measures do not adequately count against the 2% goal. In short, spending more is not the same as spending well. Spending levels alone tell us little whether allies are doing what they need to do to deter, defend, manage crisis, enhance cooperative security, and ensure greater resilience.

The 2% goal has had positive impact on defense spending and thus it would be ill-advised to abandon it. But ways can be developed to improve output measures and count expenditures that are security-related. A new Strategic Concept that promotes European strategic responsibility, generates attention to a diverse range of external dangers, and highlights the need to enhance resilience and human security, could offer the Alliance a way to tune the burden-sharing debate to new circumstances.

V. Connecting the North Atlantic and the Indo-Pacific

The Indo-Pacific and European theaters are increasingly linked. NATO's ability to address traditional and unconventional threats in Europe is becoming intertwined with related challenges to Alliance security interests posed by China.

1. Strategic Challenges

The strategic challenges to the Alliance from China are multifold. Seven broad categories of challenges are discussed below.

a. Chinese technological advances have a number of direct security implications for NATO.

- *5G/6G infrastructures.* Huawei's emergence as a dominant 5G telecommunications infrastructure supplier for many countries gives Beijing access to key parts of emerging communications networks, generating choke points of vulnerability for Allied nations. Within 15 years, 5G is likely to be replaced by dual-use 6G technologies with embedded AI-enabled capabilities of military significance. China is likely to incorporate them into its military-civil fusion strategy, as it has with 5G.³⁸
- *Defense-relevant technologies.* Beijing is seeking technological dominance in Command, Control, Communication Systems (key for political and military decision-making); Intelligence, Surveillance, Reconnaissance (key for situation awareness); logistical and digital cyber systems (key for deployment of forces and military operations across all domains); and artificial intelligence (key for long-term competitiveness in unmanned systems, C4ISR, and novel operational concepts). China's civil-military fusion strategy leverages investments in traditionally civilian sectors to enhance development of its military and emerging disruptive technologies.
- *Quantum technologies.* Beijing is developing quantum technology with military applications in sensing, communications, and data processing. A universal fault-tolerant quantum computer would render Alliance encryption systems vulnerable.
- *Cyberattacks.* Beijing has the ability to tap into data flows via intercontinental and inter-regional cables. It has used China Telecom's "points of presence" in North America and Europe to hijack data traffic

through Chinese servers. The challenge is likely to grow: use of AI in cyberattacks is likely to enable malware to adapt to countermeasures and security controls more rapidly than human-centered systems.

- *Splinternet*. China, through Huawei, is proposing a New Internet Protocol that is nothing less than an attempt to set the rules and design the architecture of a new internet. New IP would bake authoritarianism into the architecture underpinning the web and give state-run internet service providers granular control over citizens' use.
- *Power projection*. China's military rise is starting to match its economic ascent. Over the past decade, its defense budget has grown significantly and it has embarked on an ambitious process of military modernization using its cutting-edge technologies. Currently a regional military power that pursues a variety of hybrid tactics in its maritime disputes with many of its neighbors, it will be able to increasingly project extra-regional power in the next decade.³⁹

b. European and North Atlantic security can be impaired by dangerous dependencies. Those dependencies are created by Chinese investments in European infrastructure and technologies, including strategic ports, telecoms, power grids, defense-related supply chains, and extreme reliance on China for rare earths and critical materials. Beijing has instrumentalized these dependencies in the past. Moreover, China's connectivity strategies, including through its Belt and Road initiatives (BRI), are not only intended to extend supply chains and logistics routes; they are about creating conditions to push forward Chinese standards, practices and digital flows. More than half of NATO's allies have signed BRI-related agreements. Those dependencies can affect European decision-making and Alliance operations in time of crisis and/or conflict.

c. China's maritime claims, its space policies and activities in the Arctic could threaten key principles of the global commons. Those claims could be further accentuated by Beijing's efforts to erode the East Asian regional order.

