Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

The Case for a Comprehensive Approach 2.0:

How NATO Can Combat Chinese and Russian Political Warfare

Kathleen J. McInnis and Clementine G. Starling

The **Scowcroft Center for Strategy and Security** works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

The Scowcroft Center's Transatlantic Security Initiative brings together top policymakers, government and military officials, business leaders, and experts from Europe and North America to share insights, strengthen cooperation, and develop innovative approaches to the key challenges facing NATO and the transatlantic community.
This publication was produced in partnership with the Swiss Federal Department of Foreign Affairs in close cooperation with the Permanent Mission of Switzerland to NATO.

Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

The Case for a Comprehensive Approach 2.0:

How NATO Can Combat Chinese and Russian Political Warfare

Kathleen J. McInnis and Clementine G. Starling

ISBN-13: 978-1-61977-182-6

June 2021

Contents

Executive Summary

French President Emmanuel Macron initiated a furious international political debate when he stated in 2019 that NATO is becoming brain-dead.[1] Scholars and practitioners on both sides of the Atlantic quickly, and rightly, pushed back by noting that the North Atlantic Alliance is, and will remain for the foreseeable future, the most important international military organization in modern human history. Indeed, the Alliance has proven remarkably resilient and has transformed itself and its mission set to match an evolving strategic environment, despite decades worth of pronouncements that NATO is in crisis or on the verge of irrelevance. Further, the international political landscape has changed in profound ways since 2019, particularly as a result of the COVID-19 pandemic. It is tempting, therefore, to conclude that Macron's remark is but one of many premature announcements of NATO's death.

Yet in at least one important respect, Macron's statement hit an uncomfortable mark. Namely, for all the Alliance's work on deterrence, crisis management, and so on, it is still caught flat-footed when it comes to some of the most important geostrategic and geo-economic questions facing its member states. China and Russia are increasingly using the nonmilitary tools of political warfare—a suite of tactics and techniques designed to influence a state or other institution's behavior short of the use of military force—to achieve their strategic objectives against NATO and its member states. While their tactics vary, the fact that they are waging political warfare campaigns in nations across the Alliance and its partners is hardly in doubt. Viewed in that light, relatively common commercial transactions like the sale of Germany's KUKA Robotics to Chinese owners, or decisions to allow Huawei to build 5G telecommunications infrastructure suddenly take on urgent strategic importance. Thomas de Maizière, a former German minister of defense, and A. Wess Mitchell, a former US assistant secretary of state for European and Eurasian affairs, recently argued that "the scope for NATO to do more on China is considerable—and underdeveloped."[2] Likewise, Russian disinformation operations—some of which have actively and powerfully spread myths about the COVID-19 vaccine—take advantage of cleavages within and between democratic societies.[3] With COVID-19, disinformation and falsehoods have been weaponized to create confusion, panic, and, in some cases, undermine public trust in government and institutions.[4] In essence, some of the most profound questions with security dimensions facing NATO allies and partners today are rooted in nonmilitary sectors.

To be sure, NATO has a demonstrated track record of responding to crises commanding and controlling multilateral military operations and activities.[5] NATO allies operate together in Afghanistan, Kosovo, in the Mediterranean Sea, and elsewhere,[6] while training and exercising regularly for kinetic scenarios and to improve preparedness, deterrence, and interoperability. Still, as Macron went on to note in 2019, "strategically and politically, we need to recognise [sic] that we have a problem."[7] It is this area of NATO's strategic and political liability—identifying and countering authoritarian political warfare—that this report addresses.

Arguably, NATO has yet to fully utilize its mandate in Article 2 of the 1949 Washington Treaty to help its allies and partners manage and mitigate the effects of political warfare. Article 2 states:

> The Parties will contribute toward the further development of peaceful and friendly international relations by strengthening their free institutions, by bringing about a better understanding of the principles upon which these institutions are founded, and by promoting conditions of stability and well-being. They will seek to eliminate conflict in

1 *Economist*, "Emmanuel Macron warns Europe: NATO is becoming brain-dead," November 7, 2019, https://www.economist.com/europe/2019/11/07/emmanuel-macron-warns-europe-nato-is-becoming-brain-dead.

2 Thomas de Maizière and A. Wess Mitchell, "NATO Needs to Deal With China Head-On," *Foreign Policy*, February 23, 2021, https://foreignpolicy.com/2021/02/23/nato-china-brussels-summit-biden-europe-alliance/.

3 Peter W. Singer and Emerson T Brooking, *LikeWar: The Weaponization of Social Media* (Eamon Dolan/Houghton Mifflin Harcourt, 2018).

4 Luiza Bandeira et al., *Weaponized: How rumors about COVID-19's origins led to a narrative arms race*, *Digital Forensic Research Lab*, *Atlantic Council*, February 2021, https://www.atlanticcouncil.org/wp-content/uploads/2021/02/Weaponized-How-rumors-about-COVID-19s-origins-led-to-a-narrative-arms-race.pdf.

5 https://www.belfercenter.org/publication/assessing-value-nato-alliance John Kriendler, "NATO Crisis Management: Cooperation with PfP Partners and Other International Organizations," *Connections* 3 (4) (December 2004): 59-68, https://www.jstor.org/stable/26323065?seq=1#metadata_info_tab_contents.

6 "Operations and missions: past and present," North Atlantic Treaty Organization, last updated April 22, 2021, https://www.nato.int/cps/en/natohq/topics_52060.htm.

7 France 24, "France's Macron says NATO experiencing 'brain death,'" November 7, 2019, https://www.france24.com/en/20191107-france-s-macron-says-nato-experiencing-brain-death.

Mr. Dean Acheson (Minister of Foreign Affairs) signs the NATO Treaty for the United States. *Source:* NATO/flickr

their international economic policies and will encourage economic collaboration between any or all of them.

While Article 2 is often viewed as simply a statement of NATO's values, viewed through the lens of authoritarian political warfare it becomes an important mandate and an opening to more comprehensively counter threats to transatlantic civil institutions, both multilateral and domestic. This is because the principles of Article 2 that NATO allies have agreed to uphold are the very elements at risk from Russian and Chinese political warfare. As a result, NATO should reinvigorate Article 2 and use this mantle to uphold the values espoused and add teeth to allied counter-political warfare responses.

But how might Article 2 be translated into action? Through operations in Afghanistan and elsewhere, NATO possesses hard-won, relevant operational experience developing and applying multi-stakeholder solutions to complex security challenges. NATO's Comprehensive Approach program can serve as a model for a comparable multi-stakeholder process to counter political warfare at the strategic level, a construct that this paper calls for by way of a "Comprehensive Approach 2.0." A Comprehensive Approach 2.0 would help operationalize a NATO Article 2 agenda, thereby empowering NATO allies and partners to take a new approach to political warfare.

While tensions flare up at times, NATO's success has been its flexibility and adaptability to meet both emerging security challenges as well as the political demands of its members and partners.[8] Now is a critical time, once again, for NATO to answer the call, in this instance by embracing and acting upon its important role in countering nonmilitary coercion strategies. Traditional and nontraditional security, economics, trade, diplomacy, and emerging technologies can no longer be considered discretely, nor can the interrelationships be ignored to satisfy preferences for bureaucratic stovepiping. As a matter of urgency, NATO must help its member states and partners grapple with how to think about authoritarian coercion strategies and develop holistic responses to them. Failure to do so risks the possibility of the international system, upon which NATO allies rely, being hollowed out from within—commercially, technologically, socially, or otherwise—and allies being unable to either defend themselves or contribute to the common defense. Responding to political warfare is arguably the most important geopolitical challenge of our time. NATO can, and must, help address it.

8 Wallace J. Thies, *Why NATO Endures* (Cambridge, UK: Cambridge University Press, 2009).

Introduction: The Wasp and the Orb Spider

Mother Nature can be a curious steward of the animal kingdom. Take, for instance, the *Hymenoepimecis argyraphaga*, a wasp in Costa Rica that lays its eggs in the bellies of orb spiders.[9] After preying on its host for several weeks, hatched larvae then inject chemicals into the orb spider. The spider subsequently begins building a web that is unlike anything it would otherwise create; this is because the new web is not designed for the spider, but instead for the parasitic larvae.[10] In other words, the poor spider becomes a "zombie" coopted from within, that mindlessly turns its own web into the home of a much more dangerous creature.

While the fate of the Costa Rican orb spider is disturbing, it provides a powerful metaphor through which we can grapple with present challenges in the international strategic environment, namely the fate of the liberal international order that has been a bedrock of international stability for decades. In particular, what if transatlantic norms and institutions have become the orb spider, and authoritarian regimes in Beijing and Moscow the wasp? What if these actors are finding ways to coopt transatlantic political and economic instruments that have been essential elements of the liberal order, to utilize those institutions against transatlantic actors? In other words, what if Russia and China are actively waging political warfare against the international institutions of cooperation underpinned by liberal democratic values? As a recent report from a task force co-chaired by Eric Edelman and Avril Haines put it, "The United States and other liberal democracies face a persistent asymmetric threat from authoritarian challengers who aim to reshape the global order in their favor.... To date, democracies have been slow to adapt to this contest, allowing autocrats to seize the initiative by taking advantage of the openness of liberal systems."[11]

Source: Benjamin Balazs/Pixabay

One of the dominant challenges of contemporary statecraft is the "cylinders of excellence" problem: the stovepiping of key policies, activities, and even worldviews by bureaucracies that, practically speaking, limits the ability of nations to design and implement holistic strategies to address current and emerging threats.[12] To date, NATO allies and partners have generally muddled through on countering political warfare with discrete efforts to identify and

9 Mary Bates, "Meet 5 'zombie' parasites that mind-control their hosts," *National Geographic,* October 22, 2018, https://www.nationalgeographic.com/news/2018/10/141031-zombies-parasites-animals-science-halloween/#close.

10 William G. Eberhard, "Under the Influence: Webs and Building Behavior of *Plesiometa Argyra* (Araneae, Tetragnathidae) When Parasitized by Hymenopimecis Argyraphaga (Hymenopetera, Ichneumonidaae)," *Journal of Arachnology* 29 (3) (December 2001): 354-366, https://repository.si.edu/bitstream/handle/10088/1507/William_Eberhard.pdf.

11 Jessica Brandt et al., *Linking Values and Strategy: How Democracies Can Offset Autocratic Advances*, *Alliance for Securing Democracy, German Marshall Fund of the United States*, 3, October 30, 2020, https://securingdemocracy.gmfus.org/linking-values-and-strategy/.

12 These problems are most thoroughly explored in literature on US statecraft, although the authors' experience and conversations with actors in other governments suggests that the US situation is far from unique. See, for example: Joseph R. Cerami and Jeffrey A. Engel, *Rethinking Leadership and "Whole of Government" National Security Reform: Problems, Progress, and Prospects* (Strategic Studies Institute, 2010); Gordon Lederman, "National Security Reform for the Twenty-first Century: A New National Security Act and Reflections on Legislation's Role in Organizational Change," *Journal of National Security Law and Policy* 3: 363, https://jnslp.com/wp-content/uploads/2010/08/08_Lederman-Master-12-14-09.pdf; Project on National Security Reform, *Forging a New Shield*, November 2008, https://apps.dtic.mil/dtic/tr/fulltext/u2/a491826.pdf; US Commission on National Security in the 21st Century, *Road Map for National Security: Imperative for Change: The Phase III Report of the U.S. Commission on National Security/21st Century*, January 31, 2001, https://www.hsdl.org/?view&did=2079; Sverrir Steinsson, "NATO's Comprehensive Approach in Afghanistan: Origins, Development, and Outcome," *E-International Relations*, July 26, 2015, https://www.e-ir.info/2015/07/26/natos-comprehensive-approach-in-afghanistan-origins-development-and-outcome/; Cedric de Coning et al., *Norway's Whole-of-Government Approach and its Engagement with Afghanistan*, *Norwegian Institute of International Affairs*, 2009, https://www.oecd.org/dac/evaluation/dcdndep/47107380.pdf; Claudia Berchtold et al., "Barriers and Facilitators in Interorganizational Response: Identifying Examples Across Europe," *International Journal of Disaster Risk Science* 11 (February 17, 2020): 46-58, https://link.springer.com/article/10.1007/s13753-020-00249-y.

Defining 'Authoritarian Political Warfare'

"Political warfare" involves a set of tactics and techniques designed to influence a state or other institution's behavior short of the use of military force. "Authoritarian" refers to a regime type in which power is concentrated in a leader or elite. Although, historically speaking, political warfare is not exclusively utilized by authoritarian regimes, "authoritarian political warfare" is political coercion conducted by authoritarian states. One key distinguishing feature of contemporary political warfare campaigns of authoritarian actors, such as China and Russia, is the relative ease with which they are able to able to develop and prosecute whole-of-government (if not whole-of-society) political warfare campaigns.[1]

1 See also: Brandt et al., *Linking Values and Strategy*, 3: "Illiberal regimes use a wide range of tools across the political, economic, technological, and information domains to undermine democratic institutions and alliances, prevent criticism of their own regimes and governance systems, and establish norms and standards favorable to autocratic rule."

counter disinformation, improve cyber defenses, and sanction Russia and other actors in response to below-threshold attacks. Yet, these counterefforts have been mixed in terms of effectiveness, scope of response, and the actors involved. China and Russia's authoritarian political warfare campaigns are neither siloed, piecemeal, nor singular in nature. Accordingly, these challenges demand a much more robust and comprehensive approach from NATO allies and—crucially—they require a reimagined response that better incorporates external partners (including partner states, multilateral organizations, civil society, and private sector actors). Ultimately, political warfare is a matter that NATO allies and partners must attend to with more urgency and intentionality lest they be at risk of becoming the orb spider: having mindlessly, inadvertently contributed to the design of a world that is no longer compatible with transatlantic security and the democratic values and freedoms that are central to our way of life.

This paper argues that NATO has both a designated strategic role to play due to its mandate in the 1949 Washington Treaty, and an operational-level toolkit to utilize, when it comes to developing and implementing an urgently needed Comprehensive Approach to countering authoritarian political warfare.[13] Political warfare can be difficult to pinpoint, as both malign and non-malign activities can be blended together as part of an ultimately coercive influence campaign. Political warfare is, therefore, most readily discerned at the strategic level, where a clearer picture of overall behaviors and trends can be aggregated and analyzed—a task that NATO headquarters is well positioned to take on. NATO convenes not only heads of state and government, military leaders, and ministers of defense, but also ministers of foreign affairs and others civilian leaders on a regular basis. With multiple divisions and directorates, NATO headquarters has the ability to engage with outside actors, including nongovernment actors and civil society. NATO has the platform to further dialogue and coordinate action among multiple stakeholders in a way that is necessary to spur cross-national and multinational counter-political warfare efforts in the transatlantic community. For NATO to get a handle on countering political warfare, it can also benefit from its various partnership frameworks to learn from and employ the capabilities of partner nations and nongovernment actors. Partners like Finland and Sweden have often led the way on countering political warfare nationally, while partners like Georgia and Ukraine have much experience to share. Civil society and commercial actors also have a part to play in any proposed counterstrategies and in developing potential solutions. A whole-of-system approach is required to combat whole-of-system attacks. NATO is well positioned to help build that holistic approach and it should do so with greater urgency.

