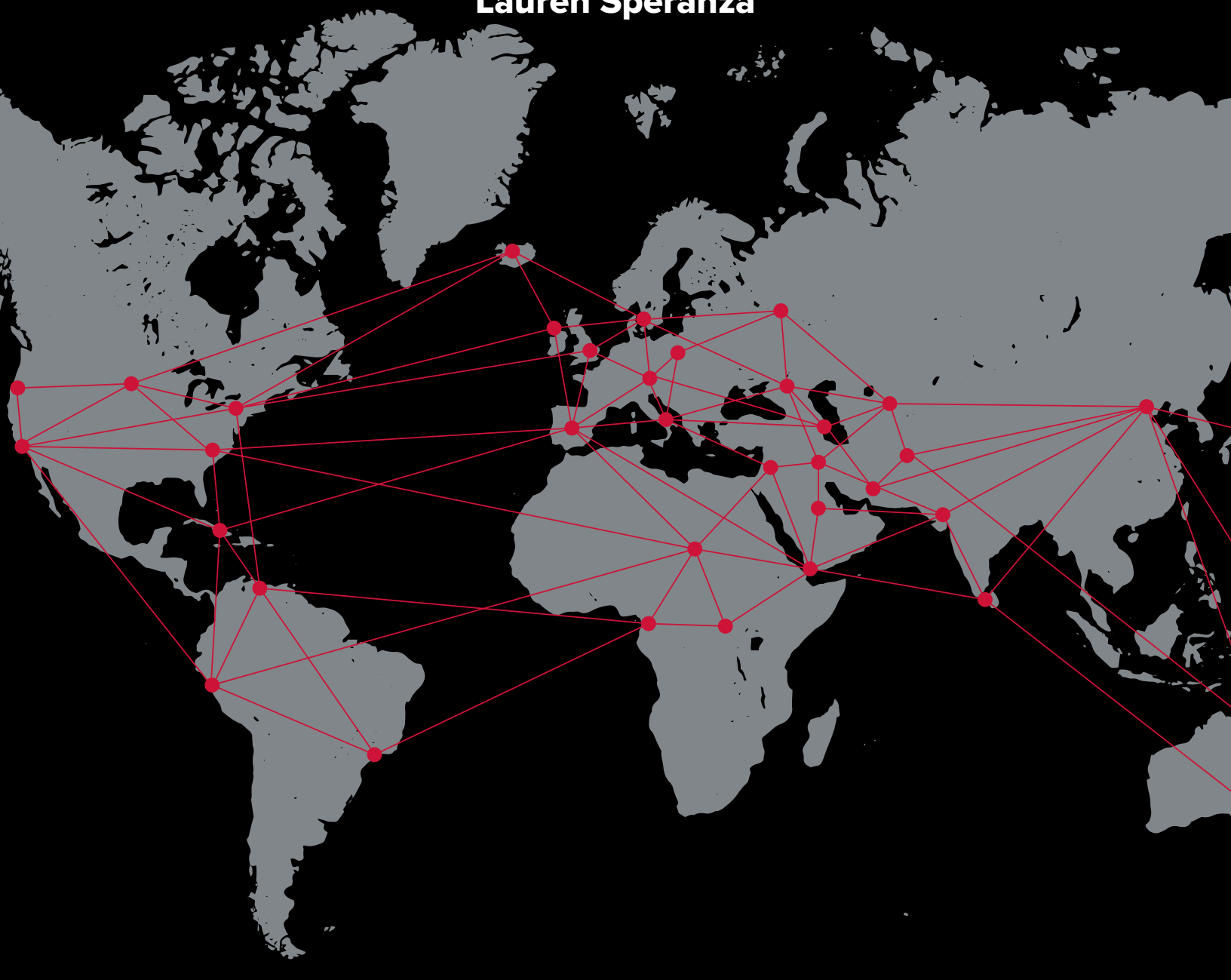
Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

A Strategic Concept for Countering Russian and Chinese Hybrid Threats

Lauren Speranza



Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

Scowcroft Center for Strategy and Security

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.

Transatlantic Security Initiative

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 report was produced as part of the Transatlantic Security Initiative's work focused on hybrid threats in partnership with the Ministry for Foreign Affairs of Sweden.

A Strategic Concept for Countering Russian and Chinese Hybrid Threats

Lauren Speranza

ISBN: 978-1-61977-103-1

Cover: World map by vecteezy.com

July 2020

Table of Contents

Executive Summary

Tackling hybrid threats, particularly from state actors such as Russia and China, remains one of the greatest challenges for the transatlantic community. Hybrid threats have gained more traction among policymakers and publics across Europe and the United States, especially in a world with COVID-19. The recent coronavirus pandemic has thrust hybrid activities to the center of transatlantic debates. Both China and Russia capitalized on the crisis to wage disinformation campaigns against the West, while strategically delivering aid to European countries in attempts to build good will on the international stage. Yet, even as hybrid activities have accelerated, limited progress has been achieved in countering them or deterring competitors from using them. Over the last five years, Euro-Atlantic nations and institutions, such as NATO and the European Union (EU), have taken important steps to respond to hybrid issues. But as hybrid threats become more prominent in the future, policymakers must move toward a more coherent, effective, and proactive strategy for countering Russian and Chinese hybrid threats.

To develop such a transatlantic counter-hybrid strategy for Russia and China, this paper argues that two major things need to happen. First, transatlantic policymakers have to build a common strategic concept to guide collective thinking on hybrid threats. The paper offers five strategic priorities that could form the basis of this strategic concept.

1) **Redefine the conceptual framework for hybrid threats.**

2) **Forge a common, in-depth understanding of the impact of hybrid activities.**

3) **Articulate clear strategic goals for countering hybrid threats.**

4) **Adopt a more proactive, campaign approach to counter-hybrid.**

5) **Build clear parameters to support joint attribution and action.**

Second, transatlantic policymakers need to take a range of practical actions in service of that strategic concept. The paper concludes by recommending a series of constructive steps—each corresponding with one of the strategic priorities above—that NATO, the EU, and nations can take, in cooperation with the private sector and civil society, to enhance their counter-hybrid capabilities against Russia and China.

To help redefine the conceptual framework for hybrid threats

- selectively decouple relations with Russia and China in specific sectors to discourage hybrid behavior; and
- create a new platform for cooperation between NATO, the EU, their nations, and the private sector.

To help forge a common, in-depth understanding of the impact of hybrid activities

- increase transparency and information sharing around Russian and Chinese hybrid activities;
- stand up national hybrid fusion centers; and
- conduct hybrid campaign analysis.

To reinforce strategic goals for countering hybrid threats

- invest in civic education, media training, and civil preparedness;
- produce key messages in different languages; and
- provide guidance to the private sector to support counter-hybrid goals.

To support a more proactive, campaign approach to counter-hybrid

- clarify counter-hybrid standard operating procedures (SOPs);
- pair highly capable nations with less capable nations to build counter-hybrid capacities;
- review resource allocation periodically to support the most effective counter-hybrid capabilities; and
- create new legislation and keep it up to date.