- *Freedom of the seas*. In the South China Sea, China's maritime claims and grey-zone dominance activities have restricted the ability of its neighbors to access resources in their own waters in contravention of international law. The vast majority of Europe's trade with Asia flows through maritime passages that are contested by China. In addition, China has been commissioning ships at a rate unprecedented in peacetime since before World War II, adding the equivalent of a full British Royal Navy each year. China's naval build-up has made China a peer competitor to the United States, increasing China's capacity to challenge freedom of navigation operations and harass foreign vessels. Over the next decade, China is likely to extend its maritime reach into the Atlantic; it is already working to establish Atlantic ports in Africa.
- *Freedom of information*. In the global information commons, China's diffusion of surveillance, censorship, and disinformation, as well as the use of its economic weight for narrative control threaten the open information environment upon which democracies depend.⁴⁰
- *Militarizing space*. China continues to invest in improving its military space capabilities, including for intelligence, surveillance and reconnaissance, satellite communication, satellite navigation, anti-satellite capabilities, and meteorology, despite Beijing's public stance against the militarization of space. Chinese strategists regard the ability to use space-based systems and deny them to adversaries as central to digitally-enabled warfare.
- *Arctic security*. China has asserted itself as much as possible as a "near-Arctic" state, and has stated a goal of connecting China to Europe through a "Polar Silk Road" over the Arctic Ocean to deepen economic ties and gain access to resources in the region. There is skepticism, however, as to whether China will remain committed to respecting international law, especially as melting ice opens new shipping and transit routes. While China's current activities in the Arctic are primarily economic or scientific in nature, many have dual-use potential and could serve as precursors to eventual military build-up.

d. China-Russia entente raises concerns for NATO. Beijing and Moscow have stepped up the frequency and scale of joint military exercises, including in the Baltic and Mediterranean Seas, complicating NATO defense planning, which has been based on the premise that Putin’s Russia posed the only serious threat to Allies territorial integrity, and that Russia stood alone, without militarily capable allies. Greater Russian-Chinese defense industrial cooperation on sensitive technology, such as theatre hypersonic weapons, counter-space capabilities, or submarine technology, would present significant challenges for NATO Allies. Moreover, China-Russia entente could change the risk calculus of either or both parties, possibly leading to reckless behavior that could imperil Alliance security.

e. Conflict in the Indo-Pacific has significant implications for Europe. China’s military growth, its worrying military-technological advances, and its aggressive regional policies have made it America’s pacing factor in developing defense capabilities and policies. China’s aggressive territorial claims in the South and East China Seas, and its threats to the integrity of Taiwan, present a real risk of conflict in the Indo-Pacific, including direct confrontation between China and the United States. In such a situation, critical sea lanes of communication, maritime shipping, and European commercial interactions with China, and with Asia more broadly, would be disrupted. The interests of various European allies in the Indo-Pacific would be at risk. Opportunities would be created for Russia. U.S. forces might not be available to adequately reinforce European allies against a simultaneous Russian military challenge. European allies would need to quickly fill those gaps. They need to plan now how they would do so.

f. Chinese nuclear warheads and missiles can reach all parts of the North Atlantic region. In addition, China’s nuclear developments threaten to complicate U.S.-Russian arms control arrangements, even as Beijing refuses to enter into arms control discussions. NATO efforts to encourage China to engage in nuclear arms control negotiations are important.⁴¹

g. Humanitarian and diplomatic practices concern NATO. In addition to these security risks, the interests of NATO member states are affected by Beijing’s stated ambitions and assertive behavior on other fronts, all of which together NATO leaders have agreed “present systemic challenges to the rules-based international order.”⁴² Those challenges include gross human rights abuses, widespread diplomatic coercion and disinformation campaigns, unfair trade and investment practices, and creation of economic and technological dependencies among a range of states across Eurasia and into Africa. At the same time, NATO leaders have been careful not to label China a military adversary or an enemy. They have noted areas of potential cooperation, including global warming, pandemic control, arms control, non-proliferation, and counter-terrorism. This wide array of issues beyond NATO’s immediate remit underscores the need for NATO’s efforts to be carefully coordinated with diplomatic, economic, and technology approaches organized by the EU, the G7, and other like-minded democratic partners.

2. Implications for the Strategic Concept and Recommendations

With these security challenges and broader considerations in mind, NATO’s new Strategic Concept needs to define the strategic connections between North Atlantic and Indo-Pacific security, including the nature of China’s strategic relationship with the Alliance, and chart ways to address them. As part of an overall approach to the Indo-Pacific, allies should design a dual-track policy toward China that focuses on competition and possible confrontation on the one hand, and cooperation where possible on the other hand. It should contain the following measures:

a. Explore deeper coordination under Article 2 of the North Atlantic Treaty, which commits allies to promote “conditions of stability and well-being” and to “encourage economic collaboration.” Article 2 offers a frame through which allies could work to enhance investment screening of foreign investment in security-related infrastructures, companies and technologies, as well as other steps to protect individual allied nations from security-related dependencies on China. Article 2 also offers a framework for enhanced

cooperation with the European Union on these issues, including common or complementary principles of action with regard to economic-security contingencies.

b. Bolster NATO's commitment to critical infrastructure defense and secure supply chains within the upgraded frame of comprehensive resilience.