Further, NATO and its partners might usefully build off—and improve upon—the hard-won experiences developing civil-military approaches to crisis management operations in the Balkans, Iraq, and Afghanistan, in order to develop a Comprehensive Approach 2.0 agenda that is nested under Article 2 of the Washington Treaty. Broadly speaking, the Comprehensive Approach represented an important innovation in NATO's processes for tackling complex challenges that require civilian and military stakeholder input in strategy development and execution. While it has, to date, been largely focused on tactical and operational-level problems, the process itself could be usefully adapted to the strategic-level challenges that authoritarian political warfare presents. Toward that end, two key areas

13 This paper uses the terms political warfare, authoritarian political warfare, coercion, and authoritarian coercion interchangeably. The key difference this paper highlights is the distinction between hybrid and political warfare/coercion. Parsing these terms from the overall conceptual umbrella of "hybrid warfare" enables an analysis of what, specifically, NATO might do to counter the political warfare components of hybrid warfare.

NATO's Comprehensive Approach

This paper proposes NATO adapt best practices from its Comprehensive Approach model used in Afghanistan and apply it, with amendments, to meet today's challenge of countering political warfare. NATO's initial Comprehensive Approach was not without flaws, but it can still serve as a useful organizing principle.

NATO led the United Nations (UN)-mandated International Security Assistance Force (ISAF) in Afghanistan from August 2003 to December 2014, and deployed forces under the non-combat Resolute Support Mission (RSM), which had been training, advising, and assisting Afghan security forces and institutions since January 2015;[1] those troops started being withdrawn from Afghanistan as of May 1, 2021.

As the NATO campaign in Afghanistan progressed from 2003 onward, it became clear that military operations alone could not create lasting stability and security on the ground. And while civilian actors were responsible for important development and governance capacity building work, those civil efforts were often conducted apart from military efforts. This led to fragmentation of national and international efforts and a general sense that the whole of the international community's support for Afghanistan was less than the sum of its parts. A broader, better coordinated civil-military effort was required.

In 2008, NATO established the Comprehensive Approach in order to facilitate better synchronization and coordination of civilian and military activities in Afghanistan. In 2017, the Comprehensive Approach work plan was updated to enhance NATO's civil-military coordination for crisis management operations, and to help NATO allies better integrate civilian advice and perspectives into broader defense and military planning. Other activities under the Comprehensive Approach framework include sharing lessons learned, promoting civil-military training, coordination with other international organizations such as the European Union and the United Nations, and sharing communications strategies with other international actors as appropriate. Much of the work being conducted under the Comprehensive Approach framework was arguably targeted toward NATO's more operational-level activities.

This report ultimately argues that the extant Comprehensive Approach provides a useful starting point for NATO to begin better addressing the more strategic-level challenges presented by authoritarian political warfare. By drawing from, and building upon, its civil-military consultation experiences and organizing them into a "Comprehensive Approach 2.0" work stream under the auspices of Article 2 of the Washington Treaty, NATO could serve as a powerful catalyst for allies and partners to develop shared approaches to contending with the growing threats posed by authoritarian political warfare on both sides of the Atlantic and beyond.[2]

1 "NATO and Afghanistan," North Atlantic Treaty Organization, accessed May 26, 2021, https://www.nato.int/cps/en/natohq/topics_8189.htm.

2 "A 'Comprehensive Approach' to Crises," North Atlantic Treaty Organization, last updated June 26, 2018, https://www.nato.int/cps/en/natolive/topics_51633.htm.

that NATO might focus on as part of that Comprehensive Approach 2.0 agenda—countering disinformation and economic coercion—are evaluated in this paper, both in terms of understanding what NATO allies and partners are currently doing in these areas and assessing what more ought to be done.[14] The paper concludes with design principles for NATO to consider in order to build a Comprehensive Approach 2.0 and initiate an agenda. Ultimately, NATO allies and partners can do an enormous strategic service by bringing greater coherence to existing counter-coercion activities and serving as a catalyst and enabler for a broader, holistic approach to countering political warfare. An Alliance-only approach is insufficient to counter authoritarian political warfare; partners are key. By including partners and other key stakeholders, a stronger and more comprehensive global approach can be built.

14 While cybersecurity and defense is a critical component of any counter-political warfare strategy, this report does not focus on this issue. For more information on NATO's cyber defense policy, see: "Cyber defence," North Atlantic Treaty Organization, last updated April 12, 2021, https://www.nato.int/cyberdefence/. For information on cyber threats NATO faces from Russia, China, and other actors, see: James Black and Alice Lynch, "Cyber Threats to NATO from a Multi-Domain Perspective" in *Cyber Threats and NATO 2030: Horizon Scanning and Analysis* [NATO Cooperative Cyber Defense Centre of Excellence (CCDOE), January 12, 2021], https://www.rand.org/pubs/external_publications/EP68434.html. For ideas on potential NATO responses to cyber threats, see Franklin D. Kramer, Lauren M. Speranza, and Conor Rodihan, "NATO needs continuous responses in cyberspace," *New Atlanticist*, Atlantic Council, December 9, 2020 https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-continuous-responses-in-cyberspace/.

Political versus Hybrid Warfare?

In recent years, a growing consensus amongst scholars and practitioners has emerged that both Russia and China are utilizing a wide range of overt and covert coercive tools to achieve their objectives against NATO allies and partners.[15] The most commonly applied framing of these activities is that of "hybrid threats," which, according to NATO, is the utilization of "military and non-military as well as covert and overt means, including disinformation, cyberattacks, economic pressure, deployment of irregular armed groups and use of regular forces."[16]

Hybrid warfare generally assumes that military instruments of national power will be utilized in some form or fashion.[17] As Frank G. Hoffman maintains, "instead of separate challengers with fundamentally different approaches (conventional, irregular, or terrorist), we can expect to face competitors who will employ all forms of war and tactics, perhaps simultaneously."[18]

By contrast, "political warfare" refers to the exercise of actions short of war that are part of a coercive statecraft strategy. The phrase was coined by George Kennan who wrote:

> "Political warfare is the logical application of Clausewitz's doctrine in time of peace. In broadest definition, political warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures… and 'white' propaganda to such covert operations as clandestine support of 'friendly' foreign elements, 'black' psychological warfare and even encouragement of underground resistance in hostile states."[19]

The concept of conducting synchronized activities short of overt warfare to achieve strategic ends has subsequently been expressed by policy makers through terms such as "gray zone competition" and "comprehensive coercion."[20] Hybrid warfare is conceptually distinct but related to political warfare and authoritarian coercion as it describes the application of these hostile activities and strategies across the conflict spectrum during times of war and peace.[21] Political warfare refers to these coercive activities outside the context of overt hostilities. In the strategic calculations of both Moscow and Beijing, political warfare appears to be a critical—if not decisive—line of effort in hybrid warfare campaigns.

NATO's work to date on hybrid warfare—coordinating with the European Union (EU) and other partners and providing support to NATO allies on critical areas upon request—represents crucially important steps in the right direction. Further, NATO's Public Diplomacy Division (PDD) counters disinformation and propaganda every day. Still, by framing NATO's response as one of hybrid warfare, its conceptual strength may also be a fundamental limitation. In terms

15 Danny Pronk, "The Return of Political Warfare," Strategic Monitor 2018-2019, Hague Centre for Strategic Studies, https://www.clingendael.org/pub/2018/strategic-monitor-2018-2019/the-return-of-political-warfare/; Alina Polyakova and Spencer P. Boyer, *The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition*, *Brookings Institution*, March 2018, https://www.brookings.edu/wp-content/uploads/2018/03/the-future-of-political-warfare.pdf; Lyle J. Morris et al., *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War*, *RAND Corporation*, 2019, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2942/RAND_RR2942.pdf; Anthony H. Cordesman, *Chronology of Possible Russian Gray Area and Hybrid Warfare Operations*, *Center for Strategic and International Studies*, December 8, 2020, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200702_Burke_Chair_Russian_Chronology.pdf; Kerry Gershaneck, "To Win Without Fighting: Defining China's Political Warfare," US Marine Corps University, April 2020, https://doi.org/10.36304/ExpwMCUP.2020.04; Kathleen H. Hicks, Joseph Federici, and Connor Akiyama, *China in the grey zone*, European Center of Excellence for Countering Hybrid Threats, Hybrid CoE Strategic Analysis 18, September 2019, https://www.hybridcoe.fi/wp-content/uploads/2020/07/Strategic-Analysis-18_2019.pdf; Lauren Speranza, *A Strategic Concept for Countering Russian and Chinese Hybrid Threats*, *Atlantic Council*, July 6, 2020, https://www.atlanticcouncil.org/in-depth-research-reports/a-strategic-concept-for-countering-russian-and-chinese-hybrid-threats/.

16 "NATO's response to hybrid threats," North Atlantic Treaty Organization, last updated March 16, 2021, https://www.nato.int/cps/en/natohq/topics_156338.htm#:~:text=Hybrid%20threats%20combine%20military%20and,and%20use%20of%20regular%20forces.

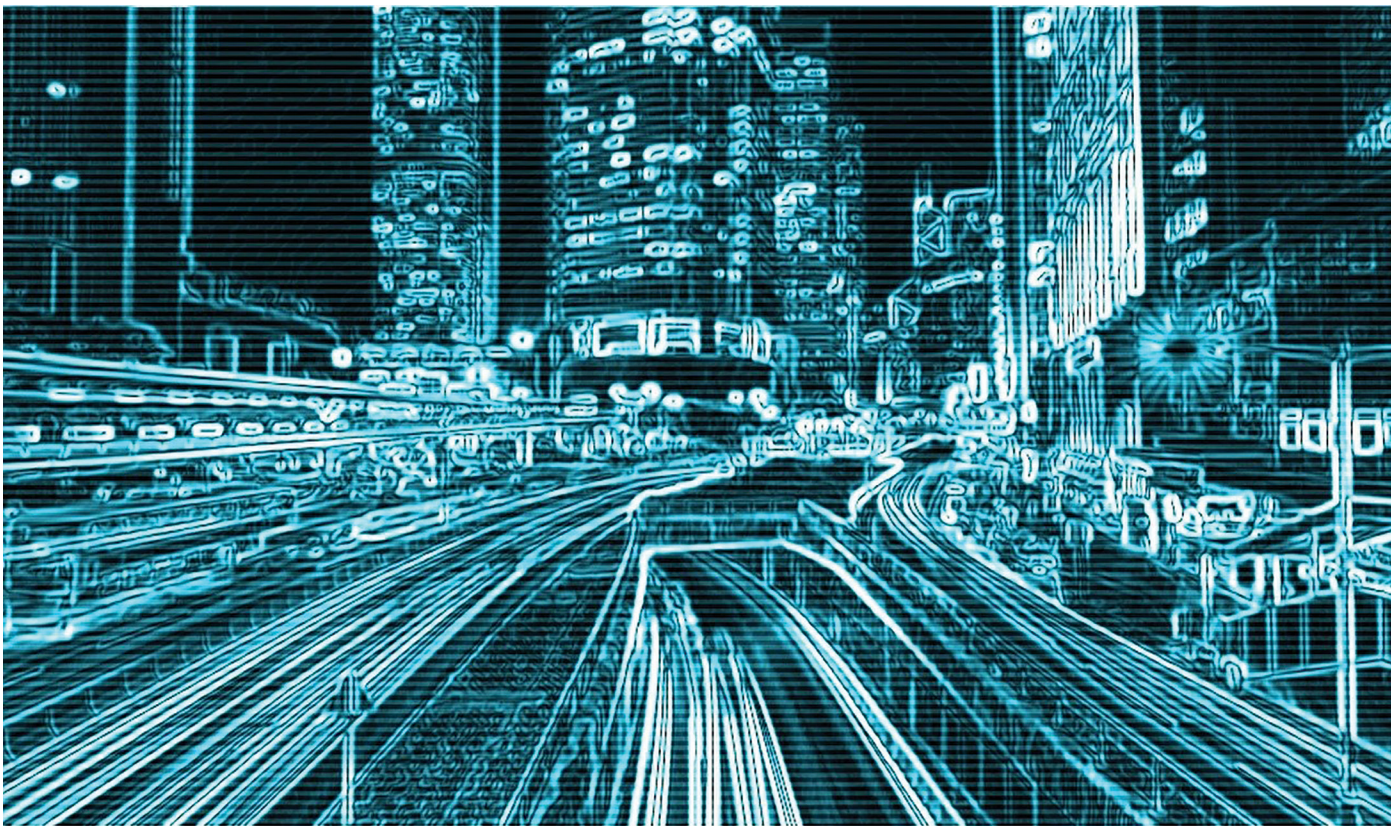
17 Put differently by Ross Babbage, "Whereas political warfare employs a range of instruments, it does not involve combat by military or para-military forces. Hybrid warfare operations, by contrast, involve the use of or commitment to use military or paramilitary forces in kinetic combat operations or a strategic commitment to engage in combat if deploying forces are seriously challenged." Ross Babbage, *Winning Without Fighting: Chinese and Russian Political Warfare Campaigns and How the West Can Prevail, Volume I*, *Center for Strategic and Budgetary Assessments*, 2, 2019, https://csbaonline.org/uploads/documents/Winning_Without_Fighting_Final.pdf.

18 Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, *Potomac Institute for Policy Studies*, 7, December 2007, https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf; Alina Polyakova et al., *The Evolution of Russian Hybrid Warfare*, *Center for European Policy Analysis*, January 2021, https://cepa.org/wp-content/uploads/2021/01/CEPA-Hybrid-Warfare-1.28.21.pdf.

19 Office of the Historian, Department of State, 269. Policy Planning Staff Memorandum, Washington, May 4, 1948, https://history.state.gov/historicaldocuments/frus1945-50Intel/d269.

20 Kathleen H. Hicks et al., *By Other Means: Part I: A Campaign in the Gray Zone*, *International Security Program*, *Center for Strategic and International Studies*, July 2019, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/Hicks_GrayZone_interior_v4_FULL_WEB_0.pdf.

21 Interestingly, within a NATO context, hybrid warfare is usually discussed in the context of Articles 4 and 5 of the Washington Treaty; by comparison, Article 2 is rarely mentioned.



Source: ItNeverEnds/Pixabay

of policy and activities, NATO has long applied itself as a "military" alliance, preferring to focus its efforts on *military support to* civilian authorities and applying expertise in areas that NATO militaries have established competencies, such as strategic communications; cyber defense; civil preparedness; chemical, biological, radiological and nuclear (CBRN) incident response; critical infrastructure protection; protection of civilians; and counterterrorism.[22] This leaves other multilateral organizations, such as the EU, as well as domestic agencies, including home, economic, and trade departments, responsible for activities that fall outside the military realm.[23] Put slightly differently, the balance of NATO's activities and focus has, at least in recent years, been on its military, rather than its political dimensions and the Alliance has generally shied away from taking an active role in responding to political-strategic challenges.