To support joint attribution and action

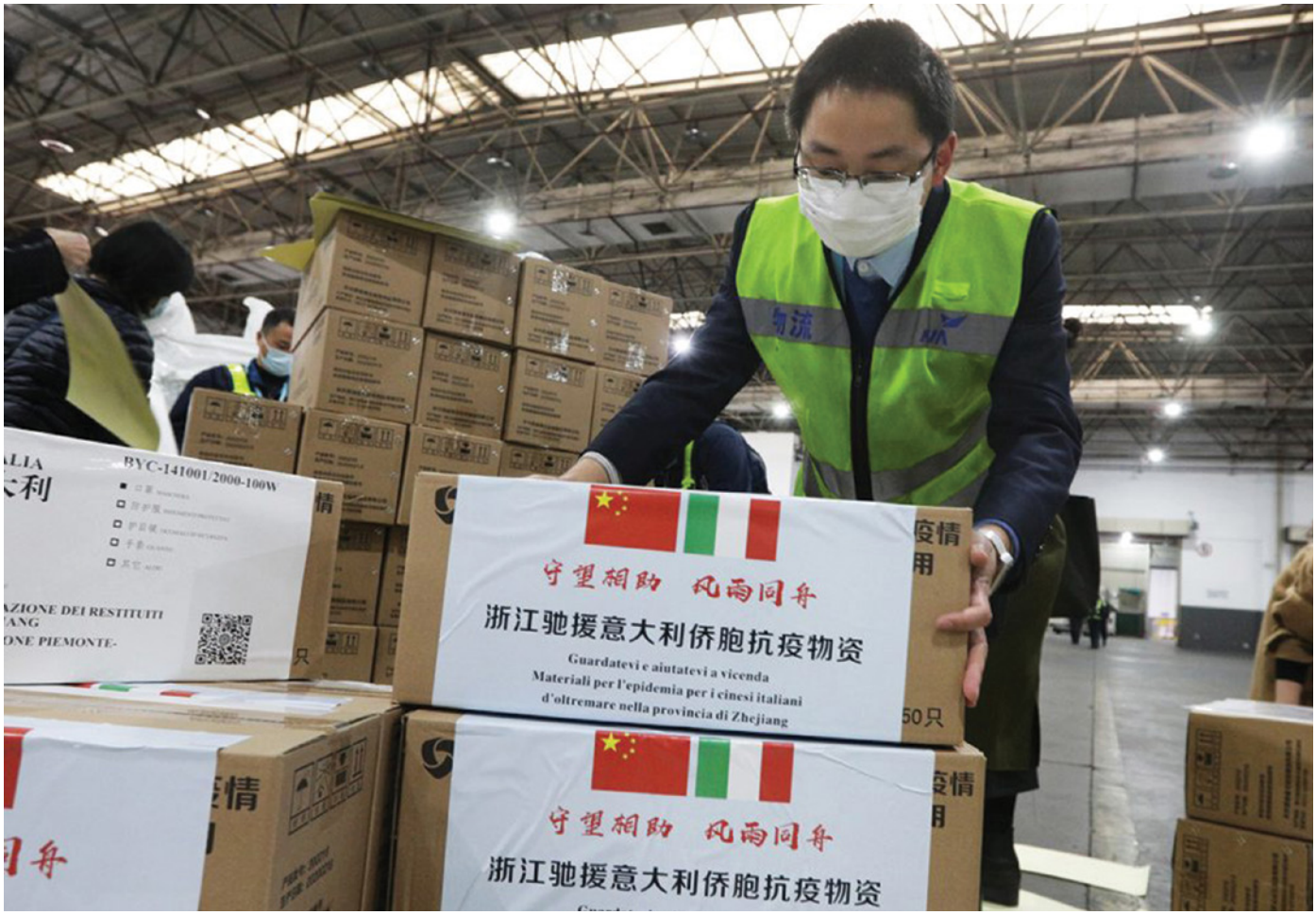
- leverage emerging technologies, such as artificial intelligence; and
- conduct national interagency exercises based on real hybrid scenarios.

Introduction

Managing hybrid threats remains one of the greatest challenges for the transatlantic community. Hybrid threats have gained more traction and visibility in policy debates and news headlines—and among publics across Europe and the United States—in a world with COVID-19. The recent coronavirus pandemic has highlighted the transatlantic community's vulnerabilities to a range of hybrid issues—from manipulation of global supply chains to biowarfare to disinformation. Yet, even as the transatlantic community has witnessed these challenges, limited progress has been achieved in effectively countering these threats. Euro-Atlantic nations and institutions, such as NATO and the European Union (EU), have certainly made important strides to respond to hybrid issues. Collective approaches, however, have been reactive, falling short of deterring adversaries from using hybrid actions. Recognizing the many constraints and challenging nature of hybrid activities, this paper argues that the transatlantic community can, and should, do more to enhance its counter-hybrid strategy.

While the term "hybrid" can be debated and defined in many ways, this paper refers to hybrid as an approach that blends conventional and unconventional, overt and covert, kinetic and non-kinetic, and military and nonmilitary means to undermine a target and achieve the perpetrator's political and strategic goals.

Hybrid threats can stem from many actors, but this analysis focuses on hybrid threats primarily as a result of deliberate and persistent actions by state actors, notably Russia and China. Russian and Chinese hybrid activities involve a mix of diplomatic, economic, security, information, and technological actions designed to quietly undermine democratic



Medical supplies to be sent to Italy for the prevention of the novel coronavirus at a logistics center of the international airport in Hangzhou, China on March 10, 2020. *Photo: China Daily via REUTERS*

states and institutions to Moscow's or Beijing's benefit while avoiding a traditional conflict. These state-sponsored hybrid activities are among the most pressing challenges for the transatlantic community. This analysis conceptualizes hybrid activities in four categories: below-threshold conflict or use of force (e.g., from kidnappings to assassinations to bioweapons); cyber and related operational attacks (e.g., on critical infrastructure); political subversion and economic coercion; and information operations.[1] The paper that follows looks at these hybrid threats as they relate to transatlantic countries, including the United States and the members and closest partners of NATO and the EU.

Indeed, traditional security concerns, such as nuclear weapons and conventional defense and deterrence, will not go away for the transatlantic community. Yet, going forward, transatlantic nations and institutions will increasingly need to focus on hybrid and nontraditional threats too.[2] This is particularly underscored by the 2020 coronavirus crisis, in which both Russia and China have played various roles. Both China and Russia capitalized on the crisis to wage disinformation campaigns against the West. They promulgated conspiracy theories designed to sow fear about America's handling of the outbreak and to promote the successes of their own authoritarian regimes. Moscow and Beijing also strategically delivered aid and medical supplies to European countries in attempts to build good will and clout on the international stage. These issues cannot be effectively addressed alone or in a vacuum, making global cooperation and collective action—especially among transatlantic allies—paramount. Even as transatlantic nations and institutions shift priorities in the wake of the coronavirus crisis, key counter-hybrid priorities, such as building resilience, strengthening civil response capacities, and investing in civic education, simultaneously serve priorities for pandemic prevention and response. This is all the more reason to prioritize the counter-hybrid agenda.

> "At its heart, the paper offers five strategic priorities that could form the basis of a new strategic concept to guide transatlantic thinking on hybrid threats."

To that end, this paper outlines steps for transatlantic policymakers to move toward a more coherent, effective, and proactive strategy for countering Russian and Chinese hybrid threats. At its heart, the paper offers five strategic priorities that could form the basis of a new strategic concept to guide transatlantic thinking on hybrid threats. It concludes with several practical recommendations that nations and institutions should undertake in service of that strategic concept.