- *Update NATO's secure telecommunications requirements for 5G.* Incorporate secure 5G spending and other cyber and infrastructure protections into NATO's spending goals.⁴³
- *Conduct an Alliance-wide review of defense supply chain dependencies on China.* Establish a NATO-EU Dialogue to address threats to critical infrastructure, investment screening, export controls (including of dual-use technology), telecommunications, and supply chains.
- *Set standards for NATO members and partners regarding external investment in critical infrastructure,* particularly if that infrastructure plays a role in the NATO mission.
- *Increase cooperation between NATO and international development finance corporations* to highlight alternative investment options for critical infrastructure, especially among newer members and partners.

c. Create new North Atlantic-Indo-Pacific partnerships.

- *Invite Japan and the Republic of Korea to join Australia as NATO Enhanced Opportunities Partners.* Varying levels of enhanced military cooperation could be considered, from information sharing and joint exercises to joint operational planning or joint command centers.
- *Create a NATO Liaison Office in Tokyo or Seoul.*
- *Create an Indo-Pacific/NATO Council or Commission* as a forum by which the Alliance and close partners from the region can identify cooperative activities and share assessments about evolving security challenges, including from China.
- *Establish Centers of Excellence (COE) in the Indo-Pacific.* Much like current COEs in Helsinki and Bucharest, these centers would not be formal NATO entities but be open to participation by a host of actors, including NATO. Private sector actors could also participate. Priority issues are a) addressing security challenges arising from economic interdependencies and technological advances; and b) security challenges related to competition in the global commons.
- *Establish a Freedom of Navigation Operations program in the South China Sea* in which NATO Allies and other partner nations would participate.
- *Explore an ad-hoc, issue-by-issue dialogue with India,* which has not indicated interest in a deeper partnership with NATO yet shares overlapping concerns regarding Chinese actions and intentions.
- *Consider creation of a NATO-China Council* to maintain diplomatic dialogue, explore potential areas of cooperation, and design crisis management measures.

VI. Implementing NATO's Overarching Military Concept Informed by Innovative and Disruptive Technologies

In Ernest Hemingway's novel *The Sun Also Rises*, a character named Mike is asked how he went bankrupt. "Two ways," he answers. "Gradually, then suddenly." Technological changes can happen much the same way. Seemingly small or incremental innovations accumulate, and suddenly the world is a different place. In recent decades there have been a lot of "gradually, then suddenly" movements: the World Wide Web, open-source software, big data, cloud computing, sensors and ubiquitous computing, and now the pervasive effects of artificial intelligence (AI), 5G networks, and algorithmic systems.⁴⁴ These and other rapid technological advances can be used to improve the human condition, but they are also changing the character of modern conflict.⁴⁵

State and non-state actors alike are employing enabling technologies to enhance their ability to prevail in conflict. Unmanned platforms are proliferating on land, at sea, and in the air. The literature on previous revolutions in military affairs (RMAs) suggests that those who manage to harness and exploit new technologies, combine them with novel operational and organizational concepts, and evolve a new way of war, stand to gain significantly – a sobering insight in this era of strategic competition.⁴⁶ “Artificial intelligence is the future,” Vladimir Putin has said. “Whoever becomes the leader in this sphere will become ruler of the world.”⁴⁷ According to China’s leader Xi Jinping, “technological innovation has become the main battleground of the global playing field, and competition for tech dominance will grow unprecedentedly fierce.”⁴⁸

NATO cannot just keep pace with rapid technological advances; it must maintain its technological edge. The Alliance has recognized this imperative, launching various capability initiatives, including its Emerging and Disruptive Technologies (EDT) Roadmap for research on emerging technologies such as AI, quantum computing, autonomy and hypersonic missiles. European NATO members that are also EU members have similarly agreed on a series of capability improvement initiatives, and the United States is working to harness emerging technological capabilities through new operational concepts such as multi-domain or integrated operations. Nonetheless, developments in the United States are outstripping those in Europe, risking a military-technological gap between the two sides of the Atlantic that can make it difficult for allied forces to operate together, even when they want to. Allied nations also have diverse positions with regard to the legitimacy, desirability and practicality of new types of military systems.

The Strategic Concept is an opportunity to highlight this challenge and guide expeditious and comprehensive implementation of NATO’s effort to foster and protect EDTs, a strategy that allows for military modernization among NATO member states at various speeds and with varying scope, while avoiding technical, tactical and doctrinal loss of interoperability.