In theory, this is an effective division of labor. In practice, the separation of responsibilities in such a rigid manner leaves bureaucratic seams that adversaries, including Russia and China, can, and do, exploit. Indeed, in 2015 China established the People's Liberation Army's (PLA's) Strategic Support Force as part of a wave of military reforms. This Strategic Support Force pulled together China's psyops,

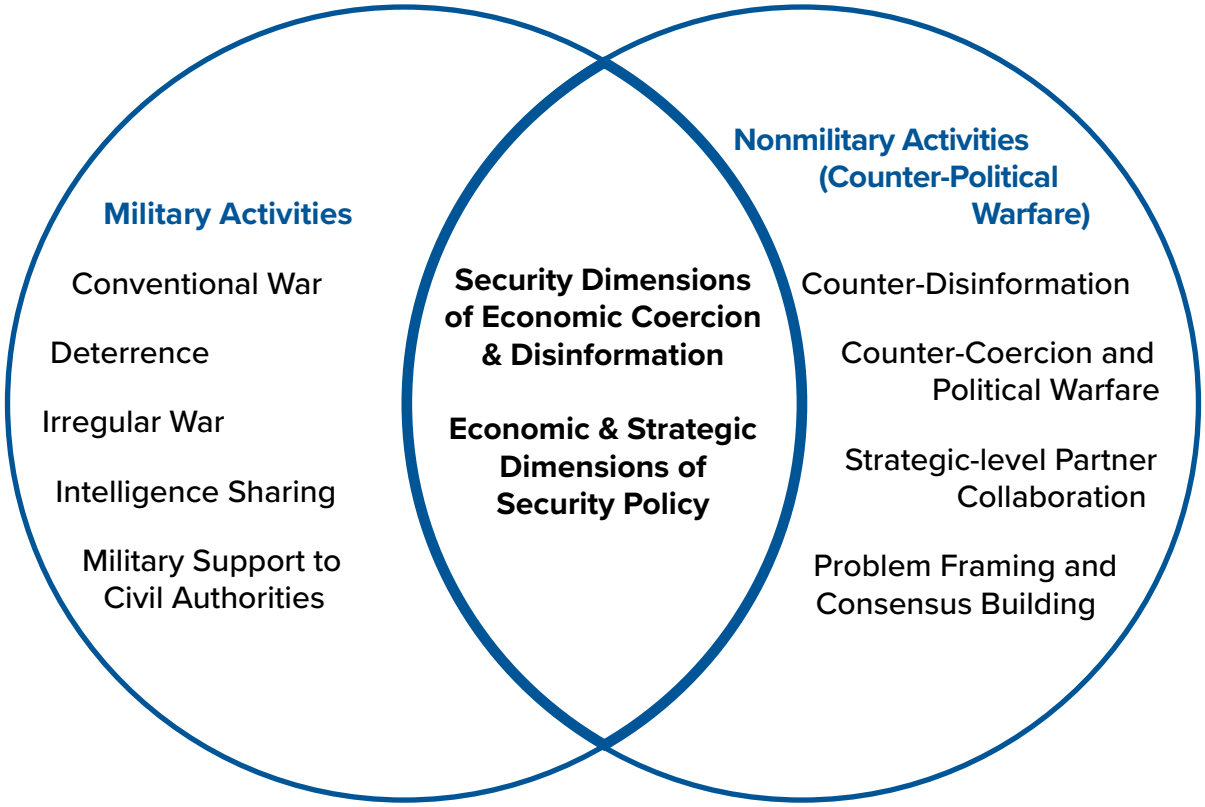
22 One notable exception to this list: NATO's development of energy security expertise, which allies can draw upon to build their counter-hybrid warfare plans.

23 For more information on the EU/NATO division of civilian/political and military responsibilities in hybrid warfare, see: Hanna Smith, "Countering Hybrid Threats" in *NATO and the EU: The Essential Partners,* NATO Defense College (September 2019), NDC Research Paper No. 5, https://www.jstor.org/stable/resrep19964.7?seq=1#metadata_info_tab_contents; Michael Rühle and Clare Roberts, "NATO's Response to Hybrid Threats" in *The Alliance Five Years after Crimea: Implementing the Wales Summit Pledges*, NATO Defense College (2019), NDC Research Paper No. 7, https://www.jstor.org/stable/resrep23664.11?seq=1#metadata_info_tab_contents. This division of labor has governed approaches to complex operational challenges for some time; for example, NATO International Security Assistance Force's (ISAF's) role in Afghanistan, which was limited to military support to civilian (in that instance, the United Nations, ISAF civilian agencies, and the government of the Islamic Republic of Afghanistan) activities. Further, NATO's own strategy for countering hybrid threats focuses on military support to civilian and domestic authorities. While these activities are certainly necessary, they are not sufficient. A comprehensive and coordinated approach to understanding and contending with the political and economic aspects of hybrid warfare strategies is needed to enable allies to get ahead of these issues rather than consistently play catch-up. See: "NATO's response to hybrid threats," North Atlantic Treaty Organization, last updated March 16, 2021, https://www.nato.int/cps/en/natohq/topics_156338.htm?selectedLocale=en; "What is NATO?" North Atlantic Treaty Organization, https://www.nato.int/nato-welcome/index.html.

disinformation, space, and cyber capabilities under one, centrally controlled roof.[24] This move is arguably indicative of China's belief in the comparative advantage of a holistic approach to these domains, which enables it to be more encompassing and synchronous in its execution of nonmilitary operations. While NATO allies and partners may not organize their own nonmilitary operations in the same way, it is critical to know that its adversaries are doing so and the edge that gives nations like China. Further, everyday competition with Russia and China is largely taking place outside the military sphere of competence. Threats in nonmilitary areas are having an impact on transatlantic security. It is thus incumbent upon NATO to come to grips with issues related to technological, economic, homeland security, and other areas that impact shared security, and for the Alliance to take a broader approach to countering these challenges. By framing the problem as one of hybrid warfare and organizing itself in a relatively rigid manner to prosecute it, NATO risks, in essence, defining itself out of playing an important role in countering Chinese and Russian coercion in the primarily nonmilitary arenas in which they are playing.

Figure 1 sketches out the conceptual challenge of NATO's current approach to hybrid warfare. Of note, the military dimensions of hybrid warfare are but one part of a broader political-military strategy; a truly holistic strategy for countering hybrid warfare requires action in both the military and nonmilitary spheres of national power. The political and economic dimensions of hybrid campaigns are given short shrift while the military role in these contexts is strengthened. By primarily concentrating NATO's efforts on military support to other actors in hybrid threat contexts, the Alliance is failing to meaningfully grapple with nonmilitary dimensions of hybrid warfare, and, therefore, inherently unable to help its members and partners develop much-needed comprehensive approaches to these hybrid threats. This is especially problematic given that many, if not all, of these nonmilitary activities have national security and defense implications that are difficult to counter

Figure 1. Elements and Overlaps: A Holistic NATO Hybrid Warfare Strategy



24 John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era*, China Strategic Perspectives 13, Center for the Study of Chinese Military Affairs, Institute for National Strategic Studies, National Defense University, October 2, 2018, https://ndupress.ndu.edu/Media/News/Article/1651760/chinas-strategic-support-force-a-force-for-a-new-era/.

absent a common, comprehensive framework that enables stakeholders to take into account the interplay and overlap between these spheres.

The failure to build shared threat assessments early on—or to even appreciate the different perspectives that exist on an emerging threat—often means that the interconnections between issues only become apparent *after* becoming a crisis. In this, the high-profile example of Huawei and 5G technologies provides an important lesson.[25] Only after a number of NATO allies had already agreed to commercial deals allowing Huawei to build 5G telecommunications infrastructure did security practitioners raise serious concerns about these deals and their implementation. As a result, many allies have raised concerns over the security of future intra-Alliance commercial and military communications, primarily because of risks posed by non-allied suppliers,[26] like Huawei, that give China the ability to sit close and access systems on the back end. After much discussion in 2018 and 2019, NATO allies signed the 2019 Leaders' Meeting London Declaration that outlined the importance of "the security of communications, including 5G" and recognized "the need to rely on secure and resilient systems."[27] In response to this, allies like the United Kingdom have backtracked on their plans to incorporate Huawei into their 5G plans. Indeed, in 2020, Estonia passed new legislation—dubbed the "Huawei law"—empowering the Estonian government and intelligence services to conduct security reviews of equipment intended for use in developing future telecommunications networks.[28]

From a commercial point of view, Huawei was an obvious choice due to its cost-effectiveness and relative quality. From a security standpoint, however, the widespread embedding of telecommunications technologies by companies with close linkages to the Chinese state—arguably a state with strategic interests counter to those of NATO allies and partners—set off alarm bells. All too often the communities of practice responsible, for example, for economic and trade policy on the one hand, and security policy on the other, operate like ships passing in the night. Developing a shared understanding of different national and sectoral perspectives on issues, including when there are red flags, is challenging but must be addressed. Looking forward, the relative sophistication of these authoritarian coercion strategies, combined with the sheer complexity of the international strategic environment, means that developing a sense of how issues and sectors interrelate—from the working to leadership levels of governments and organizations—will become a critically important enabler of effective hybrid strategy development. Fortunately, NATO is well positioned to help allies and partners identify and address these issues before they become international commercial and diplomatic flash points; what is needed is the political will and an actionable framework to do so.

Indeed, NATO has spent many years honing its military muscle, but to combat the full spectrum of hybrid threats, it must strengthen the counter-political warfare elements of its hybrid warfare strategy, focusing more on how it can play a role in the nonmilitary dimensions of countering coercion. NATO must start embracing the important roles it can play in developing common approaches to the nonmilitary dimensions of hybrid warfare; in particular, it should serve as a catalyst for developing strategies to counter the political warfare campaigns of authoritarian states. Thomas G. Mahnken, Ross Babbage, and Toshi Yoshihara note that these regimes engage in these activities in order to:

> "[A]void dissent, discourage foreign narratives that are inimical to their interests, generate support for policies they favor, enhance their freedom of action by keeping rivals distracted, and mitigate pushback against overt acts of revisionism."[29]

Crucially, because of the interplay between external and domestic threats to regime survival, the activities of Beijing and Moscow are best conceived as part of concerted, comprehensive, whole-of-society strategies to weaken adversaries and undermine many of the key institutions of the liberal international order. As Mahnken, Babbage, and Yoshihara argue:

> "These authoritarian states practice a form of political warfare that is notable in three respects. First,

25 According to a Congressional Research Service report, "In the aftermath of the 2008-2009 financial crisis and the ensuing eurozone debt crisis, notable Chinese investments in Europe included significant ownership shares in major European port terminals and acquisitions of leading firms in the robotics and high technology sector. Although Chinese investment in Europe has been on a downward trend since peaking at EUR 37 billion in 2016… studies indicate a sustained Chinese investment interest in information and communications technology, transport and infrastructure, and research and development collaborations." Kristin Archick et al., *Transatlantic Relations: U.S. Interests and Key Issues*, Congressional Research Service, 15, April 27, 2020, https://fas.org/sgp/crs/row/R45745.pdf.

26 Andrea Gilli and Francesco Bechis, "NATO and the 5G Challenge," *NATO Review,* September 30, 2020, https://www.nato.int/docu/review/articles/2020/09/30/nato-and-the-5g-challenge/index.html.

27 North Atlantic Treaty Organization, London Declaration, press release, December 4, 2019, https://www.nato.int/cps/en/natohq/official_texts_171584.htm.

28 Reuters Staff, "Estonia passes 'Huawei law' for telecom security reviews," Reuters, May 12, 2020, https://www.reuters.com/article/us-estonia-telecoms-law/estonia-passes-huawei-law-for-telecom-security-reviews-idUSKBN22O22I.

29 Thomas G. Mahnken, Ross Babbage, and Toshi Yoshihara, *Countering Comprehensive Coercion: Competitive Strategies Against Authoritarian Political Warfare*, *Center for Strategic and Budgetary Assessments*, 4, 2018, https://csbaonline.org/research/publications/countering-comprehensive-coercion-competitive-strategies-against-authoritar.

> due to their long history of using political warfare to consolidate and maintain Communist Party control during the 20th century, Moscow and Beijing continue to lean heavily on influence campaigns and view them as a core element of their competitive toolkit. Second, because these regimes remain deeply insecure and fearful of both internal challengers and external threats, they often eschew restraint and conduct a particularly aggressive form of political warfare. Lastly, thanks to their centralized governments, Russia and China enjoy a significant unity of effort and can engage in highly coordinated whole-of-nation campaigns to manipulate public opinion and political debate. Considering the inherent vulnerabilities of open democratic societies and decentralized governments against which these efforts are utilized, these attributes make comprehensive coercion an especially appealing strategy for authoritarian nations."[30]

Echoing these concerns, a number of NATO and partner heads of state and government have recently made the argument that political warfare and coercion needs to be addressed as a matter of urgency. At the Munich Security Conference in February, French President Emmanuel Macron argued, "I do believe NATO needs a new political momentum and clarification of its strategic concept. NATO needs a more political approach."[31] Likewise, NATO Secretary General Jens Stoltenberg noted, "Our potential adversaries use all the tools at their disposal—military, political, and economic—to challenge our institutions, weaken our societies, and undermine our security. Of course, to keep our people safe, we need a strong military. But we also need strong societies. As our first line of defense, we need a broader, more integrated and better coordinated approach to resilience."[32]

What is needed, therefore, is greater coherence in efforts by NATO allies and partners to counter political coercion. Current responses to these coercive strategies by NATO allies have tended to focus on specific types of warfare rather than the collective whole. While it is important to have tailored responses in each domain, the lack of a national or multinational approach to political warfare, as a collective and interconnected web of issues, hinders a truly comprehensive response to what are comprehensive hybrid campaigns. At NATO, no one body is charged with pulling together a situational picture of Russian and Chinese political warfare that would allow an understanding of linkages, patterns, strengths, and potential weaknesses in an adversary's campaigns. NATO can play a key role in providing that situational picture of hybrid warfare across the spectrum, including countering political coercion. However, the Alliance requires cooperation and information sharing from allies, partners, and other key stakeholders and an organizing process like a Comprehensive Approach 2.0.

30 Ibid., 4. Mahnken, Babbage, and Yoshihara note that China and Russia are not the only countries to utilize political warfare strategies. They also note that there are important differences between Beijing and Moscow's approaches to political warfare and as such they deserve thorough individual examination. Still, enough similarities between their political warfare approaches exist as to lend them to be categorized as "authoritarian political warfare." This paper, in turn, builds on their analysis.

31 Reuters Staff, "France's Macron: 'I do believe in NATO,'" Reuters, February 19, 2021, https://www.reuters.com/article/uk-germany-security-conference-macron-idUKKBN2AJ22T.

32 NATO Secretary General Jens Stoltenberg, "NATO2030: future-proofing the Alliance," remarks at the Munich Security Conference, February 19, 2021, https://www.nato.int/cps/en/natohq/opinions_181696.htm?selectedLocale=en.

National Hybrid Fusion Approaches

NATO allies and partners have made strides to counter political warfare in recent years, with varying degrees of success. Indeed, the *NATO 2030* report, produced after a yearlong reflection process in 2020, addressed the need for the Alliance to build shared terminology and situational awareness of the nature of hybrid threats, develop a comprehensive response framework, and create an ethical and legal framework for operating in the cognitive and virtual dimensions.[33] The report rightly identified gaps in the Alliance's current response to hybrid warfare, stating that NATO needs "a common political framework" for "assess[ment], attribut[ion], and respon[ses]."[34] Yet, at present, a full picture of the landscape of political warfare is missing in NATO. While NATO has Fusion Centers and Centers of Excellence (COEs) to further understanding of political warfare threats *among* allies, the information shared is only as good as the information garnered at a national level. Few nations have adequate cross-government frameworks at a *national* level for addressing political warfare as it cuts across multiple domains and departments' responsibilities. As such, assessments shared by nations multilaterally are not as comprehensive as they need to be to manage the threat. As a starting point, nations could usefully improve their national approaches to improve collective efforts to counter political warfare.

The UK provides an interesting example to get at this challenge. Acknowledging the importance of a collated national picture and coordinated national responses, the UK has developed a national fusion approach, a national effort to further whole-of-government responses to political warfare.