Threat Environment

Over the past five years, hybrid activities targeting the Euro-Atlantic community have increased in size, scope, and intensity. From growing foreign interference in US and European elections to looming concerns of manipulation of fifth-generation (5G) infrastructure, hybrid threats have increasingly captured the headlines and the attention of top policymakers. Among transatlantic countries, there has also been a growing recognition that—in addition to Russia, whose hybrid activities are well understood—China poses serious hybrid challenges, albeit in somewhat different ways. This diversification of the threat environment requires a recalibration of the transatlantic approach, based on an in-depth understanding of the motivations behind, the nature of, and the similarities and differences between Russian and Chinese hybrid activities.

Russian Hybrid Activities

For Russia, hybrid warfare is a set of means for it to roll back the post-Cold War settlement and undermine the predominantly US-led, rules-based international order to regain clout as a major player on the global stage. The Kremlin's key objectives to that end include: dividing and weakening NATO and the EU, both of which the Kremlin sees as a threat; subverting pro-Western governments and institutions; promoting pro-Russia policies; expanding Russia's sphere of influence (geographically, economically,

1 "Below-threshold" refers to the threshold of armed attack, e.g., NATO's Article 5, the European Union's Article 42.7, and the United Nations' Article 51. See Franklin D. Kramer and Lauren Speranza, *Meeting the Russian Hybrid Challenge: A Comprehensive Strategic Framework, Atlantic Council,* May 2017, https://www.atlanticcouncil.org/in-depth-research-reports/report/meeting-the-russian-hybrid-challenge/.

2 For more on NATO's role in these types of crises, see Lauren Speranza, "Six Reasons NATO's Euro-Atlantic Disaster Response Coordination Centre is Important for our Future Security," *New Atlanticist*, April 7, 2020, https://www.atlanticcouncil.org/blogs/new-atlanticist/six-reasons-natos-euro-atlantic-disaster-response-coordination-centre-is-important-for-our-future-security/.

politically, etc.); and establishing a "moral equivalence" between Russia and the West.[3] Moreover, hybrid activities help the Kremlin pursue these goals in a more effective and realistic way. Its leaders recognize Russia cannot necessarily counter or outright compete with the West militarily, technologically, or economically. By employing hybrid methods as part of an overarching strategy of intimidation, however, the Kremlin can have significant influence over international affairs.[4]

Russia's hybrid toolkit is multi-level and often country specific, which has made it highly effective and difficult to combat. In its most widely known example, Russia used below-threshold force to illegally invade eastern Ukraine and annex Crimea. The Kremlin has also used proxies and privately contracted forces to influence the outcome of conflicts abroad, from Syria to Libya. Other examples of Russia's low-level uses of force include attempted assassinations of pro-Western leaders and the use of deadly chemical attacks to target political enemies on foreign soil. In terms of cyber and operational activities, Russia has conducted reckless and dangerous cyberattacks, infiltrated critical infrastructure in the United States, and manipulated gas pipelines, electric grids, and financial systems in Eastern Europe and beyond to increase its leverage abroad.

With respect to political subversion and economic coercion, Russia has interfered in elections in the United States and across Europe in attempts to divide transatlantic populations and influence the outcomes toward candidates the Kremlin views as favorable to Russia. Other tools and tactics include: bribing officials in foreign countries; financing anti-European parties in Central and Eastern Europe to promote pro-Russian narratives; and investing in strategic sectors in foreign countries to maximize dependency on Russia. On the information-warfare front, the Kremlin has orchestrated widespread disinformation campaigns and strategic hack-and-release efforts designed to sow doubt, create chaos, and sway public opinion in its favor on key policy issues.

While Russian hybrid activities can be traced much further back than these examples—including to the major cyberattacks in Estonia in 2007 and the Russo-Georgia conflict in 2008—they have been steadily increasing since the Kremlin's illegal annexation of Crimea in 2014. Looking ahead, several elements could impact the future course of Russia's hybrid actions. First are the constitutional changes that Russian President Vladimir Putin has pushed through national courts to reset presidential term limits.[5] The reforms allow Putin to remain in power until 2036, or possibly for life, pending a final national referendum.[6] With his grip on power soon to be cemented, Putin is likely to attempt more aggressive hybrid actions, knowing the domestic political risks for him are low.

Another factor is the 2020 coronavirus pandemic, which has triggered a global recession and a drastic decline in demand for oil so critical to Russia's energy-reliant economy. In early 2020, Russia and Saudi Arabia, the world's biggest crude producers, failed to agree to mutual production cuts in response to the crisis, fueling a price war that further hurt Russia's economy.[7] Economic, public health, and social pressures inside Russia could push the Kremlin to temporarily scale back its ambitions in the short term. However, at the same time, uncertainty and anxiety around the pandemic could create more fertile conditions for Russia's hybrid activities beyond its borders, especially as Euro-Atlantic governments take extraordinary domestic measures to respond.[8] In the long term—even as the pandemic subsides, oil prices rebound, and the global economy begins to recover—conditions will remain difficult for Russia, whose economy has suffered from stagnation and sanctions from the West. These dynamics may lead Putin to be more assertive with hybrid strategies abroad with the aim of appealing to nationalist sentiments at home in order to quell domestic political tensions.

3 Some experts argue this strategy stems from Valery Gerasimov's New Generation Warfare doctrine of 2013, while others posit that the Gerasimov doctrine was just a particularly compelling articulation of what Russia's strategy has historically been. Regardless of the origin, it is clear that this overarching set of ideas guides the Kremlin's goals and tactics. For more, see General Valery Gerasimov, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations," *Voyenno Promyshlennyy Kurier*, February 26, 2013, http://vpknews.ru/articles/14632; and, for example, Keir Giles, "Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power," Chatham House, March 2016, https://www.chathamhouse.org/publication/russias-new-tools-confronting-west.