This effort should be animated by implementation of NATO’s Comprehensive Concept for Deterrence and Defense in the Euro-Atlantic Area (DDA), the 2021 NATO Warfighting Capstone Concept, and SACEUR’s AOR-wide Strategic Plan (SASP), which undergird NATO’s overall strategic posture. During the Cold War, deterrence relied on an operational concept that tied NATO’s nuclear and conventional forces together to undermine the preferred strategy of NATO’s adversary. During the 1970s and 1980s, the basis for military modernization among NATO’s militaries was provided by the concept of Follow-On Forces Attack and the rediscovery of maneuver warfare through AirLand Battle. These concepts clearly defined roles and missions in the various domains, which in turn provided the logic for weapon system development and procurement, and for investments in promising emerging technologies. Today, the United States is exploring the merits and implications of Multi-Domain Operations, yet NATO currently lacks an equivalent overarching concept. Such an approach needs to identify “defeat mechanisms,” which will help the Alliance consider the capability and organizational requirements that will be needed.⁴⁹ This is an important weakness that must be addressed. This overarching military concept should:

- Identify for allies the priority technologies impacting its core tasks. Members should be asked to resource these priorities. NATO has already identified seven priority science and technology areas.⁵⁰ Given the rapid pace of technological developments, it should review these on an ongoing basis.
- Use NATO’s Defense Innovation Accelerator for the North Atlantic (DIANA) and its two Innovation Hubs in Europe and the U.S., and grow the Alliance’s €1 billion Innovation Fund, to support the development of a protected transatlantic innovation community, including via cooperation on 6G technologies, testbeds and accelerators, and assessments of vulnerabilities and threats to 6G networks.
- Launch an annual process, perhaps via NDPP, to assess national progress in adopting new technologies. Select partner nations can be invited to participate voluntarily.
- Identify relevant NATO standards and system interoperability requirements for priority technologies.

- Seek to align around an agreed set of NATO principles for the use of AI in warfare. The U.S. Department of Defense principles are a start.
- Identify and integrate emerging and disruptive technology applications into NATO training, exercises, experimentation, plans and operations. Approve relevant NATO standards and system interoperability requirements for such technologies.
- Establish vibrant connections with industry partners and with EU institutions, such as the European Defense Agency (EDA), the European Commission's DG Innovation & Research, and CERT-EU.

VII. Conclusions

The foundation for NATO's next Strategic Concept should be renewed alliance cohesion rooted in a common commitment to shared values and effective decision-making procedures. Today, those values and procedures are under assault from external and internal challengers. To deal with the threats inherent in an age of disruption, strengthening Alliance cohesion needs to be the new Strategic Concept's number one priority.

NATO's 2010 Strategic Concept was functional for a dozen years despite the fact that the global environment changed dramatically after only four years. The primary reason was that its core tasks allowed for continued adaptation. A new Strategic Concept should recognize that NATO is now operating in more integrated ways that blur neat conceptual distinctions among the Alliance's core tasks. And each of the three existing core tasks has expanded to accommodate new challenges. Crisis management in the south, for instance, involves a big component of collective defense and reassurance for an ally such as Turkey. Collective defense in the east, on the other hand, requires more effective integration of partners such as Finland and Sweden, as well as the agility of crisis management to defeat hybrid warfare. Cooperative security measures can be used to deter Russia and address challenges coming from China. Unconventional challenges to the resilience of allied and partner societies can have cascading effects that could degrade conventional defense and deterrence measures, impair crisis management, and weaken cooperative security. To maintain the vitality of NATO's core tasks for the future, each of the three existing tasks needs to be updated and a fourth task of comprehensive resilience, should be added. Collective defense should be declared *primus inter pares* among the four.

NATO's ability to perform each of these four tasks, in turn, is affected by its ability to integrate its capacities across all domains: land, sea, air, space, and the digital domain, which encompasses, but goes beyond, cyber to include artificial intelligence, quantum, data dominance, and interoperability. The new Strategic Concept needs to establish mechanisms to further develop NATO's approach to multi-domain operations.

The Indo-Pacific and North Atlantic theaters are increasingly linked. NATO's ability to address traditional and unconventional threats in Europe is becoming intertwined with related challenges to Alliance security interests posed by China. NATO must identify and meet the security risks posed by China.

Over the next decade, the United States will therefore need to focus greater military attention on the Indo-Pacific. NATO must thus transform itself into a more balanced transatlantic partnership in which Europe assumes greater strategic responsibility while reinforcing the transatlantic link. Setting the goal of a rebalanced Alliance in the new Strategic Concept would move allies beyond contentious arguments over burden-sharing and embrace Europe's longstanding ambition to play a larger role in its own defense.

Allies cannot know the future. But they can future-proof the Alliance by making continual adaptation a built-in routine, a fundamental feature of NATO's business model. The next Strategic Concept has to establish that principle and the practices that will make it operational. The linchpin of effective anticipation

and adaptation is cohesion, grounded in a common commitment to NATO as an alliance of democracies, and in extensive connectivity, consultations and information-sharing among all allies, across many different levels and agencies.