The UK's national Fusion Doctrine is aimed at bringing together the full suite of security, economic, and diplomatic tools at the UK's disposal and increasing understanding of political warfare threats across the UK government.[35] This Fusion Doctrine enables the UK to consider broader response options to political coercion; for instance, communications would be considered with the same seriousness as financial or military options to certain below-threshold attacks. The UK has also undergone an Integrated Review of Security, Defence, Foreign Policy and Development,[36] which has enabled all related departments of the UK government to participate in a net assessment of the threat landscape and the tools available across government to combat cross-cutting issues like political warfare. This whole-of-government assessment has enabled the UK to define roles and responsibilities, orient solutions across government agencies, and focus more on the issues and less on the actors executing the job. This has resulted in initiatives like the merging of the UK's Foreign and Commonwealth Office (FCO) with the Department for International Development (DFID) to form the Foreign, Commonwealth & Development Office,[37] with a belief that a combined office will improve synergies across government and enable a more collective and comprehensive response to cross-cutting issues. Other NATO allies and partners should consider pursuing national-level fusion strategies like the UK's Fusion Doctrine to improve whole-of-government assessments of threats and coordinate national responses to political warfare.

The United States has similarly considered the creation of a "National Fusion Center to Respond to Hybrid Threats" to coordinate its interagency responses to Russian hybrid threats from disinformation and political influence to cyber security.[38] While the proposal in Act S.482[39] did not pass, the center could have been a useful way to coordinate policy analysis across the US interagency in response to hybrid threats. The United States ought to reconsider the need for a national Fusion Center or similar body to coordinate and synchronize across government, to examine current and emerging threats by malign actors, and to close the gaps across departments and agencies with regard to expertise, readiness, and planning around hybrid threats.

Despite not having a fusion center, the United States has put in place a number of different approaches to meet this

33 North Atlantic Treaty Organization, *NATO 2030: United for a New Era: Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General*, 45, November 25, 2020, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf.

34 Ibid.

35 William McKeran, *Fusion Doctrine: One Year On*, *Royal United Services Institute,* March 8, 2019, https://rusi.org/commentary/fusion-doctrine-one-year.

36 "Ministry of Defence Integrated Review Command Paper," UK Government, September 14, 2020, https://www.gov.uk/government/collections/integrated-review-ministry-of-defence.

37 UK Parliament, Sixth Special Report, *Merging success: Bringing together the FCO and DFID: Government Response to Committee's Second Report*, September 17, 2020, https://publications.parliament.uk/pa/cm5801/cmselect/cmfaff/809/80902.htm.

38 Defending American Security from Kremlin Aggression Act of 2019, S. 482 — 116th Congress (2019-2020), 1st Session, Section 704: 90-95, December 18, 2019, https://www.congress.gov/116/bills/s482/BILLS-116s482is.pdf.

39 Ibid., 93.

Press point by NATO Secretary General Jens Stoltenberg on occasion of the inauguration of the European Centre of Excellence (CoE) for Countering Hybrid Threats.
Source: NATO/flickr

whole-of-government challenge. The United States' Open Source Enterprise in the Office of the Director of National Intelligence (ODNI)[40] works to collect, analyze, and distribute data gleaned from traditional and social media to create actionable intelligence that can be applied throughout the US Intelligence Community. This approach is evolving into a unique form of analytic tradecraft that can provide real-time information for policy makers.[41] In addition, the FY20 National Defense Authorization Act authorized the creation of a Social Media Data and Threat Analysis Center (DTAC) funded by the ODNI. While not yet stood up, the center is intended to encourage public-private cooperation to detect and counter foreign influence operations against the United States[42] and could help improve the threat assessment picture nationally. The United States also appropriated $250 million for fiscal years 2020 and 2021 for a Countering Russian Influence Fund,[43] putting resources toward its counter-political warfare efforts and emphasizing the need to work with civil society and European partners to strengthen the resilience of institutions to Russian malign influence.

Both the US and UK examples cited above provide useful models for other NATO allies to consider. The more allies are able to coordinate whole-of-government approaches to better understand and respond to political warfare, the more effective nations will become at tackling the whole spectrum and in their ability to coordinate with each other. Given Russia and China are waging political warfare as a campaign, rather than discrete, singular attacks, NATO allies must become better placed at understanding the strategic intent and respond to the challenge holistically.

Finland's European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) also takes on the full spectrum of hybrid challenges under one roof. The Hybrid CoE, based in Helsinki, was established in 2017 as the first Center of Excellence (CoE) of its kind. Under a national flag, it is uniquely placed to work across NATO, the EU, and with NATO and non-NATO countries to pool expertise, conduct research and analysis, and facilitate EU-NATO cooperation on countering hybrid threats.[44] As a national hub, the Hybrid CoE is well placed to enhance collaboration among European allies and partners and between national and international institutions. With three Community of Interest (COI) networks led by the UK, Finland, and Germany, the Hybrid CoE acts as a hub enabling participating countries and institutions to share best practices, experience, and expertise while offering a place for action to be coordinated.[45] The CoE also supports training and exercising among its twenty-eight participating nations from within and outside NATO. As a NATO partner, Finland, in particular, has been very effective at dealing with Russian political warfare, backed by its "strong public education system, long history of balancing Russia, and a comprehensive government strategy [which] allow it to deflect

40 Steven Aftergood, "Open Source Center (OSC) Becomes Open Source Enterprise (OSE)," Federation of American Scientists, October 28, 2015, https://fas.org/blogs/secrecy/2015/10/osc-ose/.

41 Esther Carey, Federal News Radio, "Spies give way to 'sexy' social media," Office of the Director of National Intelligence, August 2, 2012, https://www.dni.gov/index.php/newsroom/news-articles/ic-in-the-news-2012/item/584-spies-give-way-to-sexy-social-media?highlight=WyJzb2NpYWwiLCJzb2NpYWxseSIsInNvY2lhbGl6YXRpb24iLCJtZWRpYSIsIm1lZGlhJyIsIm1lZGlhJ3MiLCJzb2NpYWwgbWVkaWEiXQ==.

42 Dwight Weingarten, "Solarium Commission Makes Recommendations to Counter Disinformation," MeriTalk, June 4, 2020, https://www.meritalk.com/articles/solarium-commission-makes-recommendations-to-counter-disinformation/.

43 Defending American Security from Kremlin Aggression Act of 2019, 95.

44 "Hybrid CoE," European Centre of Excellence for Countering Hybrid Threats, https://www.hybridcoe.fi/.

45 "What is Hybrid CoE," European Centre of Excellence for Countering Hybrid Threats, https://www.hybridcoe.fi/who-what-and-how/.

coordinated propaganda and disinformation,"[46] and, therefore, can add real value to a Comprehensive Approach 2.0 and NATO discussions. On the contrary, while the NATO Strategic Communications Centre of Excellence in Riga, Latvia, (discussed in the disinformation section below) has sponsored cutting-edge research on information manipulation, the center's mandate as an advisory body has limited its real-world impact. A strengthened Article 2 mandate to increase political consultations could start with the work being done in Riga to debate, circulate, and implement its recommendations.

Beyond these US, UK, and Finnish examples, comprehensive approaches to political warfare among NATO members and partners are less prominent. Perhaps in part owing to bureaucratic stovepiping and policymaking preferences, many capitals of NATO member states that are targets of these campaigns tend to view each of Moscow and Beijing's actions discretely rather than as constituent parts of a holistic strategy. Failure to consider these activities and their implications holistically—and, therefore, failing to address their respective behaviors in a likewise holistic manner— risks the United States and its allies taking actions that achieve short-term successes at the expense of longer-term gains. Progress on areas like the EU-China Comprehensive Agreement on Investment (CAI), for example, which seeks to replace bilateral trade agreements between EU members and China with a common EU-wide investment framework, can present longer-term strategic risks to European states, including increased vulnerability to Chinese economic coercion and influence campaigns—not to mention heightened tensions in the transatlantic relationship due to increasingly divergent strategic approaches to China.[47] In other words, a strategic-level approach between NATO, its member states and partners, the private sector, and like-minded multilateral organizations like the EU is needed, as is a framework to turn strategic consensus into concrete action. Fortunately, both by treaty and by recent operational practice, NATO is well positioned to serve as a bedrock for both. The Alliance can, therefore, usefully serve as a catalyst for developing a Comprehensive Approach to combat coercion and political warfare.

46 Reid Standish, "Why Is Finland Able to Fend Off Putin's Information War?" *Foreign Policy*, March 1, 2017, https://foreignpolicy.com/2017/03/01/why-is-finland-able-to-fend-off-putins-information-war/.

47 In surveying the policy analytic landscape on the EU-China CAI, the European Parliamentary Research Service notes that, "James Andrew Lewis of the Center for Strategic & International Studies (CSIS) argues that the 'agreement itself is vulnerable' in terms of China's compliance with it, as 'some parts of the deal run counter to long-standing Chinese economic policy and practices' and China might be willing to live up to its commitments only to the extent this could 'prevent stronger transatlantic cooperation.'" It also notes the view of, "Noah Barkin of the German Marshall Fund (GMF) argues that the CAI 'exposes the transatlantic divide in three ways. First, it shows that the EU…still believes that economic and broader strategic interests can be neatly separated—an idea that is no longer accepted in Washington. Second, the deal shows that European capitals still see value in Chinese promises, despite evidence in recent years…that they are often tactical and empty. Third, after four years of Trump, the deal is a clear signal that the EU is embracing 'strategic autonomy.'" Gisela Grieger, "EU-China Comprehensive Agreement on Investment: Levelling the Playing Field with China," PE 679.103, Briefing, European Parliamentary Research Service, European Parliament, February 2021, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/679103/EPRS_BRI(2021)679103_EN.pdf.

Article 2 and the Art of the Political: NATO's Strategic Role in Countering Political Warfare

NATO stepping up to take on a larger role in countering political warfare has its trade-offs, and some might reasonably express concern about the knock-on effect that such an approach might have on the conduct of military affairs. Some concerns may include: first, if NATO is predominantly a military alliance, then it doesn't have a significant role to play in countering political warfare, which is the realm of politicians, statesmen, home departments, departments of commerce, and so on. Second, to assign political warfare as a supporting task to militaries, and military institutions like NATO, would likely dilute their focus on their essential defense functions (which are hard enough to perform on the best of days). It might also lessen the pressure on NATO allies and partners to effectively share the costs of hard defense. In the minds of critics, adding political warfare to the growing list of NATO's tasks means diminishing Alliance effectiveness.

These arguments—however well-intentioned—are unhelpfully divorced from both NATO's history and current realities. NATO is, and always has been, a political-military alliance in large part because contemporary alliances are themselves an inherently political-military construct.[48] To argue for the disaggregation of the military from the economic and political spheres is a conceit, arguably framed by present bureaucratic realities rather than institutional history. The post-World War II order, of which NATO is a part, was designed to be a proactive, forward-looking answer to the security dilemmas and distrust that had previously characterized alliance politics.[49] "Despair, disorder, decay from within—these were the likely dangers, not a Soviet invasion."[50] As the USSR's aggressive intentions became more clear, NATO itself became a solution to enabling European integration and economic revitalization rather than an end in and of itself.[51]

As NATO was established, reconstituting the economic and political health of its member states was seen as inextricably linked to military strength; military strength was one important pillar of a comprehensive strategy to counter Soviet influence and aggression.[52] NATO's purpose, therefore, as established in the Washington Treaty, is not only to grapple with military and defense challenges, but also to foster and protect the values core to its mission and that distinguish NATO as an alliance of like-minded nations. This is why NATO not only convenes military leaders and defense ministers at regular defense ministerial meetings,[53] but it also hosts foreign ministers at the same regularity[54] and heads of state and government roughly once a year at summits or Leaders Meetings.[55] Protecting the rights of its members as free and self-determining nations means, in essence, NATO allies have committed to upholding the integrity of the very institutions that are vulnerable to political warfare. This is why Article 2 of the Washington Treaty exists. It reads:

> "The Parties will contribute toward the further development of peaceful and friendly international relations by strengthening their free institutions, by bringing about a better understanding of the principles upon which these institutions are founded, and by promoting conditions of stability and well-being. They will seek to eliminate conflict in their international economic policies and will encourage economic collaboration between any or all of them."[56]

48 Glenn Snyder refers to this as the "political penumbra" of alliances. Glenn H. Snyder, *Alliance Politics* (Ithaca, New York: Cornell University Press, 1997).

49 Thies, *Why NATO*, 90-104.

50 Ibid., 95.

51 Ibid., 90-104. As NATO's official historians note, "It is often said that the North Atlantic Treaty Organization was founded in response to the threat posed by the Soviet Union. This is only partially true. In fact, the Alliance's creation was part of a broader effort to serve three purposes: deterring Soviet expansionism, forbidding the revival of nationalist militarism in Europe through a strong North American presence on the continent, and encouraging European political integration." "A Short History of NATO," North Atlantic Treaty Organization, accessed February 20, 2021, https://www.nato.int/cps/en/natohq/declassified_139339.htm; David S. Yost, *NATO's Balancing Act* (Washington, DC: United States Institute of Peace Press, 2014).

52 Dean Acheson, *Present at the Creation: My Years in the State Department* (W. W. Norton & Company, 1969) 266.

53 "Meetings of NATO Ministers of Defence," North Atlantic Treaty Organization, last updated February 18, 2021, https://www.nato.int/cps/en/natohq/events_181298.htm.

54 "Meeting of NATO Ministers of Foreign Affairs," North Atlantic Treaty Organization, last updated April 3, 2020, https://www.nato.int/cps/en/natohq/events_174657.htm?selectedLocale=en; "Events," North Atlantic Treaty Organization, https://www.nato.int/cps/en/natohq/events.htm.

55 "Summit meetings," North Atlantic Treaty Organization, last updated April 22, 2021, https://www.nato.int/cps/en/natolive/topics_50115.htm.

56 "Founding treaty," North Atlantic Treaty Organization, last updated September 24, 2020, https://www.nato.int/cps/en/natolive/topics_67656.htm.

Article 2 of NATO's founding charter is sometimes viewed as the "Canadian clause" or a throwaway paragraph in the Washington Treaty.[57] Yet negotiators of NATO agreements know that they should never discount a good diplomatic "hook," especially when it might be used to prompt positive action. Viewed in that light, Article 2 holds enormous utility in supporting and justifying much-needed NATO action on the political warfare challenges allies face on a routine basis. NATO has forgotten how to exercise its political arm to proactively contend with political and economic coercion as effectively as it does its military arm. Article 2 is critical to establishing an effective counter-political warfare response from NATO.

Specifically, in Article 2, allies have pledged to:

- Shore up free institutions;
- Establish public understanding of the principles undergirding institutions;
- Promote stability and well-being; and
- Eliminate conflict from international economic policies and promote economic collaboration.

These Article 2 principles are the very areas at risk from Russian and Chinese political warfare today. NATO allies and partners have fallen behind in combatting the political and economic components of political warfare across the spectrum; as a result, NATO should rethink the mandate it already has and reinvigorate Article 2 to help empower and enable a more effective, comprehensive response to future political warfare campaigns.