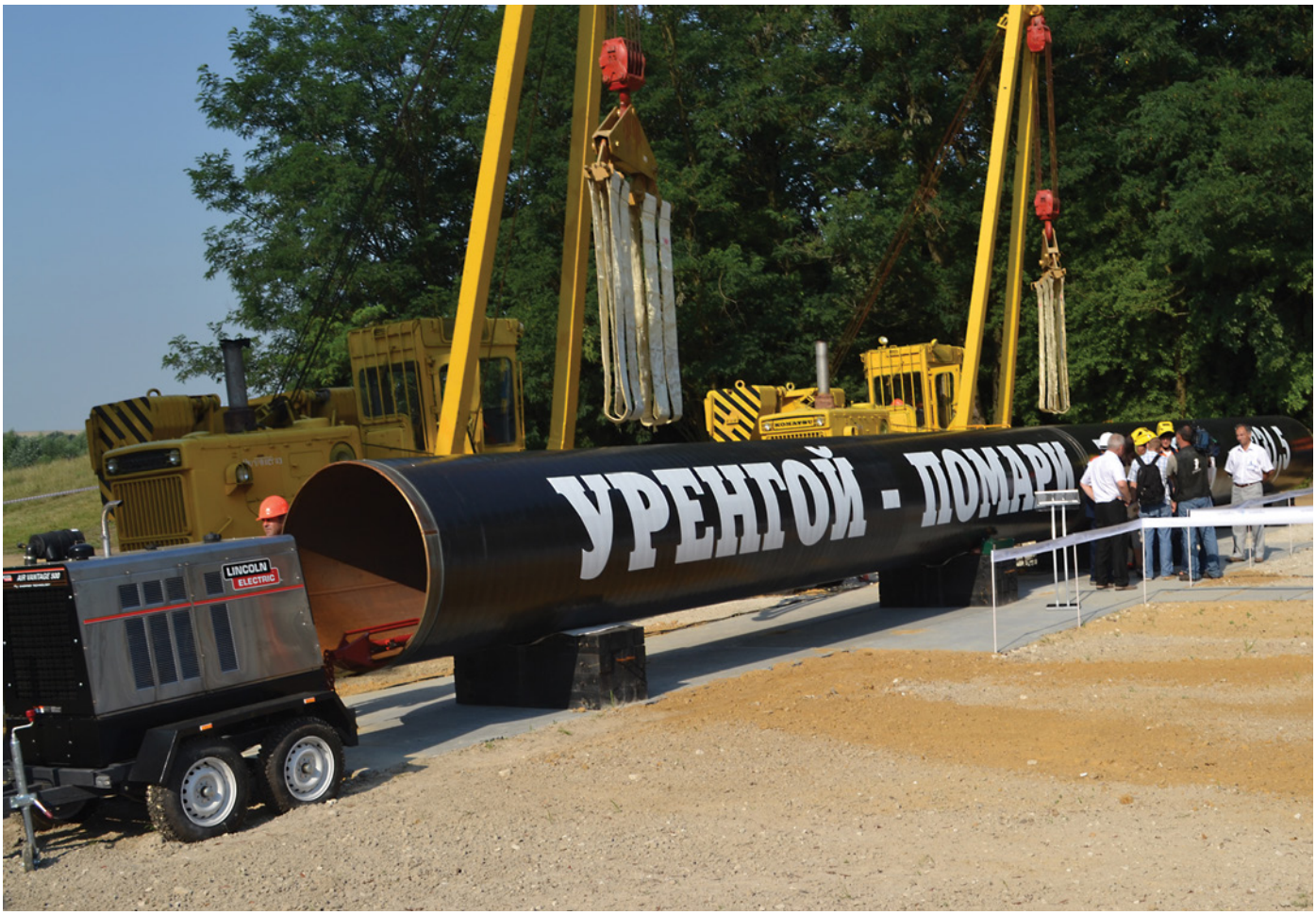
4 For more on Russia's hybrid activities, see, for example: Alina Polyakova, et al., *The Kremlin's Trojan Horses 2.0, Atlantic Council,* November 15, 2017, https://www.atlanticcouncil.org/in-depth-research-reports/report/the-kremlin-s-trojan-horses-2-0/; Heather Conley, et al., "The Kremlin Playbook," Center for Strategic and International Studies, October 13, 2016, https://www.csis.org/analysis/kremlin-playbook; and Kramer and Speranza, "Meeting the Russian Hybrid Challenge."

5 Anton Troianovsky, "Putin Endorses Brazen Remedy to Extend His Rule, Possibly for Life," *New York Times*, March 10, 2020, https://www.nytimes.com/2020/03/10/world/europe/putin-president-russia.html.

6 While the outbreak of COVID-19 could delay the nationwide vote, many Russia watchers agree the measure will pass. See Andrew Higgins, "Russia's Highest Court Opens Way for Putin to Rule Until 2036," *New York Times*, March 16, 2020, https://www.nytimes.com/2020/03/16/world/europe/russia-putin-president-for-life.html

7 Anne Gearan, Steven Mufson, and Will Englund, "Trump Assures U.S. Oil Companies That They Will Get Federal Help to Offset Pandemic Effects on Oil Prices," *Washington Post*, April 3, 2020, https://www.washingtonpost.com/politics/trump-assures-us-oil-companies-will-get-federal-help-to-offset-pandemic-effects-on-oil-prices/2020/04/03/5f0e7308-75dd-11ea-87da-77a8136c1a6d_story.html.

8 Chris Skaluba and Ian Brzezinski, *Coronavirus and Transatlantic Security: Implications for Defense Planning, Atlantic Council*, March 30, 2020, https://www.atlanticcouncil.org/blogs/new-atlanticist/coronavirus-and-transatlantic-security-implications-for-defense-planning/.



Ukrainian gas pipeline, a type of critical infrastructure manipulated by Russia through its hybrid activities. *Photo: Dmytro Glazkov/World Bank*

Further emboldening Putin is the lack of traditional US leadership and pushback that has helped to keep Russia in check. US President Donald Trump has instead tried to appeal to Putin, describing his own policy as "getting along with Russia" and reducing perceived or actual consequences of hybrid actions against the United States. Political allegations of the Trump campaign "colluding" with Russia to affect US elections[9] have further divided the American public toward Russian aims, creating more fertile ground for the Kremlin's malign influence.[10] Compounding this is fraying transatlantic solidarity, whether the US-Germany feud over defense spending or French President Macron's comments that NATO is "braindead."[11] These divisions not only constrain the West's response to Russia's hybrid actions, but also expose cracks in the Alliance that Putin is all too eager to exploit.

Together, these factors indicate that as long as Putin remains in power, the Kremlin will likely continue escalating hybrid activities, short of an all-out war with NATO, to push boundaries and test what is acceptable going forward. In the relative near term, the transatlantic community must plan according to Russia's current trajectory on hybrid issues, which demands a more proactive and widespread approach.

Chinese Hybrid Activities

Similar to Russia, China seeks a world that is less dominated by the US-led international system and gives China more influence over global affairs. However, given its history, governance model, geopolitical position, and relations with the transatlantic community, China has a different

9 See "The Russia Investigation," CNN, accessed April 2020, https://www.cnn.com/specials/politics/trump-russia-ties.
10 Andrew Weiss, "Trump's Confused Russia Policy Is a Boon for Putin," Politico, June 25, 2019, https://www.politico.com/magazine/story/2019/06/25/trump-putin-russia-weiss-227205.
11 "NATO Alliance Experiencing Brain Death, Says Macron," BBC, November 7, 2019, https://www.bbc.com/news/world-europe-50335257.

worldview and strategic endgame. All Chinese policies are underpinned by the need to keep the Chinese Communist Party (CCP) in power. Beyond that, several long-standing Chinese narratives impact China's foreign policy. One such narrative relates to the "hundred years of humiliation" China experienced as its once-central global role was diminished by a series of Western incursions in the 1800s.[12] The CCP has leveraged this mentality, combined with the filial piety between the Chinese state and its people, to keep China stable and unified against external territorial, economic, political, and cultural threats.[13] With another core principle of "history as destiny," China believes it will regain its stature as a powerful, respected actor in the world and a benevolent overseer of its broader region.[14] Described by Chinese President Xi Jinping as the "Chinese Dream," this notion underpins many of the government's maneuvers to expand its international influence and reach. At the same time, China has traditionally preserved a culture of peaceful coexistence, indicating it does not seek *aggressive* expansion or view foreign interference in the same way as other powers. Yet Chinese officials have manipulated this narrative to support China "defending against threats" to its perceived regional and global role, which the Chinese government defines at its discretion.[15] Other factors, such as the unique role and leadership style of President Xi Jinping and China's growing material capabilities, have also created new dynamics suggesting China has shifted toward a much more assertive role, as evidenced by its hostile actions in the South China Sea, for example.[16]

In light of this, many experts argue that China seeks to displace, or at least gradually adapt, the current international system in order to return to its desired role.[17] Yet, such adaptation must be understood with nuance. Indeed, China has benefitted from many of the current order's features, such as Western capitalism, the Euro-Atlantic trade order, and the US guarantee of free and secure trade routes. Rather than disrupting or entirely displacing those aspects, China wants to manipulate them to fuel its own rise as a great power. Much of China's strategy to do so involves working with willing nations bilaterally where opportunities for investment and influence exist. This is a necessary in Europe, where shared interests are ample, but where a mismatch of values and political models limits the ceiling for cooperation. Many European democracies desperate for investment from Beijing are only willing to cooperate to a certain extent with communist China. The EU has described it as follows.