* * *

One Plus Four: a NATO that is more cohesive, capable, balanced, and resilient—an Alliance prepared for the Age of Disruption.

Notes

¹ “Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation,” Adopted by Heads of State and Government in Lisbon, November 19, 2010, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120203_strategic-concept-2010-eng.pdf. For more on this period, see Daniel S. Hamilton and Kristina Spohr, eds., *Open Door: NATO and Euro-Atlantic Security After the Cold War* (Washington, DC: Johns Hopkins University School of Advanced International Studies, 2019); Sławomir Dębski & Daniel S. Hamilton, eds., *Europe Whole and Free: Vision and Reality* (Washington, DC/Warsaw Poland: Transatlantic Leadership Network/Polish Institute of International Affairs PISM).

² See Lt. Gen. (Ret.) Ben Hodges, Janusz Bugajski, Col. (Ret.) Ray Wojcik, Carsten Schmiedl, “One Flank, One Threat, One Presence: A Strategy for NATO’s Eastern Flank,” Center for European Policy Analysis, May 2020, https://cepa.org/cepa_files/2020-CEPA-report-one_flank_one_threat_one_presence.pdf; Michael Kofman, “It’s Time to Talk About A2/AD: Rethinking the Russian Military Challenge,” War on the Rocks, September 5, 2019, <https://warontherocks.com/2019/09/its-time-to-talk-about-a2-ad-rethinking-the-russian-military-challenge/>.

³ See Dmitry (Dima) Adamsky, “From Moscow with coercion: Russian deterrence theory and strategic culture,” *Journal of Strategic Studies*, Vol. 18, 2018, Issues 1-2, <https://www.tandfonline.com/doi/abs/10.1080/01402390.2017.1347872>; Dmitry (Dima) Adamsky, “Cross-Doman Coercion: The Current Russian Art of Strategy,” *Proliferation Papers*, French Institute of International Affairs IFRI, November 2015, <https://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf>.

⁴ See Paul Bernstein, “Rethinking Deterrence and Assurance,” NATO Defense College Conference Report, September 2013.

⁵ See Tim Sweijs, Rob Johnson and Martijn Kitzen, “Conclusion: Assessing change and continuity in the character of war,” in Rob Johnson, Martijn Kitzen and Tim Sweijs, eds., *The Conduct of War in the 21st Century: Kinetic, Connected and Synthetic* (London: Routledge, 2021), https://tandfbis.s3-us-west-2.amazonaws.com/rt-files/docs/Open+Access+Chapters/9780367515249_oachapter19.pdf; Benedikt Franke, “Are We Witnessing a “Zeitenwende” in European Security?” in Daniel S. Hamilton, Gregor Kirchhof, and Andreas Rödder, eds., *Paradigm Lost? The European Union and the Challenges of a New World* (Washington, DC: Johns Hopkins SAIS/Brookings Institution Press/Mohr Siebeck, 2021), <https://sais.jhu.edu/kissinger/paradigm-lost-the-european-union-and-the-challenges-of-a-new-world>.

⁶ See Richard L. Kugler and Hans Binnendijk, *Should NATO Write a New Strategic Concept?* National Defense University Press, 2008.

⁷ “NATO 2030: United for a New Era,” Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General, November 25, 2020, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf.

⁸ The North Atlantic Treaty, Washington, D.C., 4 April 1949, https://www.nato.int/cps/en/natohq/official_texts_17120.htm

⁹ Article II, in *Ibid.*

¹⁰ Celeste A. Wallander, “NATO’s Enemies Within: How Democratic Decline Could Destroy the Alliance,” *Foreign Affairs*, May/June 2018, <https://www.foreignaffairs.com/articles/2018-06-14/natos-enemies-within>; NATO 2030.

¹¹ See Torrey Taussig and Jonathan Katz, “An Inconvenient Truth: Addressing Democratic Backsliding Within NATO,” Brookings Institution, July 10, 2018, <https://www.brookings.edu/blog/order-from-chaos/2018/07/10/an-inconvenient-truth-addressing-democratic-backsliding-within-nato/>.

¹² NATO 2030, p. 24.

¹³ See Hans Binnendijk and Julian Lindley-French, “Prioritize NATO’s core task: collective defense,” *Defense News*, November 23, 2021.