This leads to the second concern articulated above, namely, that expanding the aperture of NATO's activities will inherently dilute the Alliance and its military capabilities. This logic perhaps makes sense in the narrower context of burden sharing and defense planning. Yet the military is not an end in and of itself; rather, the object of the military is to be one means toward the promotion of national security and prosperity. Promotion of stability and security—and, therefore, (if indirectly) prosperity—has been interpreted in a variety of manners over the course of NATO's history: from deterring Soviet aggression to responding to crises in the Balkans and the Middle East to overcoming Franco-German and Greco-Turkish differences. Further, identifying and countering political warfare is largely an intellectual endeavor; organized appropriately, the cost of building a NATO counter-political warfare capability would be miniscule in comparison to the cost of purchasing defense equipment and acquiring capabilities. Given that today the stability, security, and prosperity of NATO allies and partners are being directly challenged by both Russia and China, this marginal investment would likely yield enormous strategic dividends.

Economic and political coercion campaigns have important linkages to national security—linkages that are often difficult for agencies and institutions to fully appreciate on their own. Trade ministries have a different set of priorities than defense ministries, but they both work on matters that have a direct bearing on the security and well-being of their states. A greater cross-pollination of government efforts improves assessments of the threat and development of potential solutions.

57 These points have been made to the authors by any number of interlocuters that study NATO.

Taking Stock: Assessing Existing Alliance and Partner Efforts to Counter Political Warfare

NATO might usefully seek to build shared understandings of, and approaches to, countering authoritarian coercion in two key areas: disinformation and election interference, and coercive diplomacy and economic subversion.[58] What follows is an assessment of the current state of play and areas ripe for multi-stakeholder collaboration on these key issues. Current efforts underway by the Alliance and its members tend to focus on discrete areas of political warfare rather than the full gambit. Countering disinformation and cyber defense are the two most advanced areas of the transatlantic response to hybrid warfare, yet NATO allies and partners lack advanced strategies to mitigate coercive diplomacy and predatory economic practices.

Disinformation and Election Interference

Alliance-Wide Efforts

Disinformation is one of the most nefarious challenges NATO faces. False news and the spread of "alternative" facts and narratives creates confusion, foments distrust in democratic institutions and government itself, sharpens societal divisions, and creates negative psychological and emotional responses that can be used to manipulate people's viewpoints and beliefs. Across Europe, nations come under near-daily attack from state-supported and rogue actor disinformation, from Russian-language campaigns, Chinese propaganda, social media swarms, and online bots. As Russia and China seek to shape the information environment in their favor,[59] NATO allies have put various initiatives in place to help combat disinformation and build societal resilience. Allies have pursued different national initiatives and the Alliance has worked to share best practices. It is worth noting that NATO is further advanced in its understanding and response to Russian disinformation than it is of Chinese disinformation which is much less analyzed and understood in a transatlantic context.

NATO's Strategic Communications Centre of Excellence (StratCom COE), based in Riga, Latvia, is focused on improving allied strategic communications capabilities.[60] The COE, staffed by experts from fourteen European countries, including partners Finland and Sweden, provides training and education for participating NATO leaders and specialists to help combat disinformation. The StratCom COE is intended to sharpen thinking and focus research on information manipulation around the world and advance the discipline, which allows it to serve a useful analysis function. Indeed, the COE has helped to develop doctrine and publications on countering disinformation that shape NATO discourse on the problem set. However, as an essentially analytical center with limited resources, it has a smaller impact on operations and national bureaucracies. The COE does not provide resources to nations to support campaigns or actively engage in countering disinformation as it spreads (unlike some NATO Force Integration Units, e.g., in Latvia), meaning its operational role is limited. While the COE's analysis has shaped PDD's understanding of how Russia uses a broad spectrum of influence operations, for example, against NATO enhanced Forward Presence (eFP) battlegroups, it is unclear how NATO engages with this analysis across the board and whether it has shaped policy responses to influence operations.

National Approaches to Countering Disinformation

On the practical side, there is no one NATO method or approach to countering disinformation. However, some NATO allies, especially in Northern Europe, are leading the way with full-scale efforts to identify, debunk, and attribute online disinformation.

At a national level, the UK government established a Rapid Response Unit (RRU) in 2018 to counter disinformation[61] and "reclaim a fact-based public debate."[62] The RRU, made up of UK disinformation specialists, has built a social

58 The authors recognize issues like cybersecurity are also commonly associated with hybrid warfare and have key authoritarian political warfare dimensions. Those issues fell outside the scope of this analysis but may be taken up in future work on this subject.

59 See the work done by the Atlantic Council's Digital Forensic Research Lab for more on China's use of information manipulation in regional and global competition and the dimensions of its disinformation strategy. "Countering Chinese disinformation reports," Digital Forensic Research Lab, Atlantic Council, December 17, 2020, https://www.atlanticcouncil.org/in-depth-research-reports/dfrlab-china-reports/.

60 "About Strategic Communications," NATO Strategic Communications Centre of Excellence, https://stratcomcoe.org/about_us/about-strategic-communications/1.

61 Disinformation is false information deliberately and often covertly spread (as by the planting of rumors) in order to influence public opinion or obscure the truth. Source: "Disinformation." In Merriam-Webster, online ed., https://www.merriam-webster.com/dictionary/disinformation.

62 Government Communication Service, "Alex Aiken introduces the Rapid Response Unit," July 19, 2018, https://webarchive.nationalarchives.gov.uk/20200203104056/https://gcs.civilservice.gov.uk/news/alex-aiken-introduces-the-rapid-response-unit/.

media capability using a "FACT" model; it *finds* suspicious stories, *assesses* whether they are disinformation, *creates* content rebalancing the narrative, and *targets* content to make sure the correct information is highly visible.[63] The RRU works alongside UK national security communications teams, especially in times of crisis when the UK government is trying to ensure official information is highly visible to the public. This technique ensures information deemed of high priority is disseminated nationally and that disinformation is challenged at a more rapid pace. While the RRU is not set up to combat all disinformation targeted at the UK, it helps ensure that the most critical misinformation is addressed. For example, after detecting misinformation following Syrian air strikes, including false narratives from alternative news sources that were gaining traction online, the RRU "ensured those [users] using search terms [on Google] that indicated bias—such as 'false flag'—were presented with factual information on the UK's response. The RRU improved the ranking from below 200 to number 1 within a matter of hours. Information on UKAID's work in the region was also immediately amplified amongst audiences demonstrating the highest levels of interest in humanitarian issues affecting displaced Syrians."[64] The RRU has been described as driving improvements across the UK government in response to disinformation, "providing media offices with the tools and skills needed to communicate effectively with citizens in an increasingly fragmented media landscape, [and] raising standards of reporting and evaluation."[65] The example of the RRU indicates at least some success in the UK government's approach to prioritizing the need to address misinformation. As other NATO allies and partners look for strategies to respond to disinformation in an increasingly complex online news environment, they may consider developing similar units or methods to prioritize countering disinformation.

In the Baltic states, and Lithuania in particular, an independent NGO and technological analytical center called Debunk EU[66] rapidly identifies online disinformation using a combination of AI-based analytics. Civil society volunteers, called "Baltic Elves," work with Debunk EU to challenge disinformation stories and correct the record publicly by responding with factual information to counter untruths propagated by trolls and bots. Debunk EU partners with Lithuanian government agencies and national media, as well as seventeen countries, including the United States, Germany, the UK, France, and Serbia, to support their counter-disinformation efforts. The Baltic Elves have been able to successfully detect and debunk a large amount of disinformation related to Lithuania in Russian news. This type of system is powerful; Debunk EU claims that it "is able to detect disinformation within two minutes of an article being published and can save journalists around 3-4 hours per day (on average)."[67] The Baltic Elves are organized volunteers—including journalists, IT professionals, businesspeople, students, and scientists—dedicated to tracing Russian "trolls" and challenging propaganda online. There are different types of elves—some are debunkers of false information, while others run "blame and shame" campaigns against pro-Kremlin trolls to attribute attacks to their perpetrators and hold them to account.[68]

Similarly, a Lithuanian publicist and journalist popularized the hashtag #KremlinYouWillNotFalsifyOurHistory, which went viral in a matter of hours. This created an upsurge in Lithuanians visiting the Ministry of Foreign Affairs of the Russian Federation's Facebook page, leaving thirteen thousand comments and dropping their rating from 4.2 stars to 1 star.[69] This approach demonstrates the significant value and potential implications of grassroots organizing in establishing societal buy-in to countering disinformation and degrading its reach. While the extent of the effect on Russian disinformation is unclear, popular engagement in countering disinformation can be a powerful tool if leveraged properly.

Examples like this indicate the power of combining AI-enabled systems on one hand, that can rapidly monitor online activities and share near-live detection reports of disinformation, with community-based volunteers on the other, that are able to provide the context and establish attribution in a way that AI is unable to. This model of leveraging a human-machine relationship could be explored further by other NATO allies and partners in combatting disinformation, especially online.

63 Fiona Bartosch, "How the Rapid Response Unit actually works (and why it's important)," *PR Week,* October 17, 2018, https://www.prweek.com/article/1496346/rapid-response-unit-actually-works-and-why-its-important.

64 Cabinet Office, "Mass Media: Internet: Written Question - 164285," UK Parliament, July 16, 2018, https://perma.cc/7C3D-9MGF; Library of Congress, "Government Responses to Disinformation on Social Media Platforms: United Kingdom," https://www.loc.gov/law/help/social-media-disinformation/uk.php#_ftn105.

65 UK Parliament, "Rapid Response Unit: Question for Cabinet Office," UIN 226754, tabled on February 27, 2019, accessed May 25, 2021, https://questions-statements.parliament.uk/written-questions/detail/2019-02-27/226754.

66 "About Debunk EU," Debunk EU, https://debunk.eu/about-debunk/.

67 *Financial Times*, "Debunk.eu," https://googlenewsinitiative.ft.com/dni-projects/debunk?fbclid=IwAR1rt4qtfTYgHIkm-_AI9mRE9N3LoFnteMnfqTPPE0PID0rmnOCAGE-ZUfY.

68 Michael Peel, "Fake news: How Lithuania's 'elves' take on Russian trolls," *Financial Times*, February 4, 2019, https://www.ft.com/content/b3701b12-2544-11e9-b329-c7e6ceb5ffdf.

69 Aleksander Król, "Defending the Information Space: the Lithuanian, Latvian and Estonian Example," Warsaw Institute, July 26, 2017, https://warsawinstitute.org/defending-information-space-lithuanian-latvian-estonian-example/.

Source: Jefferson Santos/Unsplash

The Role of the Commercial and Technology Sector

More private companies like Twitter and Google are experimenting with different methods to fulfill their role in preventing the spread of disinformation. For example, Google's think tank Jigsaw combined Google's search engine and YouTube's video platform to counter radicalization of potential Islamic State of Iraq and Syria (ISIS) recruits. Using the "redirect" method, Jigsaw identifies key phrases often associated with radicalization, and rather than showing potentially dangerous material, the engine instead will redirect online users to videos and articles that provide information to help mitigate radicalization, such as testimonials by former extremists, imams denouncing ISIS, and clips showcasing the caliphate's dysfunctionality. This method of diverting the user to factual information alternatives has proven to be effective at drawing more than three hundred thousand online searches to anti-ISIS videos.[70] A redirect model could be applied more effectively to stymie disinformation campaigns by establishing the parameters for typical Russian and Chinese propaganda. NATO allies and partners should enhance collaboration with social media companies and private sector actors to build partnerships and support for such efforts to prevent the spread of disinformation.

Additionally, in January 2021, Twitter announced the launch of a pilot project called Birdwatch, a community-driven experiment to help identify information in tweets believed to be misleading and respond with notes that provide informative context for users that come across them.[71] The pilot, which has yet to come into full fruition, relies on a community-based approach to flag misinformation on the platform. The company recognizes challenges of building a community-driven system, including ensuring the fact checker community itself remains "resistant to manipulation attempts [and] ensuring it isn't dominated by a simple majority or biased based on its distribution of contributors."[72] While the pilot has yet to be tested in the real world, it illustrates one example of how private actors are conceiving of new approaches, such as community-driven content moderation. As NATO allies propose government policies and approaches to counter disinformation, weighing the pros and cons of community-driven content and

70 Andy Greenberg, "Google's Clever Plan to Stop Aspiring ISIS Recruits," *Wired,* September 7, 2016, https://www.wired.com/2016/09/googles-clever-plan-stop-aspiring-isis-recruits/.

71 Birdwatch, Twitter, https://twitter.com/i/birdwatch.

72 Keith Coleman, "Introducing Birdwatch, a community-based approach to misinformation," *Twitter Blog,* January 25, 2021, https://blog.twitter.com/en_us/topics/product/2021/introducing-birdwatch-a-community-based-approach-to-misinformation.html.

assessing the effectiveness of private-sector strategies such as this will be key.

Current Efforts to Build Long-Term Societal Resilience through Education

Some NATO allies and partners are also working to both grapple with the long-term effects and mitigate the impact of disinformation by proactively improving resilience among the intended targets of the disinformation: the transatlantic public. NATO partners and some allies are attempting to thwart the power of disinformation by safeguarding their publics from its effects through education, improving information literacy, and bolstering resilience and recognition of false information. The idea being that if publics recognize disinformation, they are less likely to be taken in by its effects.

Northern European allies and partners, including the Baltic states,[73] Norway,[74] Sweden,[75] and Finland,[76] each have inculcated "Total Defence" concepts into their defense planning. Having experienced ongoing information operations following the Cold War, these countries have recognized the importance of building whole-of-society resilience to information and influence operations. While each nation's concept is slightly different, the overall intent is a government-supported effort to build resilience at every level to prepare for worst-case scenarios like a crisis or war, while improving the country's psychological defenses to everyday influence operations. This approach involves building public awareness of misinformation and educating children and adults to improve their cyber and information literacy. The success of this model requires the willingness of society to participate in the defense of the country by empowering individual responsibility. For example, in Finland, media literacy is taught in classrooms from K-12. Schools partner with fact-checking agencies such as Faktabaari to teach the implications of disinformation to citizens. A Reboot report found that simple interventions, like reading an article on how to spot illegitimate sources of information, can help people identify misleading news. Simply making people aware of misinformation may make them more likely to spot it in the short term.[77]

This form of societal hardening and focus on information literacy has proven effective at mitigating the impact of political warfare.[78] The idea being that if society is able to recognize an influence operation and disinformation for what it is, then such attacks lose their impact because the goal of influencing society, undermining trust, or reshaping reality has little effect on its intended audience. While smaller countries may have an easier job when it comes to educating their populations, influence operations are not limited to NATO's northeast. Other NATO allies and partners should learn from the experiences of the Nordic-Baltic states and institute their own versions of Total Defense Concepts, focusing on specific areas of vulnerability in their own societies. Currently, more than one-third of students in US middle schools report rarely learning key media literacy skills like judging source reliability.[79] Teaching media literacy and critical thinking when engaging with social media and news articles is an important step to get at the root of the effects of disinformation. Alone it is not enough, though; institutional change must occur, including within media and social media companies which must work to prevent the spread of disinformation on their platforms. A combination of societal education and resilience and countering disinformation when it occurs can help prevent disinformation from disrupting society and impacting national security.

Overall, responses to disinformation across the Alliance remain slow and fragmented. While good strides have been made in Northern Europe, efforts have been mixed elsewhere in the Alliance. NATO's focus is still largely on pushing back on disinformation as it occurs, but reactive responses alone remain insufficient. As reliance on technology and online platforms for information continues to grow, mitigation strategies must become more proactive and sophisticated. The Alliance should focus on societal resilience as a key element to diffuse the potency of the effects of disinformation by introducing more widespread

73 Marta Kepe and Jan Osburg, "Total Defense: How the Baltic States Are Integrating Citizenry Into Their National Security Strategies," *Small Wars Journal,* September 24, 2017, https://smallwarsjournal.com/jrnl/art/total-defense-how-the-baltic-states-are-integrating-citizenry-into-their-national-security-.