> "There is a growing appreciation in Europe that the balance of challenges and opportunities presented by China has shifted…China is, simultaneously, in different policy areas, a cooperation partner with whom the EU has closely aligned objectives, a negotiating partner with whom the EU needs to find a balance of interests, an economic competitor in the pursuit of technological leadership, and a systemic rival promoting alternative models of governance."[18]

This realization and, subsequently, more restrictive policies toward China are increasingly being adopted by Euro-Atlantic countries and institutions. Because China prefers to work through mechanisms in which it has more control, this has driven it to create its own frameworks for engagement in Europe and Eurasia, supported by its growing economic and military might. As a result, China's moves to gain new political and economic partners have begun to undermine EU, NATO, and transatlantic efforts.[19] This has led to the rise of China's own kind of hybrid activities.

China's hybrid toolkit in Europe largely focuses on political and economic coercion to advance its objectives. Chinese tools include: leveraging unequal trade relationships with foreign countries to secure favorable terms for China; making large foreign direct investments in strategic sectors, prioritizing investments that give China access to European

12 Matt Schiavenza, "How Humiliation Drove Modern Chinese History," *Atlantic*, October 25, 2013, https://www.theatlantic.com/china/archive/2013/10/how-humiliation-drove-modern-chinese-history/280878/.

13 Merriden Varrall, "Chinese Worldviews and China's Foreign Policy," Lowy Institute for Foreign Policy, November 2015, https://www.lowyinstitute.org/sites/default/files/chinese-worldviews-chinas-foreign-policy_0.pdf.

14 Ibid.

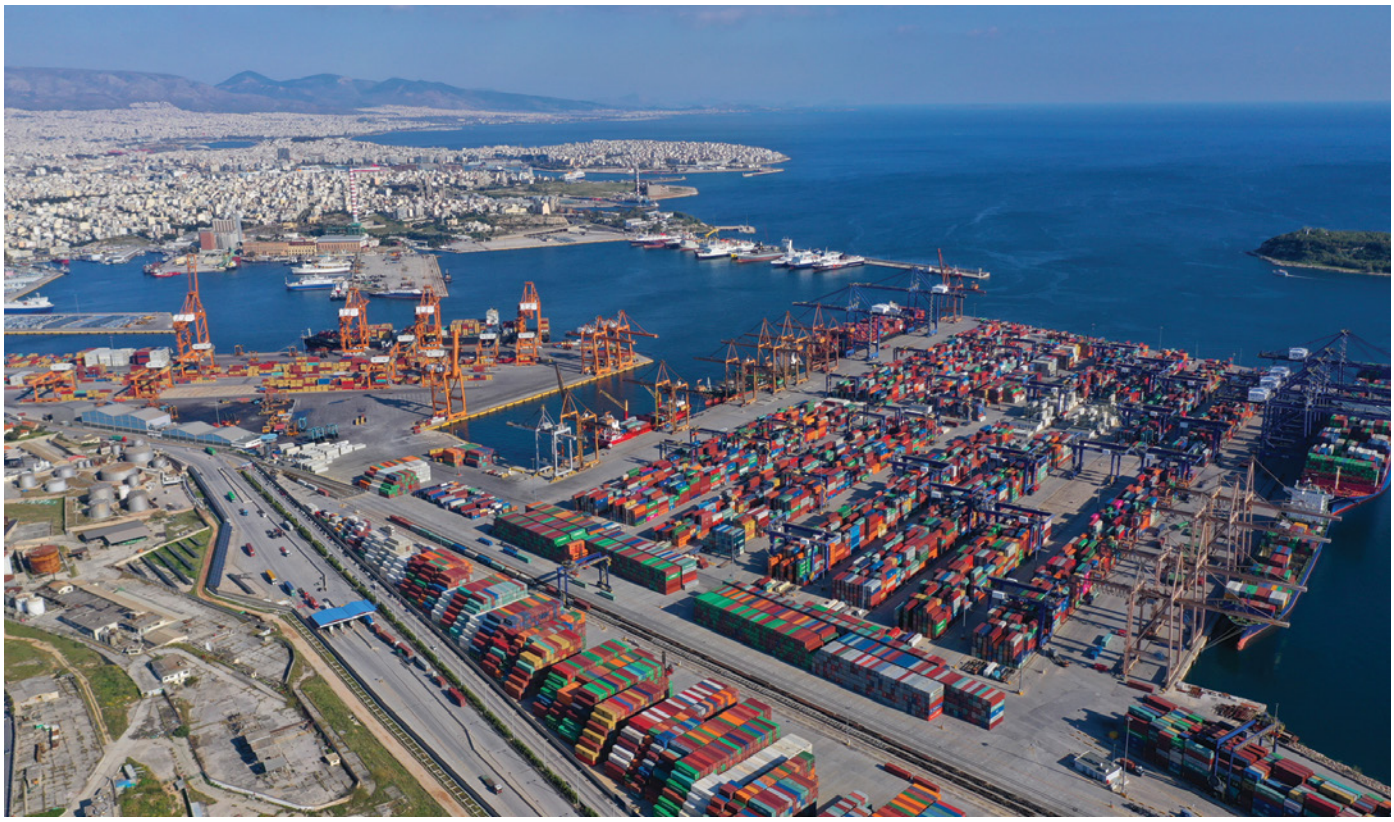
15 There is debate over why China has recently become more assertive in its defense against threats to its international claims and perceived global role. For more, see Varrall, "Chinese Worldviews and China's Foreign Policy"; and Ankit Panda, "Reflecting on China's Five Principles, 60 Years Later," *Diplomat*, June 26, 2014, https://thediplomat.com/2014/06/reflecting-on-chinas-five-principles-60-years-later/.

16 "Xi Jinping and the 'Chinese Dream,'" *DW*, May 7, 2018, https://www.dw.com/en/xi-jinping-and-the-chinese-dream/a-43685630. For more on China's South China Sea hybrid activities, see Sergio Miracola, "Chinese Hybrid Warfare," Italian Institute for International Political Studies, December 2018, https://www.ispionline.it/en/pubblicazione/chinese-hybrid-warfare-21853.

17 For example, see Weizhen Tan, "Why China's Rise May Call for 'a New World Order,'" CNBC, April 25, 2019, https://www.cnbc.com/2019/04/25/why-chinas-rise-may-call-for-a-new-world-order.html.