¹⁴ Russia’s major tactical nuclear weapons arsenal is considered to be a hedge against the perceived superiority of NATO’s conventional forces, in order to “level the playing field in the event that Russia starts losing a major continental war.” The doctrine was officially endorsed by Russian President Vladimir Putin in 2020 by including a non-nuclear attack as a potential trigger for Russian nuclear retaliation. These developments, combined with the ongoing modernization of Russia’s nuclear forces since 2011, the increased air patrols of nuclear-capable planes, and military exercises which include nuclear weapons, have further fueled concerns about Russia’s nuclear threat. See Tim Sweijs, Paul van Hooft, and Philip Geurts, “Comparing Deterrence in Europe and Asia: Strengthening deterrence against nuclear, conventional, and hybrid threats: Strengths, weaknesses, and insights for US allies in Europe and Asia,” Hague Centre for Strategic Studies, January 2022, <https://hcss.nl/wp-content/uploads/2022/01/06-The-State-of-Deterrence-in-Europe-and-Asia-HCSS-2022-1.pdf>, pp. 11-12; Also Kristin Ven Bruusgaard, “Russian nuclear strategy and conventional inferiority,” *Journal of Strategic Studies*, Vol. 44, 2021, Issue 1, <https://www.tandfonline.com/doi/full/10.1080/01402390.2020.1818070>; Edward Lucas and A. Wess Mitchell, et. al, “Central European Security After Crimea: The Case for Strengthening NATO’s Eastern Defenses,” Center for European Policy Analysis, March 25, 2014.

¹⁵ Bernstein.

¹⁶ This separate product has been prepared by Heinrich Brauss.

¹⁷ The 4x30 Readiness Initiative would make 30 battalions, 30 air squadrons, and 30 combat ships available in theater within 30 days, and based on these forces to develop a number of army brigades, air wings and maritime task groups at very high readiness.

¹⁸ A full U.S. Aircraft Carrier Strike Group was placed under NATO command for the first time since the end of the Cold War.

¹⁹ For more, see Sweijs, van Hooft, and Geurts.

²⁰ NATO 2030, pp. 45–46.

²¹ North Atlantic Council, “Brussels Summit Communique,” North Atlantic Treaty Organization, June 14, 2021, https://www.nato.int/cps/en/natohq/news_185000.htm.

²² These are: Denmark, Estonia, the Netherlands, the United Kingdom, and the United States. See Wiesław Goździewicz, “Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA),” *Cyber Defense*, November 11, 2019, [https:// www.cyberdefensemagazine.com/sovereign-cyber/](https://www.cyberdefensemagazine.com/sovereign-cyber/).

²³ This section draws on Jason Blessing, “Fail-Deadly, Fail-Safe, and Safe-to-Fail: The Strategic Necessity of Resilience in the Cyber Domain,” in Jason Blessing, Katherine Kjellström Elgin, Nele Marianne Ewers-Peters, and Raket Tiderman, eds., *NATO 2030: Towards a New Strategic Concept and Beyond* (Washington, DC: Johns Hopkins SAIS, 2021), <https://sais.jhu.edu/sites/default/files/NATO2030AndBeyondAccessibleVersion.pdf#page=271>.

²⁴ Drawing on Blessing, ‘safe-to-fail’ implementation could include the following measures:

- Develop and use common defensive metrics, defensive capability standards, and frameworks for reporting major cyber incidents. In this regard, formalizing the ‘information broker’ role currently being played by NATO’s Emerging Security Challenges Division (ESCD) vis-à-vis the Cyber Defense Pledge would be a significant initiative. NATO should formalize the ways in which ESCD collects, processes, and disseminates data on allied cyber defense, deterrence, and resilience.
- Leverage consultation mechanisms and processes derived from Article 4, which can transfer crucial skills and expertise among allies, and help build domestic cyber exercise staging capabilities in smaller allies. One such avenue for greater coordination, consultation, and mutual aid would be to expand the scope of NATO’s Computer Incident Response Capability (NCIRC) so that teams are available outside of crisis situations, much like its Resilience Advisory Support Teams. While NATO’s Communications and Information Agency (NCIA) does offer advisory teams, these teams are not formalized like emergency response teams under NCIRC. Should NCIRC be expanded to include formal advisory teams, member states could request these teams as an observing or assessing party for bilateral and multilateral “hunt forward” missions. This would facilitate NATO’s broader goals of situational awareness, threat intelligence sharing, and vulnerability assessment.
- Expand the NATO Industry Cyber Partnership on a case-by-case basis to include actors in like-minded non-NATO nations. Companies in Enhanced Opportunity Partner nations, like Ericsson in Sweden and Nokia in Finland, represent natural candidates for expansion. The Alliance should also look to broader Interoperability Platform Partners with vibrant telecommunications sectors like South Korea and Japan, home to Samsung and Sony, respectively. Expanding the NATO Industry Cyber Partnership on a case-by-case basis can help build greater resilience into digital supply chains and spur the development of viable alternatives to digital infrastructures and products from companies in countries like China.
- Task a new NATO Office of Net Assessment (discussed elsewhere in this report), to analyze organizational strengths and weaknesses vis-à-vis adversaries in the cyber domain. This should include developing metrics for assessing Allied operational success in cyberspace, and horizon-scanning for emerging cyber technologies that could affect Alliance security.
- Develop a normative ‘code of conduct’ for states operating in the cyber domain that focuses on behavior and standardization. This would be a critical first step in determining when and how to respond to the cumulative costs of below-threshold cyber incidents over time. It could be the basis for promoting best practices for cyber hygiene and for outlining responsible applications for artificial intelligence and emerging technologies like quantum computing in military contexts.
- Adopt risk minimization strategies, including continuous threat monitoring and the development of continuity-of-operations plans for cyber crises. Involve the private sector. Continuity plans are particularly crucial for ensuring that adversaries gain fewer and shorter-term payoffs from disruptions like ransomware attacks or sophisticated wiper worms that delete information.