74 Second Line of Defense, "Norway Releases its Long Term Defence Plan, 2020: Resilience as a Core Defense Capability," April 20, 2020, https://sldinfo.com/2020/04/norway-releases-its-long-term-defence-plan-2020-resilience-as-a-core-defense-capability/.

75 Dr. Björn von Sydow, "Resilience: Planning for Sweden's 'Total Defence'" *NATO Review,* April 4, 2018, https://www.nato.int/docu/review/articles/2018/04/04/resilience-planning-for-swedens-total-defence/index.html.

76 James Kenneth Wither, "Back to the future? Nordic total defence concepts," *Defence Studies* 20 (1) (January 26, 2020): 61-81 https://www.tandfonline.com/doi/abs/10.1080/14702436.2020.1718498?journalCode=fdef20.

77 Reboot, *Fighting Fake News: Lessons from the Information Wars*, November 6, 2019, https://reboot-foundation.org/fighting-fake-news/; see also, Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (Farrar, Straus and Giroux, 2020).

78 Edda Humprecht, Frank Esser, and Peter Van Aelst, "Resilience to Online Disinformation: A Framework for Cross-National Comparative Research," *International Journal of Press/Politics*, January 24, 2020, https://journals.sagepub.com/doi/10.1177/1940161219900126.

79 Cision, PR Newswire, "Combating Fake News: Only a Third of Students Regularly Learn to Judge Reliability of Sources," November 6, 2019, https://www.prnewswire.com/news-releases/combating-fake-news-only-a-third-of-students-regularly-learn-to-judge-reliability-of-sources-300952345.html.

education campaigns and information and media literacy education.[80] Building long-lasting and generational societal resilience to false information helps stymie the effects of disinformation by protecting the targets that malign actors are trying to corrupt. In other words, these are areas that require the kind of cross-alliance, cross-government, and cross-functional civil-military collaboration that could usefully be advanced by an enhanced NATO Comprehensive Approach work stream, outlined in more detail later in this report. By starting a Comprehensive Approach to address this issue, Alliance members can learn from each other and partners' best practices and develop a toolkit that draws lessons from national pilots, education programs, disinformation and cyber literacy efforts, private sector engagement and social media regulation, and the development of total defense concepts, to name a few.

NATO's PDD also plays a key role in proactively shaping positive narratives with NATO publics, such as through the "We Are NATO" campaign. Yet PDD could likely do more to counter the disinformation components of political warfare campaigns. The North Atlantic Council might, therefore, usefully assess whether PDD is presently staffed and resourced to respond to the intensity of Russian and Chinese political warfare, and the extent to which PDD is properly integrated into NATO bodies' counter-disinformation efforts. Further, effective and active strategic communications should be plussed up across the transatlantic community to get out ahead of disinformation stories preemptively and to promulgate facts and honest narratives. NATO should note that it is more familiar with the tactics and applications of Russian disinformation, but now and in the long run allies and partners must become better acquainted with Chinese propaganda as well. To build more effective national and transatlantic counter-disinformation systems, sufficient resourcing and prioritization of these efforts, coupled with coordination among key stakeholders, is a crucial starting point—including government support, technology sector engagement, civil society empowerment, and integration of NATO allies and partners' strategies.

Coercive Diplomacy and Economic Subversion

Responding to Chinese Economic Subversion and Coercive Diplomacy

While NATO has traditionally focused on Russian coercive behavior in Europe,[81] allies and partners have begun focusing on Chinese coercive diplomacy as an emerging challenge. Besides recently considering restrictions on Chinese companies like Huawei,[82] transatlantic countries have discussed the need for more conscious economic decoupling of supply chains[83] and the risks of Chinese debt diplomacy[84] while more explicitly calling out the security challenges China poses to the transatlantic community. An Australian report documents cases of coercive diplomacy by the Chinese Communist Party (CCP) from 2010 to 2019, noting a significant uptick since 2018.[85] While coercive diplomacy has often been a tenuous way to achieve interests, the CCP has threatened "countermeasures, retaliation, pain, and the right to further react"[86] and has used coercion as a low-risk, high-reward way to ensure compliance from countries that are economically dependent on China. Many analysts have suggested stronger multilateral economic security partnerships and policies are required to combat China's active coercive threats.[87]

In December 2020, NATO huddled with Asia-Pacific democracies Australia, New Zealand, Japan, and South Korea to discuss China.[88] The Alliance's *NATO 2030* report acknowledges the oversized threat of China, asserting that "NATO must provide a position of security and strength to contribute to Allies' relations with China and guard against any attempts by Beijing to employ coercion against them....

80 Another interesting digital literacy project that may soon have insights to share toward promoting disinformation resilience is one currently being run by New America in conjunction with the University of South Florida. Together, they are piloting a "cyber citizenship" program to improve digital literacy skills for K-12 students in Florida. See: P.W. Singer and Michael McConnell, "Want to Stop the Next Crisis? Teaching Cyber Citizenship Must Become a National Priority," *Time*, January 21, 2021, https://time.com/5932134/cyber-citizenship-national-priority/; New America, Cyber Florida, Florida Center for Instructional Technology and New America Launch New Partnership to Improve "Cyber Citizenship" Skills for K-12 Students, press release, December 16, 2020, https://www.newamerica.org/international-security/press-releases/cyber-florida-fcit-new-america-partnership-to-improve-cyber-citizenship/.

81 Julian Lindley-French, *Complex Strategic Coercion and Russian Military Modernization*, *Canadian Global Affairs Institute,* January 2019, https://www.cgai.ca/complex_strategic_coercion_and_russian_military_modernization.

82 Matthew S. Schwartz, "In Reversal, U.K. Will Ban Huawei Equipment From Its 5G Network," NPR, July 14, 2020, https://www.npr.org/2020/07/14/890812517/in-reversal-u-k-will-ban-huawei-equipment-from-its-5g-network.

83 Duanjie Chen, "Countering China's Economic Coercion with Resolve and Diversification," Ambassador's Brief, October 13, 2019, https://www.ambassadorsbrief.com/posts/qmPALCPhMvfJWxbE9.

84 Mark Green, "China's Debt Diplomacy," *Foreign Policy*, April 25, 2019, https://foreignpolicy.com/2019/04/25/chinas-debt-diplomacy/.

85 Fergus Hanson, Emilia Currey, and Tracy Beattie, *The Chinese Communist Party's coercive diplomacy*, *Australian Strategic Policy Institute,* September 1, 2020, https://www.aspi.org.au/report/chinese-communist-partys-coercive-diplomacy.

86 Fergus Hanson, Emilia Currey, and Tracy Beattie, "Report: How China Uses Trade as a Lever for Coercive Diplomacy," *Maritime Executive*, August 31, 2020, https://www.maritime-executive.com/editorials/report-how-china-uses-trade-as-a-lever-for-coercive-diplomacy.

87 Anthony Vinci, "How to Stop China From Imposing Its Values," *Atlantic,* August 2, 2020, https://www.theatlantic.com/ideas/archive/2020/08/like-nato-but-for-economics/614332/.

88 Shannon Tiezzi, "NATO Huddles With Asia-Pacific Democracies to Talk China," *Diplomat,* December 3, 2020, https://thediplomat.com/2020/12/nato-huddles-with-asia-pacific-democracies-to-talk-china.

This requires that China be unable to exploit differences between Allies."[89] Key recommendations include devoting much more time, political resources, and action to security threats posed by China, including creating a consultative body to address China. This is starkly different from the last strategic planning report issued over a decade ago that did not mention China at all, and the recommendations should be heeded.

China's coercive practices span from its Belt and Road Initiative (BRI), which involves predatory lending;[90] to investments in critical infrastructure in Europe, like the Port of Piraeus in Greece[91] and attempts to invest in Lithuania's Klaipeda Port; as well as China's 17+1 initiative labelled by some as a tool to divide Europe.[92] Coercive diplomacy is nefarious because what at face value can seem like a harmless interaction can be turned into leverage for diplomatic support on other issues. For example, China has consistently used its economic power and countries' dependence on it to leverage support for votes in the United Nations related to human rights and other issues in China's interest.[93]

Transatlantic countries have explored alternatives to mitigate the impact of China's coercive diplomacy and economic subversion. Some NATO allies have called for alternatives to the BRI, offering investment and development opportunities that can be used instead of China's. UK and US alternatives, in particular, can be used by Central and Eastern European countries to mitigate the risks of taking Chinese foreign direct investment. For example, the UK's CDC Group is a development finance institution with a $5.9 billion portfolio for primary investment,[94] and the US BUILD Act of 2018 established an International Development Finance Corporation to invest $60 billion overseas.[95] Seen as "America's development bank," it seeks to move countries toward free markets, rather than participate in Chinese debt diplomacy.[96]

Transatlantic nations have also developed the Three Seas Initiative (3SI) Fund, a US-backed regional infrastructure development project intended to foster cross-border economic and infrastructure development in Central and Eastern Europe.[97] Launched in 2015 by Croatia and Poland, 3SI is often seen as a potential counterweight to Chinese-led initiatives like the BRI and 17+1 that have sought to tie countries in the region to Chinese investments.

In addition to investment alternatives, European countries have made some headway in screening foreign direct investment that can be used to hold majority power and influence over European companies and in key markets. The EU's 2019 Foreign Direct Investment Screening Regulation provides a framework for screening foreign direct investment, including mechanisms for information-sharing and flagging specific investments that could be deemed a security concern to member states.[98] This regulation has also helped EU members develop their own national screening mechanisms.

NATO allies and partners are still in the nascent stages of understanding and mitigating Chinese coercion as it plays out in Europe. Willingness to identify and call out the security risks surrounding certain types of Chinese government and commercial engagement in Europe is a key step, but much more sober reflection is needed among transatlantic countries to determine the risks of certain engagement, as well as how and where to push back.

Responding to Russian Subversion and Coercion

Russian coercion in Europe takes a different form from China's. Russia has leveraged its energy supplies to Europe as a tool of statecraft, especially in regions where countries' energy resources are reliant on Soviet-era infrastructure. In the Baltic states, in particular, Russia has attempted to interrupt oil and gas supplies to the region

89 North Atlantic Treaty Organization, *NATO 2030*.

90 Daniel Kliman et al., *Grading China's Belt and Road*, *Center for a New American Security,* April 8, 2019, https://www.cnas.org/publications/reports/beltandroad.

91 Valbona Zeneli, "Mapping China's Investments in Europe," *Diplomat,* March 14, 2019, https://thediplomat.com/2019/03/mapping-chinas-investments-in-europe/.

92 Ivana Karásková, "Engaging China in 17+1: Time for the ACT Strategy," *Diplomat,* April 7, 2020, https://thediplomat.com/2020/04/engaging-china-in-171-time-for-the-act-strategy/.

93 Henrik B.L. Larsen, "Balancing China at the United Nations," *War on the Rocks*, November 19, 2020, https://warontherocks.com/2020/11/balancing-china-at-the-united-nations/; Human Rights Watch, "The Costs of International Advocacy: China's Interference in United Nations Human Rights Mechanisms," September 5, 2017, https://www.hrw.org/report/2017/09/05/costs-international-advocacy/chinas-interference-united-nations-human-rights.

94 CDC Group, website homepage, accessed April 7, 2021, https://www.cdcgroup.com/en/.

95 U.S. International Development Finance Corporation, website homepage, accessed April 7, 2021, https://www.dfc.gov.

96 Joel Gehrke, "New US foreign investment agency counters China Belt and Road 'colonialism,'" *Washington Examiner,* June 14, 2020, https://www.washingtonexaminer.com/policy/defense-national-security/new-us-foreign-investment-agency-counters-china-belt-and-road-colonialism.

97 Congressional Research Service, *The Three Seas Initiative*, updated April 26, 2021, May 12, 2020, https://fas.org/sgp/crs/row/IF11547.pdf.

98 European Commission, "EU foreign investment screening regulation enters into force," April 10, 2019, http://trade.ec.europa.eu/doclib/press/index.cfm?id=2008.

The NATO Energy Security Centre of Excellence in Vilnius. *Source:* NATO/flickr

threatening their energy access.[99] Crippling a country's access to energy could have devastating effects on the ability of a nation to function, potentially halting everyday activity and disrupting access to food and key resources. Russia may use energy manipulation as a tool of statecraft to coerce a country to bend to its will. This must be taken as seriously as other forms of political warfare.

NATO's Center of Excellence on Energy Security (ENSEC COE) was established in 2012 to provide technical and scientific expertise on energy security to allies. Composed of military and civilian experts from NATO and partner nations, the COE produces risk assessments, analysis on energy supply and energy infrastructure protection, as well as advice for the development of energy efficient forces and the mitigation of resource scarcity.[100] In January 2020, NATO's Science and Technology Board authorized the creation of a research task force to focus on energy security in the era of hybrid warfare.[101] One of the key aspects of this group is to provide an Alliance-wide overview of NATO's energy security posture while working to produce a range of possible mitigation strategies and countermeasures for members to implement.[102]

While these are positive developments, there is still distinct disagreement among NATO allies regarding energy supplies in Europe and their potential to be misused in political warfare. Germany has been a proponent of Nord Stream 2—a controversial natural gas pipeline that would carry Russian gas under the Baltic Sea directly to Germany, enabling Russia to circumvent the Eastern European countries through which Russian gas currently flows westward.[103] While proponents of the pipeline describe the economic benefits of a commercial investment in Europe's supply security, opponents highlight probable adverse environmental impact, concerns over increasing European reliance on Russia for energy, and the empowerment of Russia[104] at a time when it's facing criticism for its destabilizing global activities.[105] Internal disagreement within NATO continues to prevent Alliance-wide consensus to mitigate Russian economic and energy manipulation as a form of political warfare.

99 Sierra Brown, "Russia's Use of the Energy Weapon: How Russia Manipulates Ukraine, Georgia, and the Baltic States," *Scholarly Horizons: University of Minnesota, Morris Undergraduate Journal* 6 (1) (February 2019), https://digitalcommons.morris.umn.edu/cgi/viewcontent.cgi?article=1073&context=horizons.

100 "About," NATO Energy Security Center of Excellence, accessed April 7, 2021, https://www.enseccoe.org/en/about/6.

101 "Energy Security in the Era of Hybrid Warfare," Science and Technology Organization, North Atlantic Treaty Organization, https://www.sto.nato.int/Lists/STONewsArchive/displaynewsitem.aspx?ID=524.

102 Ibid.

103 Andreas Kluth, "Get Ready For a Merkel-Biden Bust-Up Over Russian Gas," Bloomberg, February 5, 2021, https://www.bloomberg.com/opinion/articles/2021-02-05/nord-stream-2-get-ready-for-a-merkel-biden-bust-up-over-russian-gas.

104 Julian Wettengel, "Gas pipeline Nord Stream 2 links Germany to Russia, but splits Europe," *Clean Energy Wire*, March 19, 2021, 2020, https://www.cleanenergywire.org/factsheets/gas-pipeline-nord-stream-2-links-germany-russia-splits-europe.

105 Agence France-Presse and Associated Press, "Russian President Vladimir Putin rejects G7 criticism, stresses cooperation," *Deutsche Welle,* October 6, 2018, https://www.dw.com/en/russian-president-vladimir-putin-rejects-g7-criticism-stresses-cooperation/a-44145201.