18 "EU-China: A Strategic Outlook," Joint Communication To The European Parliament, The European Council And The Council, European Commission, March 12, 2019, https://ec.europa.eu/commission/sites/beta-political/files/communication-eu-china-a-strategic-outlook.pdf.

19 There is some debate about whether or not this is China's goal to deliberately undermine transatlantic institutions. In some cases, China has shown it prefers to work with the EU, for instance on trade issues and the Joint Comprehensive Plan of Action for Iran. Others argue China only does this out of necessity and would prefer these institutions be replaced with its own China-dominated structures.



Chinese shipping firm COSCO purchased a majority stake in Greece's Port of Piraeus (shown above), which China has begun to rapidly develop as a key node in its Belt and Road Initiative. China plans to make Piraeus the largest commercial harbor on the Mediterranean, further connecting China to European, and eventually African, markets. *Photo: Shutterstock/Aerial-motion*

political elites; and launching massive critical infrastructure projects at cheap rates in foreign countries that connect China to European markets. These projects overtly favor Chinese workers and industry and give China control over operating the infrastructure, posing significant security and geopolitical risks for the receiving country. China has also become known for its use of "debt-trap diplomacy," which typically involves giving large loans to vulnerable countries to support these big projects, anticipating their inability to fulfill payment obligations. When the country defaults on debt, China subsequently assumes control of the projects, providing significant leverage beyond its borders. Much of this is facilitated through China's self-promoting political frameworks and initiatives such as 17+1 and the Belt and Road Initiative (BRI).[20] By focusing on pragmatic cooperation on shared challenges and interests, such as economic development, China uses these tools to build relationships and further integrate itself with transatlantic countries, despite differences on broader political issues. The Chinese government then uses those relationships to detract from the criticism against its delinquency in other international obligations (e.g., human rights, law of the sea), and to manipulate political decision-making inside institutions such as the EU.

China has also conducted a range of operational and cyber hybrid activities, which have increased as political and trade tensions have escalated between the United States and China. This has included the cyber-enabled theft of US and European intellectual property for China's commercial and technological advantage. Using coordinated hacking and espionage efforts, China has sponsored numerous operations against defense contractors and producers of civilian and military technologies, such as aerospace, semiconductors, and information technology, which China views as critical to future innovation. China reinforces these efforts by using unfair practices related to industrial policy, such as forced technology transfer, which mandates that US and European companies share their technology to gain access to Chinese markets. Many academics have

20 See Cooperation of Central and Eastern European countries and China, accessed March 24, 2020, http://www.china-ceec.org/eng/; "BRI Factsheets," Belt and Road Initiative, accessed March 24, 2020, https://www.beltroad-initiative.com/factsheets/.

also been subject to Chinese attempts at appropriating their work or intellectual property.

When it comes to information operations, China has used its Confucius Institutes across Europe and the United States to propagate Chinese language, culture, and influence.[21] Beyond this, China uses targeted messengers—whether diplomats in embassies around the world or Chinese students studying abroad in Europe or the United States—to promote misleading Chinese narratives in local, national, and social media. China also uses these organizations and people as vehicles to invest in media companies and partnerships, in hopes that they will favor and share Chinese content, which often oversimplifies complex issues, glorifies China, and misrepresents the truth.

Going forward, China's hybrid activities will be shaped by a number of factors. First among these will be the aftermath of the coronavirus pandemic. The Chinese government's management of the outbreak has sparked sharp international criticism ranging from lack of transparency to deliberate manipulation of the crisis for its own geopolitical gain.[22] Some argue that China's actions and geopolitical repositioning around the coronavirus, including its suppression of key outbreak data and propaganda initiatives to boost its authoritarian regime as a model to respond to the crisis, are a prime example of its hybrid activities at work.[23] Coupled with massive economic losses, this could limit China's political and economic ability to expand its influence in Europe and abroad in the short term. In the longer term, however, China's growth is expected to rebound, fueling renewed political and economic forays into the global arena. Moreover, some experts argue that the shocks from the pandemic crisis will hit democracies and the US-led global system harder than communist China, allowing it to emerge as a more influential world power than before.[24]

Another major factor that could affect China's course is the transatlantic community's response to its hybrid actions. Thus far, China's hybrid activities have been particularly challenging to counter because *some* of the actions are currently legitimate or legal, even if undesirable for transatlantic nations. Additionally, as highlighted by the EU's strategic outlook referenced above, many of these nations, including the United States, rely on China as a critical trading partner, which makes some level of pragmatic cooperation essential. For European nations, especially those struggling financially and in dire need of investments and modernization, few alternatives can compete with China's infrastructure and loan offers. All of this has constrained a collective response. Nevertheless, as evidenced by new strategic documents released by NATO, the EU, and nations, concerns over China's hybrid activities are growing, alongside the political will to take action.[25] In addition to recent worries about the coronavirus, another major concern involves Chinese-led infrastructure projects in Europe—from 5G telecommunications networks and undersea cables to electric grids, power plants, and nuclear projects—that utilize technology built by Chinese state-run or subsidized companies. There is a growing belief among transatlantic policymakers that the Chinese government could mandate backdoor access to this infrastructure, which it could in turn manipulate for espionage or other political purposes. As unity around this issue grows, China could be forced to change some of its behavior, but only if the transatlantic community can respond effectively.

At the same time, China will seek to utilize its influence in countries like Italy and Hungary to undermine European consensus on these issues. To stay ahead of the curve, the transatlantic community needs a more proactive and comprehensive counter-hybrid approach for China.

Since Russian and Chinese hybrid activities are directly linked to their worldviews and grand strategies, limiting them, let alone causing fundamental behavioral change, is difficult. Because Russian and Chinese hybrid activities

21 Pratik Jakhar, "Confucius Institutes: The Growth of China's Controversial Cultural Branch," BBC, September 7, 2019, https://www.bbc.com/news/world-asia-china-49511231.

22 Rebeccah Heinrichs, "Five Lies China is Telling About Coronavirus," *Washington Examiner*, April 19, 2020, https://www.washingtonexaminer.com/opinion/five-lies-china-is-telling-about-coronavirus.

23 Tobin Harshaw, "Coronavirus Response Is a Weapon in China's Brand of War," Bloomberg, March 28, 2020, https://www.bloomberg.com/opinion/articles/2020-03-28/coronavirus-response-is-a-weapon-in-china-s-brand-of-war.

24 For more on this, see Hal Brands, "Coronavirus Is China's Chance to Weaken the Liberal Order," Bloomberg, March 16, 2020, https://www.bloomberg.com/opinion/articles/2020-03-17/coronavirus-is-making-china-s-model-look-better-and-better; and Mira Rapp-Hooper, "China, America, and the International Order After the Pandemic," *War on the Rocks*, March 24, 2020, https://warontherocks.com/2020/03/china-america-and-the-international-order-after-the-pandemic/.