²⁵ Blessing; Aaron F. Brantly, “The Cyber Deterrence Problem,” in T. Minarik, R. Jakschis, and L. Lindström, eds., “2018 10th International Conference on Cyber Conflict: CyCon X: Maximising Effects” (Tallinn, Estonia: NATO CCD COE Publications, 2018), p. 44; Jacquelyn Schneider, “Deterrence in and through Cyberspace,” in Erik Gartzke and John Lindsay, eds., *Cross-Domain Deterrence: Strategy in an Era of Complexity*, edited by (Oxford: Oxford University Press, 2019), p. 111.

²⁶ Blessing; Lucas Kello, *The Virtual Weapon and International Order* (New Haven, CT: Yale University Press, 2017), p. 62.

²⁷ Blessing; NATO Cooperative Cyber Defence Centre of Excellence, “Exercises” 2021, <https://ccdcoc.org/exercises/>.

²⁸ For more, see NATO Cooperative Cyber Defence Centre of Excellence, “European Union Equipping Itself against Cyber Attacks with the Help of Cyber Diplomacy Toolbox,” <https://ccdcoc.org/in-cyber-articles/european-union-equipping-itself-against-cyber-attacks-with-the-help-of-cyber-diplomacy-toolbox/>.

²⁹ See Hans Binnendijk and David Gompert, “Decisive Response: A New Nuclear Strategy for NATO,” *Survival*, October-November 2019.

³⁰ See Tim Swejjs & Frans Osinga, “Maintaining NATO’s Technological Edge,” Whitehall Papers, 95:1 (2019), pp. 104-118, <https://hcss.nl/wp-content/uploads/2022/01/VIII-Maintaining-NATO-s-Technological-Edge-1.pdf>.

³¹ Only 14 of NATO’s 30 members participated in the Unified Protector operation in Libya, and NATO depended on Sweden and four Arab partner states for military and political support. When operational imperatives took precedence over resolving or addressing different national objectives, the Alliance was criticized for having gone beyond its mandate, and its credibility suffered. See Rebecca R. Moore, “Benefit of Burden? NATO-led Military Missions and Western Cohesion,” in Sten Rynning, ed., *War Time: Temporality and the Decline of Western Military Power* (Washington: Brookings Institution Press, 2021), pp. 70-71.

³² French Ministry for Europe and Foreign Affairs, “France’s actions in the Sahel,” <https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/terrorism-france-s-international-action/article/france-s-action-in-the-sahel>.

³³ Jen Judson, “Outgoing US Army Europe commander pushes for ‘Military Schengen Zone,’” *Defense News*, July 28, 2017, <https://www.defensenews.com/smr/european-balance-of-power/2017/07/28/outgoing-us-army-europe-commander-pushes-for-military-schengen-zone/>; Karlijn Jans, Rachel Rizzo, “Why Europe Needs a ‘Military Schengen Zone,’” *World Politics Review*, August 22, 2017, <https://www.worldpoliticsreview.com/articles/22991/why-europe-needs-a-military-schengen-zone>.

³⁴ European External Action Service, “Climate Change and Defence Roadmap,” November 9, 2020, <https://data.consilium.europa.eu/doc/document/ST-12741-2020-INIT/en/pdf>; Office of the Under Secretary of Defense for Acquisition and Sustainment, U.S. Department of Defense, “Report on Effects of a Changing Climate to the Department of Defense,” January 2019, https://partner-mco-archive.s3.amazonaws.com/client_files/1547826612.pdf. For more, see Oliver Belcher, Patrick Bigger, Ben Neimark, Cara Kennelly, “Hidden carbon costs of the ‘everywhere war’: Logistics, geopolitical ecology, and the carbon boot-print of the US military,” *Transactions of the Institute of British Geographers*, June 19, 2019, <https://rgs-ibg.onlinelibrary.wiley.com/doi/10.1111/tran.12319>; Neta C. Crawford, “Pentagon Fuel Use, Climate Change, and the Costs of War,” Boston University, November 13, 2019, <https://watson.brown.edu/costsofwar/files/cow/imce/papers/Pentagon%20Fuel%20Use%2C%20Climate%20Change%20and%20the%20Costs%20>