Next Steps: The Need for a 'Comprehensive Approach 2.0'—NATO's Operational-Level Framework for Civil-Military Coordination

While NATO as an institution, as well as its allies and partners, have made positive strides to counter disinformation and coercion from Russia and China, current efforts do not go far enough to counter the scale of the threat. Attention to the problem is also mixed across the Alliance despite political warfare being an Alliance-wide concern that requires an urgent response. Hampering things further, NATO allies and partners' countereffforts are largely stovepiped, focused on pieces of the political warfare pie but not the whole thing. In other words, coordination and collaboration could be usefully improved.[106]

To fully grapple with political warfare, NATO must make a strategic and conceptual shift in its approach. It must flex and build up the "political" arm of its toolkit by adopting a Comprehensive Approach 2.0 to combating political warfare. Such an approach would help NATO better organize itself to contend with key challenges in the economic and disinformation spheres, and to address other elements of political and hybrid warfare, such as cyber warfare.

Over the past two decades, NATO has developed a set of crisis management instruments—dubbed the Comprehensive Approach—designed to foster whole-of-government solutions to complex stability challenges in hostile environments.[107] The term Comprehensive Approach is often conflated with operations in Afghanistan and, to a somewhat lesser extent, the Balkans and Iraq—all of which are rather different operational contexts and problem sets than the challenge that authoritarian political warfare waged by Beijing and Moscow presents. Yet stepping back, the experience of trying to deliver civil-military effects on the ground offers NATO allies and partners a number of important lessons and design principles when it comes to catalyzing a shared approach amongst a number of actors. Despite some of its inevitable shortcomings on the ground—to be fair, operating in Afghanistan is difficult on the best of days—the Comprehensive Approach was an enormous and complex undertaking for synchronizing the civilian and military instruments of national and multinational power.[108] Delivering this approach in Afghanistan involved building a shared understanding of the challenges amongst an enormous number of stakeholders, including (but not limited to) the government of Afghanistan, non-NATO troop contributing nations and partners, the EU, the UN, and the World Bank—in addition to coordinating defense, development, and diplomatic efforts of NATO allies themselves. Similarly, a Comprehensive Approach to countering political warfare requires going beyond building shared perceptions of the challenge to devising mechanisms for cooperatively meeting that challenge. The value of applying the Comprehensive Approach model to the problem of political warfare is that the framework has been tested by NATO and its partners, and the Alliance has learned many lessons from its application (including what not to do). Such a process would help bring much-needed institutional coherence and cohesion to the broad, interconnected, and complex set of political warfare challenges.

Under the auspices of Article 2 of the Washington Treaty, NATO should establish a Comprehensive Approach 2.0 agenda and associated institutions to deal with countering authoritarian coercion, building on lessons learned from previous experience in delivering civil-military effects. A Comprehensive Approach 2.0 would rely on building whole-of-government and whole-of-Alliance solutions to the whole spectrum of political warfare. Collaborative planning among existing NATO institutions, national-level stakeholders, private sector actors, civil society, and other multinational institutions is vital. This means, among other things, collaborating within NATO—as well as with non-NATO actors—to develop more advanced and compatible (if not common) threat assessments; shared understandings of different roles, responsibilities, and authorities in crisis situations; and ensuring that multinational and interagency perspectives are built into NATO plans, doctrine, training, and exercises. While NATO allies share threat perceptions and best practices on specific issues—for example, within the StratCom COE, Hybrid CoE, Cyberspace

106 Bastien Geigerich, "Hybrid Warfare and the Changing Character of Conflict," *Connections* 15 (2) (Spring 2016): 65-72, https://www.jstor.org/stable/26326440.

107 "A 'comprehensive approach' to crises," North Atlantic Treaty Organization, last updated June 26, 2018, https://www.nato.int/cps/en/natohq/topics_51633.htm.

108 Michael J. Williams, *The Good War: NATO and the Liberal Conscience in Afghanistan* (Palgrave Macmillan UK, 2011); Sten Rynning, *NATO in Afghanistan: The Liberal Disconnect* (Stanford, California: Stanford University Press, 2012).

Then-NATO Deputy Secretary General Rose Gottemoeller visits the NATO Strategic Communications Centre of Excellence in Latvia and meets with Director Janis Sarts. *Source:* NATO/flickr

Operations Centre, Energy Security COE, and other fora—there is no one forum at NATO with the function to establish a holistic picture of the spectrum of political warfare across all areas of cyber, energy security, disinformation, coercive diplomacy, and economic subversion. This is what is needed to enable NATO to establish an understanding of adversarial trends, patterns, strengths, Alliance weaknesses, and how political warfare is evolving over time, and to determine the roles and responsibilities of allies and NATO departments to counter political warfare.

Design Principles of a Comprehensive Approach 2.0 for Political Warfare

Taking a Comprehensive Approach 2.0 forward, there are a range of lessons learned from NATO's previous experience developing a tactical-level Comprehensive Approach in Afghanistan, Iraq, and elsewhere. The following key design principles derived from these experiences should be used to develop the framework for a strategic-level Comprehensive Approach 2.0 for political warfare, nested under NATO's Article 2. These key principles include:

Focus on the nature of the challenge rather than roles and missions. The development of a Comprehensive Approach 2.0 should start with an exchange of views amongst stakeholders about the nature of the challenge, rather than by focusing on the roles and missions of those participating. Reflecting on the experience of Afghanistan, one of the major challenges with developing a shared approach to bringing stability to the ground was the utilization of organizational and institutional roles and missions as the conversational starting point rather than the nature of the mission itself. As Michael J. Williams writes, "In the case of the NATO-UN-EU relationship in Afghanistan, we have a situation where bureaucratic concerns led to an increasingly rigid and ordered approach to a highly complex problem."[109] By walking into conversations with a focus on the

109 Williams, *The Good War*, 139.

authorities, roles, and missions of each actor operating in that theater, the important work of building a common view of the challenge was shortchanged. As a result, it became altogether too easy to fall back into old habits of bureaucratic posturing and infighting; the net result was that the whole, enormous effort was not equal to the sum of its parts. Looking forward to a Comprehensive Approach 2.0 to countering coercion, a key aspect of the challenge is that many of the stakeholders affected by political warfare strategies are not necessarily thinking about the national security dimensions of their activities. NATO could usefully organize strategic-level dialogues, workshops, and other exchanges with actors responsible for areas, including economic policy and domestic resilience, to share their perspectives on key dimensions of political warfare challenges. After the many viewpoints on these complex challenges are appropriately aired by key stakeholders, ideas can be developed on how to tackle them and who should do what.

Prioritize a "big tent" approach. As Beijing and Moscow are applying whole-of-society approaches to waging political warfare, so too must NATO think about how it can serve as a catalyst for whole-of-society approaches to countering coercion, particularly in nonmilitary spheres that have security implications.[110] Developing and executing a Comprehensive Approach requires that other actors understand NATO's value added in grappling with common challenges. In particular, NATO must continue to build networks of individuals in other stakeholder organizations that understand the role the Alliance plays in advancing Euro-Atlantic security. Private sector partnerships and civil society engagement are critical to the success of counter disinformation, cyber defense, and technological security efforts. NATO must increasingly build inroads with critical stakeholders and private sector players, and provide on-ramps for engagement in conversations, shared situational awareness, best practices, and alignment of mitigation policies.

NATO leaders must also promote an atmosphere in which the spirit of cooperation and collaboration is propagated at the national level with the private sector and civil society, and at the international level, amongst allies, NATO partners, and key multilateral organizations such as the EU. To accomplish this requires honest and objective assessments of internal and multinational capabilities, limitations, and redundancies, and—after understanding each other's views of the threat—clearly delineating the roles and responsibilities for each agency and partner within and outside of NATO.[111]

A Comprehensive Approach 2.0 as a process rather than a product. As Dwight D. Eisenhower once quipped, "In preparing for battle I have always found that plans are useless, but planning is indispensable."[112] This is because plans themselves often become irrelevant after making first contact with the enemy. By contrast, the act of developing a shared understanding of the threat and what can be done about it enables stakeholders to advance toward a common end even when the plans themselves become less relevant as circumstances change. Related, embracing a diversity of viewpoints and perspectives in the planning process is essential. In order to genuinely harness the diversity of views necessary to develop a meaningful Comprehensive Approach, NATO might consider developing more inclusive methods of, and methodologies for, counter-coercion planning. In this, positive leadership and inclusive management is essential. Far too often participants in multi-stakeholder meetings are treated as representatives of their institutions rather than as talented people with ideas to contribute—which hampers any group's ability to have the free exchanges of views and ideas that are essential for building collaboration.

Prioritize campaign continuity. The political warfare campaigns being waged by Moscow and Beijing are of long duration; NATO's response must take an equally long view of the challenge they present and how to contend with it. Fortunately, NATO is well suited to establish the processes and systems to prompt its member states—and other key stakeholders—to continually assess their progress and approaches to countering authoritarian coercion. In order to facilitate campaign continuity, NATO should prioritize the establishment of an institutional home within its headquarters in Brussels for knowledge management, stakeholder coordination, strategy development, and monitoring the execution of counter-coercion strategies. It should be noted that NATO is particularly well suited to this task as it can provide institutional memory and build campaign continuity even as leaderships of allied and partner states change.

Articulate a clear strategy for success, including how elements of a counter-coercion campaign interrelate with each other. The first Comprehensive Approach separated its goals into three tracks: political, security, and economic. The strategy was built so that progress in one track

110 On the point of "whole-of-society" approaches, see: Eric Edelman et al., *Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission*, *National Defense Strategy Commission*, *United States Institute of Peace,* November 13, 2018, https://www.usip.org/publications/2018/11/providing-common-defense.

111 Robert L. Caslen, Jr. and Bradley S. Loudon, "Forging a Comprehensive Approach to Counterinsurgency Operations," *Prism* 2 (3) (2011), https://apps.dtic.mil/dtic/tr/fulltext/u2/1042696.pdf.

112 Susan Radcliffe, ed., *Dwight D. Eisenhower 1890–1969 American Republican statesman, 34th President 1953–61*, Oxford Essential Quotations (4th ed.), https://www.oxfordreference.com/view/10.1093/acref/9780191826719.001.0001/q-oro-ed4-00004005.

reinforced that in another. For example, as the political process moved forward and terrorists become more isolated, there was better security, improved prospects of economic progress, and expanded political participation. The spectrum of political warfare challenges are interlinked, with cybersecurity impacting the information domain, impacting the environment for diplomacy, in turn impacting economic and energy security. NATO would benefit from a clear strategy with overlapping, interlinked, and mutually reinforcing goals for countering political warfare.

Build effective indicators and benchmarks—and adapt as necessary. As a starting point for planning, an overall vision of success—guided by foreign ministers and heads of state and government—must be established that enables working-level planners to develop measures of success and, crucially, indicators of failure in the political, security, and economic dimensions of statecraft.

It is important to note that progress in countering coercion is inherently iterative and nonlinear, which means that standard approaches to campaign planning and metric developments might not be appropriate. Critically, there must be a way to provide routine feedback to foreign ministers and heads of state and government on successes and shortfalls in NATO's approach to countering authoritarian coercion and discern their further guidance—processes that NATO is well suited to provide. In the first Comprehensive Approach, numerous indicators mapped out the progress of the strategy, allowing for changes when necessary. Detailed reports were issued weekly, monthly, and quarterly by relevant agencies and participating parties. In establishing a Comprehensive Approach 2.0, NATO should set clear benchmarks and indicators and a mechanism to assess and update success. The Alliance must set itself up to self-correct as more information is revealed about Chinese political warfare and as competitors' tactics change and evolve, while having the ability to absorb new allied capabilities into response plans. To ensure accountability, as well as to harness the political and strategic acumen of foreign ministers, NATO should submit reports on the development and implementation of the Comprehensive Approach 2.0 for review at its foreign ministerial meetings.

Incorporate political-level identification and punishment into deterrence strategies. For deterrence to succeed, a relationship between an "imposer" and "target" must be 1) definable and 2) contained by rational behavior. With political warfare it is difficult to identify the target, complicating the ability of the imposer to effectively punish. If a nation or organization cannot 1) swiftly identify and 2) severely punish a bad actor, it will act based on calculated risks. While NATO allies have worked to identify and attribute malign behaviors to Russia and China in some areas, they might usefully ramp up their ability to do so and leverage name-and-shame campaigns. NATO must make imposing costs on actors waging political warfare a critical element of its counterstrategy. A more robust playbook of potential NATO responses to political warfare would help allies and partners determine how best to respond in the event of a coercive attack.

Recognize the limitations of the Comprehensive Approach. All too often, policy makers and practitioners became frustrated that the Comprehensive Approach to operations on the ground in Afghanistan failed to deliver common action and results. Yet differing institutional priorities, risk calculations, and resources amongst stakeholders meant that the kind of common action that many (particularly in the military) expected was never achievable. Nor was that the point of the Comprehensive Approach. Unity of command is not possible in these contexts. Rather, the Comprehensive Approach is best thought of as a mechanism to create space for communication, discussion, and collaboration amongst many stakeholders, which constitutes an important contribution to the NATO and partner ability to contend with current and emerging challenges stemming from authoritarian coercion strategies.

Possible Action Items for a Comprehensive Approach 2.0

With the above principles in mind, to get started on developing a Comprehensive Approach to countering authoritarian coercion, NATO, member states, and partner nations might consider the action items listed below. An important caveat should be noted: this list is meant to be *illustrative* of the kinds of issues and initiatives with which a NATO Comprehensive Approach 2.0 agenda embedded under Article 2 might grapple—not a prescription. This is because a meaningful and effective Comprehensive Approach 2.0 agenda must grow organically out of consultations and discussions amongst stakeholders, not be directed from an external group that is disconnected from such discussions. Still, the below list is intended to help decisionmakers build their own ideas for what might be usefully explored as part of a Comprehensive Approach 2.0.

- **Convene a task force to develop an Article 2 strategy.** As noted above, Article 2 has long been seen as a statement of values rather than a strategic blueprint for Alliance-wide action. Yet viewed through the lens of political warfare, Article 2 provides the Alliance with a useful framework to counter authoritarian coercion. Translating the strategic intent laid out in 1949 into a concrete vision and objectives for the Alliance today will take the time and effort of a dedicated group of scholars and practitioners—and considerable consultation among allies, partners, and other governmental and nongovernmental actors. The secretary general might consider utilizing the "Senior Officials Group"

model for such an endeavor, with an important caveat: in order to build a more holistic view of the problem set, diverse, younger voices from nontraditional communities might be prioritized for participation alongside more senior voices in the establishment of such a panel.

Exterior view of the new NATO headquarters. *Source:* NATO/flickr

- **Give countering coercion activities an institutional home.** In order to move from political consensus to action and implementation, NATO should decide which entity within the Alliance should be the institutional home for the Comprehensive Approach 2.0 efforts. Different parts of the Alliance may lead on different aspects—for example, NATO's PDD on counter-disinformation—but NATO requires a coordinating function to be placed somewhere. The placement of a directorate with this mission within NATO's bureaucracy should be at the secretary general's discretion; in order to be effective, it must be sufficiently empowered to serve as a focal point for Alliance-wide efforts on countering political warfare—without incurring unnecessary bureaucratic turf battles—and staffed and resourced accordingly. NATO's secretary general is best placed to identify where such a directorate might best integrate within NATO headquarters staff, for example the Political Affairs and Security Policy Division, and who ought to lead such a Counter-Political Warfare Directorate. Further, in order to ensure that the individuals that will be tasked with operationalizing the Comprehensive Approach 2.0 are well versed in the contours of debates surrounding the development of an Article 2 strategy, the directorate should, at a minimum, staff—if not participate in—Article 2 task force activities. While adding to the headquarters' staff (and, therefore, NATO's budget) will require additional financial resources, the stakes and the increasing risks associated with insufficient action on political warfare mean that it is worth paying the comparatively small fiscal amount needed to stand up such an office.