25 For NATO and the EU's policies on China, see: "NATO Recognizes China 'Challenges' for the First Time," *DW*, December 3, 2019, https://www.dw.com/en/nato-recognizes-china-challenges-for-the-first-time/a-51519351; and "EU Strategy on China," European Union, June 2016, http://data.consilium.europa.eu/doc/document/ST-11252-2016-INIT/en/pdf. For samples of national China strategies, see "Approach to Matters Relating to China," Government of Sweden, September 26, 2019, https://www.government.se/4adb19/contentassets/e597d50630fa4eaba140d28fb252c29f/government-communication-approach-to-matters-relating-to-china.pdf; and "National Security Strategy of the United States of America," White House, December 18, 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

come with different motivations, tactics, and effects, developing an overarching counter-hybrid strategy is all the more challenging. Complicating this further is the potential for pragmatic hybrid cooperation between Russia and China against the transatlantic community. Moscow and Beijing have already sought to harmonize their economic and military clout in pursuit of shared interests—for example by using arms sales and joint military exercises to expand their influence in Africa. Something similar could happen in Europe. This difficult threat environment makes a proactive and unified transatlantic approach to hybrid threats increasingly important.

Current Efforts to Counter Hybrid Threats and Constraints

The recognition of Russian and Chinese hybrid actions, and the detrimental impacts they can have on transatlantic societies, has prompted collective security institutions (primarily NATO and the EU) and nations to revisit their counter-hybrid approaches. As a result, significant progress has been made over the last five years.

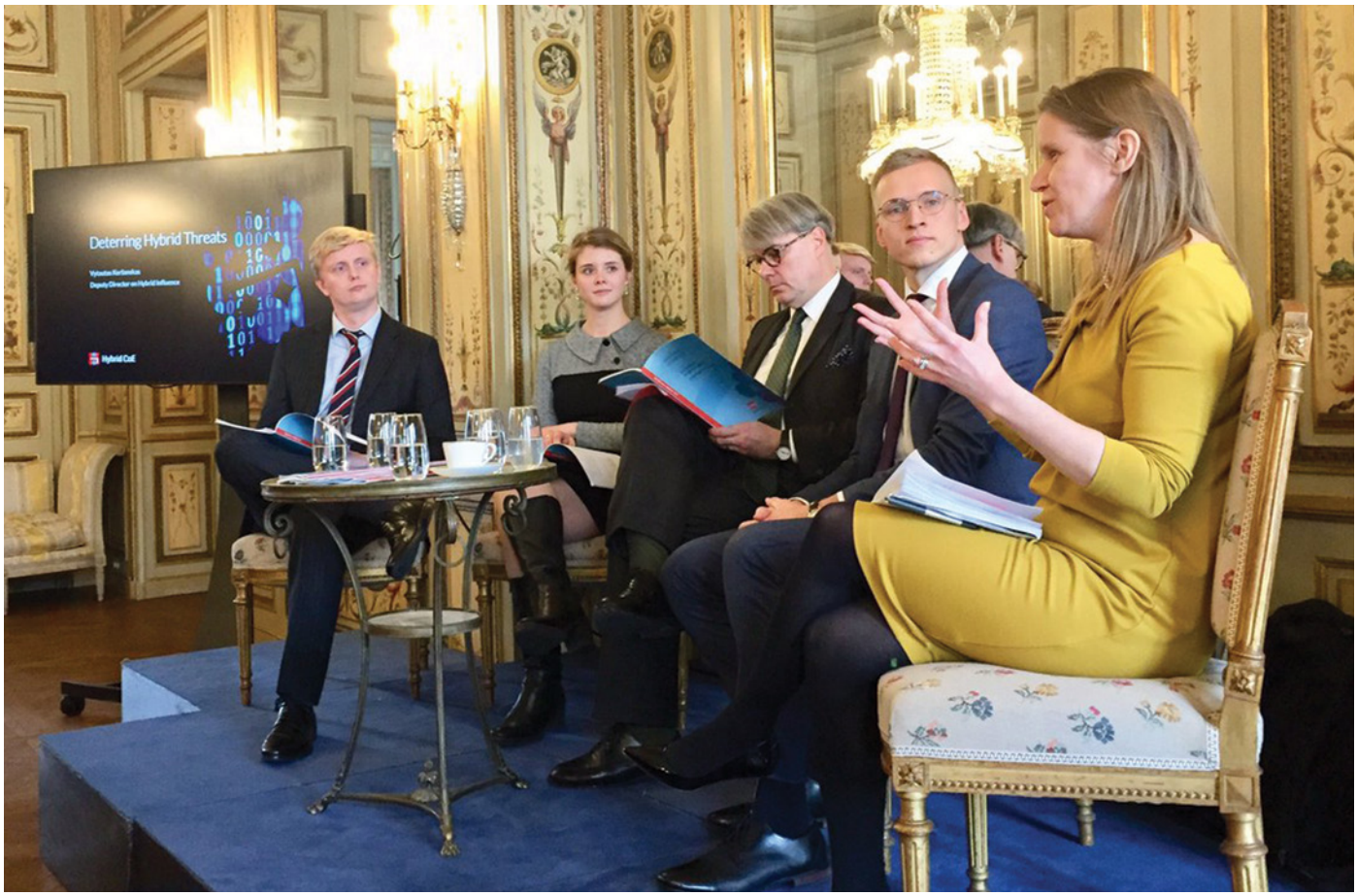
At the institutional level, in 2016, NATO and the EU signed a historic joint declaration to enhance their cooperation despite long-term political and bureaucratic obstacles.[26] This collective effort produced seventy-four concrete proposals for joint action, twenty of which focused on hybrid, signaling a new level of political ambition in tackling this challenge. As part of this, NATO and the EU also jointly supported the establishment of a unique European Center of Excellence for Countering Hybrid Threats, housed in Helsinki, which is structurally independent of the institutions and supported by twenty-seven transatlantic nations.[27]

Beyond this cooperation, each institution has taken individual measures to strengthen its counter-hybrid approaches. The EU, for its part, created a Joint Framework on Countering Hybrid Threats to clarify its mandate to act.[28] Structurally, it also created a hybrid fusion cell with national contact points across member states, to enhance intelligence gathering and situational awareness. Alongside this, it stood up functional initiatives, such as the East StratCom Task Force and its *EU vs. Disinfo* platform designed to respond to Russian disinformation campaigns against Europe. In a key legislative move, the EU also adopted a Code of Practice on Disinformation, a set of self-regulatory standards agreed to by nations, online platforms, social networks, and the advertising industry to address the spread of online disinformation and fake news.[29]

NATO, in a parallel effort to reinforce its mandate, published important language in a summit communique empowering NATO "to assist an Ally at any stage of a hybrid campaign."[30] It also made structural adaptations, including the creation of a Hybrid Analysis branch to enhance shared situational awareness. Functionally, the Alliance also established Counter-Hybrid Support Teams (CHSTs), which provide "fly-away" teams that can deploy to nations to help build resilience against hybrid threats.[31] To test these new structures and capabilities, NATO and the EU have led annual coordinated and parallel crisis-management exercises (CMXs), parts of which focus on hybrid.[32]

In addition to driving these actions inside NATO and the EU, transatlantic countries have taken steps at the national level to enhance their own ability to counter hybrid threats. Many nations have begun working hybrid issues into their national defense strategies and plans. Sweden