[0of%20War%20Revised%20November%202019%20Crawford.pdf](#); Joseph Bodnar, “NATO Has a Role to Play in Fighting Climate Change,” *The National Interest*, December 8, 2020, <https://nationalinterest.org/blog/buzz/nato-has-role-play-fighting-climate-change-174051>.

³⁵ Jacob Wallace, “Defense Experts Call on Biden to Ready Military for Climate Change,” *Scientific American*, December 16, 2020, <https://www.scientificamerican.com/article/defense-experts-call-on-biden-to-ready-military-for-climate-change/>.

³⁶ For more, see Daniel S. Hamilton, ed., *Forward Resilience: Protecting Society In An Interconnected World* (Washington, DC: Johns Hopkins University School of Advanced International Studies, 2017), <https://transatlanticrelations.org/publications/forward-resilience-protecting-society-in-an-interconnected-world/>.

³⁷ See Hans Binnendijk and Alexander Vershbow, “Needed: A transatlantic agreement on European Strategic Autonomy,” *Defense News*, October 10, 2021.

³⁸ Shirley Zhao, Scott Moritz, and Thomas Seal, “Forget 5G, the U.S. and China Are Already Fighting for 6G Dominance,” *Bloomberg*, February 8, 2021, <https://www.bloomberg.com/news/features/2021-02-08/forget-5g-the-u-s-and-china-are-already-fighting-for-6g-dominance>; “6G: The Next Hyper-Connected Experience for All,” Samsung Research, https://cdn.codeground.org/nsr/downloads/researchareas/20201201_6G_Vision_web.pdf; David Sacks, “China’s Huawei Is Winning the 5G Race. Here’s What the United States Should Do To Respond,” Council on Foreign Relations, March 29, 2021, <https://www.cfr.org/blog/china-huawei-5g>.

³⁹ Joris Teer, Tim Sweijs, Paul van Hooft, Lotje Boswinkel, Juliëtte Eijkelkamp, Jack Thompson, “China’s Military Rise and the Implications for European Security,” Hague Centre for Security Studies, November 2021, <https://hcss.nl/report/chinas-military-rise/>.

⁴⁰ Laura Rosenberger and Lindsey Gorman, “How Democracies Can Win the Information Contest,” *Washington Quarterly*, June 16, 2020.

⁴¹ See Hans Binnendijk, Sarah Kirchberger, et al., “The China Plan,” Atlantic Council, March 2021, pp. 72-87.

⁴² “Brussels Summit Communique,” June 14, 2021, https://www.nato.int/cps/en/natohq/news_185000.htm.

⁴³ Lindsay Gorman, “NATO Should Count Spending on Secure 5G Towards Its 2% Goals,” *Defense One*, December 3, 2019, <https://www.defenseone.com/ideas/2019/12/nato-should-count-secure-5g-spending-towards-its-2-goals/161648/>.

⁴⁴ Tim O’Reilly, “Gradually, then suddenly,” January 10, 2019, O’Reilly.com, <https://www.oreilly.com/radar/gradually-then-suddenly/>;

⁴⁵ Alison E. Berman and Jason Dorrier, “Technology Feels Like It’s Accelerating — Because It Actually Is,” Singularity Hub, March 22, 2016, <https://singularityhub.com/2016/03/22/technology-feels-like-its-accelerating-because-it-actually-is/#sm.00002biczi7sed8811ggbn516nd0i>

⁴⁶ This section draws on Sweijs & Osinga.

⁴⁷ James Vincent, “Putin Says the Nation That Leads in AI ‘Will Be the Ruler of the World’,” *The Verge*, September 4, 2017, <https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world>.

⁴⁸ Cited in James Kynge, “China’s high-tech rise sharpens rivalry with the US,” *Financial Times*, January 18, 2022; see also Sweijs and Osinga.

⁴⁹ For more, see Frank Hoffman, “Defeat Mechanisms in Modern Warfare,” *Parameters* 51, no. 4 (November 17, 2021); <https://hcss.nl/wp-content/uploads/2022/01/06-The-State-of-Deterrence-in-Europe-and-Asia-HCSS-2022-1.pdf>

⁵⁰ NATO, “Emerging and disruptive technologies,” October 21, 2021, https://www.nato.int/cps/en/natohq/topics_184303.htm.