- Once a coordination function is established, the **North Atlantic Council should establish a Comprehensive Approach 2.0 agenda**, to be coordinated and overseen by the Counter-Political Warfare Directorate. The directorate would serve as NATO's institutional focal point for strategic-level coordination and consultation on authoritarian political warfare matters amongst key stakeholders from across the Alliance, partner nations, and nongovernmental actors from the private sector and civil society. To facilitate cross-headquarters information sharing, NATO committees and divisions—across issues like political affairs, intelligence, defense policy and planning, security, civil emergency, partnerships, operations, and elsewhere—could be asked to appoint representatives to participate in convenings to share information and strategies, as well as feed relevant counter-political warfare insights back into their own committees and divisions.

- To more comprehensively contend with predatory economic practices and coercive diplomacy by Russia and China, **NATO allies and partners should coordinate assessments of risk areas within the transatlantic community**. They should also begin discussions about how to integrate their perspectives and offer alternative lending and investment opportunities to both each other as well as other states that are victims of predatory lending, especially for critical infrastructure projects. Working with the EU, NATO allies and partners might create a funding mechanism like an investment fund which pools allied resources and promotes private sector investment. The fund would be used to provide an alternative for nations and regions that are turning to Chinese and Russian banks and lending institutions.

- At a national level, **allies and partners could follow the example set by the UK by creating national interagency hybrid Fusion Centers** to improve national responses to political warfare. Currently, coordination on countering political warfare could be enhanced—even at the national level within many governments of allies and partners. The lack of national-level situational pictures prevents countries from engaging as effective

actors in multinational efforts, and, therefore, national coordination must be prioritized as a necessary prerequisite for more advanced multinational coordination. The establishment of national Fusion Centers should involve members from multiple government agencies and provide a regular engagement option with private sector actors. Their main function could be to serve as a pool of information to enhance national pictures of the full spectrum of hybrid challenges facing the nation. On a multinational level, delegates from each national Fusion Center should actively engage in multinational CoEs, like Finland's Hybrid CoE and NATO's StratCom COE, to share best practices from a national level with other allies and partners.

- **NATO allies and partners should consider adopting Fusion Doctrines and Cross-Domain Response Frameworks** to better utilize all national instruments of power effectively against political warfare. These doctrines should be used by each nation to conduct a net assessment of the statecraft tools at their disposal and promote whole-of-government responses to political warfare. Fusion Doctrines should be adopted by NATO allies to enable more creativity in responding to hybrid attacks, including expanding the response options considered by empowering different agency responsibilities and engagement. NATO allies and partners should also consider developing national Cross-Domain Response Frameworks that outline graduated response options to political warfare attacks (for example, in response to a cyberattack on critical infrastructure, we could respond in X and Y ways in the following domains or theaters, in such a way that we deem to be proportionate.) The framework should be developed across the country's interagency and outline, ahead of time, the types of appropriate offensive and defense responses at the country's disposal and which actions would be appropriate to achieve deterrence and defense and in what scenarios. The framework should build in the flexibility to respond in one domain to an attack in another, thereby expanding the choice of options to respond to political warfare. Such a Cross-Domain Response Framework could be discussed in concept in either the new Counter-Political Warfare Directorate (or wherever NATO determines is best suited to the task). The development of these national Cross-Domain Response Frameworks should enable allies and partners to share best practices and build shared understandings of appropriate and effective counter-political warfare responses that achieve deterrence and punishment.

- **NATO should develop a Playbook for Countering Political Warfare** to be discussed and shared across the Alliance and with partners. Such a playbook would build on the Cross-Domain Response Frameworks developed nationally, and would help build Alliance-wide consensus and serve as a guide outlining what types of attacks in the hybrid domain would trigger what kinds of responses from NATO allies. The aforementioned Counter-Political Warfare Directorate could take the lead on discussions and drafting a playbook with the assistance of NATO's PDD. Establishing a playbook would enable allies and partners to prepare and think through response options ahead of time and improve more coordinated Alliance-wide responses when hybrid attacks occur. Planning for the known unknowns will be a critical activity. A playbook should explore offensive capabilities and (pro)active defense in the cyber realm and perhaps beyond. As a first step, experimentation and wargaming will be key to furthering understanding of political coercion scenarios and potential responses and should be used to build shared assessments of the security landscape, threat perceptions, and a consensus of response.

- NATO allies and partners should **streamline their approaches to disinformation, including adopting national education programs to teach media and online literacy**. Programs like those in partner countries like Finland should be used as a model to bolster societal resilience against disinformation and mitigate the effectiveness of such campaigns by hardening public receptiveness to falsehoods. NATO should also develop an Alliance-wide disinformation Rapid Response Unit (RRU) like the UK's national unit to help align strategic communications and assist allies in prioritizing key information to ensure it remains highly visible among NATO publics. This RRU may fall under the purview of the aforementioned, newly created directorate.

- Nationally, **all NATO allies and partners should develop a version of a Total Defense Concept** tailored to each nation's vulnerabilities and strengths, in order to build societal resilience to coercion and political warfare. A NATO Defense Planning Process-style concept could be institutionalized across the Alliance in order to measure and report on societal resilience and defense planning for counter-political warfare. This approach would encourage national planners to raise key issues in the security, economic, and political spaces that may have an impact on counter-hybrid warfare strategies. Such a mechanism may encourage allies to regularly set goals for societal resilience and total defense across sectors, establish mechanisms to measure resilience, and encourage investments in counter-political warfare mechanisms and below-threshold threats.

Conclusion

Forging common approaches among NATO allies and partners on political warfare is no easy task. Political warfare is a complex beast; by design it is hard to notice, identify, call out, and grapple with. There is a reason that allies and partners, for now, have largely approached political warfare as distinct issues—including disinformation, election interference, political coercion, and economic pressure—with varying degrees of effort and success. It is challenging to put our heads around the entirety of the problem set. Nevertheless, the very nature of the problem is that it is cross-cutting, interlinked with other types of warfare and tools, and that it plays out and pulls levers in multiple actors' jurisdictions. For that reason, and for NATO to really grapple with political warfare—to achieve deterrence, mitigation, management of the effects, and to mute the impact—it must tackle the whole, holistically and comprehensively. It is helpful that NATO has both an Article 2 Washington Treaty strategic mandate and operational experience and lessons learned to help allies and partners grapple with these challenges.

Indeed, NATO has tackled multi-sector, multi-actor problems before; its prior Comprehensive Approach in Afghanistan and Iraq provides a robust framework to forge a collective and effective response to political warfare. A Comprehensive Approach 2.0 would enable NATO to bring together multiple layers of actors, including government agencies (defense, foreign affairs, treasury, homeland security, law enforcement, etc.); the public, civil society, and private sector actors; NATO member states and partner nations; and different multinational institutions like the EU and the UN. Such groups can work to forge a multi-vector approach to threat assessments of, consensus building on, and coordinating responses to Russian, Chinese, and other authoritarian political warfare. Partners across multiple countries and sectors are critical to the success of a Comprehensive Approach 2.0 and enable NATO to extend its understanding, situational awareness, and learn best practices from others.

The urgency of this problem should not be understated. While NATO allies and partners are coming to grips with aspects of Russian and Chinese political warfare tactics, they have fallen behind and remain on the back foot in effectively responding to this challenge. NATO is still not far enough along in recognizing threats in existing and emerging areas like predatory economic practices and subversive energy investments. Allies and partners' approaches to hybrid warfare, while laudable for their developments in some areas of disinformation and cyber defense, have overall been insufficient to match the evolution of the threat landscape. NATO's current approaches to hybrid warfare can be stiflingly broad, preventing effective tailoring of strategies to match the threat. There is still an overreliance on NATO's military arm and a lack of focus and intent on how to employ its political toolkit and nonmilitary competencies.

Ultimately, a strategic shift is needed within NATO for the Alliance to play a more advanced role in countering political warfare, enabled by its Article 2 mandate. A utilization of NATO's nonmilitary actors, toolkit, and responses will enable a more nimble and effective Alliance posture to the political warfare side of the hybrid spectrum. As China, Russia, and other authoritarian actors seek to thwart international institutions from within and undermine them from the outside, this is an urgent problem. Mitigating political warfare over the next decade will be critical to upholding the value and integrity of the very institutional underpinnings that provide security for transatlantic peoples. It is the only way for NATO to avoid the sad fate of the orb spider and build resilience against the coopting and subversion of the liberal world order upon which our shared security relies. In other words, NATO must protect the transatlantic web. NATO has managed challenges like this before. With the right strategic focus and approach it can more effectively counter political warfare and forge a more secure future for like-minded allies and partners.

About the Authors

Kathleen J. McInnis is an author and nonresident senior fellow at the Atlantic Council's Scowcroft Center for Strategy and Security. From 2006 to 2009, she served in the Office of the Undersecretary of Defense for Policy, working primarily on NATO's Afghanistan operations. Prior to that, she was a research consultant at Chatham House in London, where she worked on NATO and transatlantic security matters. McInnis also served in the Office of the Secretary of Defense (Policy), working NATO-Afghanistan matters and stability operations capability development. Prior to joining the Pentagon, McInnis spent several years at the Center for Strategic and International Studies (CSIS) analyzing US nuclear weapons strategy, strategic capabilities, NATO, European security, and transatlantic relations. Before joining CSIS, she was a researcher in the United Kingdom's House of Commons, working on NATO, the European Union, and US-UK political-military relations.

McInnis has commented on international affairs on television, radio, and print. She has appeared on CNN, Sky News, BBC, Al Jazeera English, and Voice of America. She is the author of dozens of reports and articles on international security matters; her work has been featured in publications, including the *Atlantic*, *Defense One*, *Foreign Policy*, the *Washington Quarterly*, *Defense News*, *War on the Rocks,* and the *Washington Times*. She was also a contributing author to several Chatham House and CSIS studies. She was awarded her MSc in international relations from the London School of Economics in 2002, and completed her PhD in the Department of War Studies, King's College London, in 2017. Her book on coalitions, *How and Why States Defect from Contemporary Military Coalitions*, was published by Palgrave in 2019. McInnis is also the author of the novel *The Heart of War: Misadventures in the Pentagon* (Post Hill Press, 2018) and a contributing author to edited volumes, including *War Time: Temporality and the Decline of Western Military Power* (Brookings/Chatham House Press 2021), *To Boldly Go: Leadership, Strategy, and Conflict in the 21st Century and Beyond* (Casemate, forthcoming), and *Strategy Strikes Back: What Star Wars Teaches Us About Modern Military Conflict* (Potomac Press 2018).

Clementine G. Starling is the deputy director of *Forward* Defense and resident fellow of the Transatlantic Security Initiative at the Atlantic Council. In her role, she oversees the initiative's programming and research and leads on the defense policy and European security practice areas. Her own research focuses on great-power competition with China and Russia, deterrence and US force posture, and transatlantic security. During her time at the Atlantic Council, Starling has produced and contributed to reports on Russia's nuclear strategy, space security, military mobility, political warfare, Europe-China relations, and the US-UK relationship. Starling's analysis has been featured in a range of publications, and she has provided commentary for NPR, the BBC, and ABC News, among others. Within the Transatlantic Security Initiative team, she played a leading role in managing NATO's official public diplomacy efforts ("NATO Engages") around the Alliance's 2019 London Leaders' Meeting and other summits. Starling was also the 2020 Security and Defense fellow at Young Professionals in Foreign Policy (YPFP). Prior to joining the Atlantic Council, Starling worked in the UK Parliament with the House of Commons Defence Select Committee, providing analysis on UK defense, Middle East security, and technology. Originally from the United Kingdom, she also worked for the Britain Stronger in Europe (BREMAIN) campaign. She graduated with honors from the London School of Economics with a Bachelor of Science in international relations and history.

This report was produced by the two authors in accordance with the Atlantic Council's policy on intellectual independence. All views expressed in this report are solely those of the authors and do not in any way represent the institutions with which they are affiliated.

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*Richard W. Edelman
*C. Boyden Gray
*Alexander V. Mirtchev
*John J. Studzinski

TREASURER
*George Lund

DIRECTORS
Stéphane Abrial
Todd Achilles
*Peter Ackerman
Timothy D. Adams
*Michael Andersson
David D. Aufhauser
Barbara Barrett
Colleen Bell
Stephen Biegun
*Rafic A. Bizri
*Linden P. Blue
Adam Boehler
Philip M. Breedlove
Myron Brilliant
*Esther Brimmer
R. Nicholas Burns
*Richard R. Burt
Teresa Carlson
James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
Beth Connaughty
*Helima Croft
Ralph D. Crosby, Jr.
*Ankit N. Desai
Dario Deste
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Thomas R. Eldridge
Mark T. Esper
*Alan H. Fleischmann
Jendayi E. Frazer
Courtney Geduldig
Meg Gentle
Thomas H. Glocer
John B. Goodman
*Sherri W. Goodman
Murathan Günal
Amir A. Handjani
Frank Haun
Michael V. Hayden
Amos Hochstein
Tim Holt
*Karl V. Hopkins
Andrew Hove
Mary L. Howell
Ian Ihnatowycz
Wolfgang F. Ischinger
Deborah Lee James
Joia M. Johnson
*Maria Pica Karp
Andre Kelleners
Henry A. Kissinger
*C. Jeffrey Knittel
Franklin D. Kramer
Laura Lane
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mark Machin
Mian M. Mansha
Marco Margheri
Michael Margolis
Chris Marlin
William Marron
Gerardo Mato
Timothy McBride
Erin McGrain
John M. McHugh
Eric D.K. Melby
*Judith A. Miller
Dariusz Mioduski
*Michael J. Morell
*Richard Morningstar
Georgette Mosbacher
Dambisa F. Moyo
Virginia A. Mulberger
Mary Claire Murphy
Edward J. Newberry
Thomas R. Nides
Franco Nuschese
Joseph S. Nye
Ahmet M. Ören
Sally A. Painter
Ana I. Palacio
*Kostas Pantazopoulos
Alan Pellegrini
David H. Petraeus
W. DeVier Pierson
Lisa Pollina
Daniel B. Poneman
*Dina H. Powell McCormick
Robert Rangel
Thomas J. Ridge
Gary Rieschel
Lawrence Di Rita
Michael J. Rogers
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Ivan A. Schlager
Rajiv Shah
Kris Singh
Walter Slocombe
Christopher Smith
Clifford M. Sobel
James G. Stavridis
Michael S. Steele
Richard J.A. Steele
Mary Streett
*Frances M. Townsend
Clyde C. Tuggle
Melanne Verveer
Charles F. Wald
Michael F. Walsh
Gine Wang-Reese
Ronald Weiser
Olin Wethington
Maciej Witucki
Neal S. Wolin
*Jenny Wood
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Ashton B. Carter
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Colin L. Powell
Condoleezza Rice
Horst Teltschik
William H. Webster

**Executive Committee Members*

List as of June 1, 2021

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor, Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org