26 "Joint Declaration on EU-NATO Cooperation," NATO, updated July 2018, https://www.nato.int/cps/en/natohq/official_texts_156626.htm.
27 Participation in the center is open to EU member states and NATO allies, and NATO and the EU as institutions actively participate in center activities. For more, see "What is Hybrid CoE?" Hybrid Centre of Excellence," CoE: https://www.hybridcoe.fi/what-is-hybridcoe/.
28 "EU Joint Framework for Countering Hybrid Threats," European Commission, April 6, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018.
29 "Code of Conduct on Disinformation," European Commission, September 26, 2018, https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.
30 NATO, press release, "Brussels Summit Declaration," July 11, 2018, paragraph 3, https://www.nato.int/cps/en/natohq/official_texts_156624.htm.
31 In 2019, these teams were deployed for the first time to Montenegro to provide support around national elections. Slobodan Lekic, "First NATO Counter-Hybrid Warfare Team to Deploy to Montenegro," *Stars and Stripes,* November 8, 2019, https://www.stripes.com/news/first-nato-counter-hybrid-warfare-team-to-deploy-to-montenegro-1.606562.
32 It is worth noting that the CMXs are "coordinated and parallel" rather than truly joint; this means NATO and the EU alternate leadership each year, and do not truly coordinate as they would have to in reality to leverage their different capabilities. Due to political sensitivities and the fear that a difficult hybrid scenario could derail these public-facing large-scale exercises and undermine deterrence, they do not test real scenarios, which limits policymakers' abilities to identify weaknesses and realistically prepare for the future.



The Hybrid CoE launching a playbook for deterring hybrid threats at an event in March 2020. *Photo: Hybrid CoE*

and Finland, for example, have also reinvested in their total defense and comprehensive security concepts, which involve all aspects of their societies and governments in countering hybrid issues. Some nations have also made important structural adaptations to bring together key capabilities for functional aspects of hybrid. For instance, the United Kingdom and Lithuania stood up centralized national cybersecurity centers. The United States Department of State also launched its Global Engagement Center to counter foreign disinformation campaigns aimed at the United States and its allies and partners.[33] The US Congress has introduced proposals that advocate for the creation of new structures, such as a Foreign Malign Influence Response Center and a Social Media Data and Threat Analysis Center, along with seed funding to support more coherent interagency counter-hybrid efforts. Other key national legislative initiatives have taken the form of sanctions, which the United States, Canada, and nations of the EU have collectively imposed on Russia, for example, in response to its annexation of Crimea and hybrid activities in eastern Ukraine. New US legislative proposals, including the Defending American Security from Kremlin Aggression (DASKA) Act and the Defending Elections against Trolls from Enemy Regimes (DETER) Act, aim to address a wider scope of Russia's hybrid activities.

Indeed, all of these efforts, among others, have helped transatlantic policymakers and publics better understand hybrid threats, build new tools to combat them, and develop the legal frameworks and mandates to take action, especially at the tactical level. Yet, even these efforts have failed to deter Russia and China from using hybrid activities. Despite the utility of many of these transatlantic efforts, the whole is less than the sum of its parts for three overarching reasons.

First is the lack of understanding. Transatlantic governments have each compiled different threat assessments based on their individual experiences with hybrid activities, which has complicated the formation of a common understanding of hybrid threats. Due to a lack of integrated analytical capabilities, information-sharing

33 See "Global Engagement Center," United States Department of State, accessed April 10, 2020, https://2009-2017.state.gov/r/gec//index.htm.

obstacles, and sensitivities around nations revealing their vulnerabilities, the transatlantic community has yet to develop a full understanding of the impacts of hybrid activities and how they connect across contexts. Relatedly, nations and institutions often hesitate to use real-world scenarios when exercising responses to hybrid threats out of fear of publicly failing to navigate them. Opting for imagined scenarios, which often lack sufficient nuances and complexities, inhibits their ability to identify shortfalls and learn which approaches work. All of this has severely limited the effectiveness of transatlantic counter-hybrid efforts thus far.

Second is the lack of sufficient resources. On the whole, transatlantic counter-hybrid efforts remain far too under-resourced in terms of budgets and appropriate personnel. For example, the EU's East StratCom Task Force has a dedicated budget of just three million euros with only sixteen staff to cover counter-disinformation efforts across the entire EU.[34] Similarly, NATO's quick-response CHSTs are not resourced to be standing forces, so they require significant time to recruit required expertise (think of white-hat hackers, as opposed to one of NATO's many policy experts), let alone form and deploy. Even when counter-hybrid efforts are well-funded in accordance with stated policy, complex governmental and institutional budget requirements often prevent funds from flowing to specific places where they are needed most. Insufficient resourcing limits the scope of these efforts and their larger strategic effect. In the face of widespread, pervasive, and diverse hybrid activities, this is a huge obstacle.

Third is the lack of coordination on the national and international levels. Cross-cutting hybrid threats often touch numerous parts of governments, requiring tireless coordination among various agencies on everything from intelligence to responses. The national interagency process in most countries also lacks adequate involvement from civil society and the private sector when it comes to counter-hybrid efforts. If not effective at the national level, coordination at the international level is more difficult for the thirty different countries inside NATO or the EU. Inter-institutional cooperation *between* NATO and the EU becomes almost impossible then, especially given long-standing political and bureaucratic obstacles plaguing their relations. This forces nearly all coordination to be informal, relying on pragmatic personalities and creative solutions among officials to achieve results. On top of everything, there is no single platform to convene relevant authorities from NATO, the EU, their nations, the private sector, and civil society to coordinate. As a result, transatlantic counter-hybrid efforts have remained largely disjointed, producing a patchwork effect.

In light of this, next-level actions are needed to address the knowledge, resource, and coordination gaps outlined above. An enhanced approach is required to meaningfully deter and limit Russia's and China's further use of hybrid actions. In the wake of the coronavirus crisis, the need for NATO and EU nations to focus on domestic political, health, and economic agendas will make coordination on hybrid issues more difficult. At the same time, the crisis underscores that hybrid issues—including those around pandemics—cannot be solved alone. This provides a stronger impetus for cooperation among core transatlantic allies. What is needed now is a much more comprehensive, coherent, and forward-leaning transatlantic strategy for countering Russian and Chinese hybrid threats.

Building a Strategic Concept for Countering Hybrid Threats

To develop such a transatlantic counter-hybrid strategy for Russia and China, two major things need to happen. First, transatlantic policymakers have to build a common strategic concept to guide collective thinking on hybrid threats. Second, transatlantic policymakers need to take a range of practical actions in service of that strategic concept. The remainder of this paper seeks to guide policymakers toward those ends.

Outlined below are five strategic priorities which, if addressed together, could form the basis of a new transatlantic strategic concept for countering Russian and Chinese hybrid threats.

1) Redefine the conceptual framework for hybrid threats. Before outlining a counter-hybrid strategy, transatlantic policymakers should reconceptualize how they think

34 "Questions and Answers about the East StratCom Task Force," European Union, 2018, https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-stratcom-task-force_en.

about hybrid threats. As a first step, this requires an acknowledgement that hybrid actions are best understood in the full spectrum of international relations, rather than *distinctly* within the scope of armed attack. In other words, hybrid activities should be viewed as part of broader day-to-day competition with Russia and China, as opposed to conflict or war. As underscored above, Russian and Chinese hybrid activities combine legitimate, undesirable, and illegal actions with those that could be considered more traditional military attacks. Because Russia and China use these actions without the intention of going to full-scale war with their targets—but, rather, to avoid it and intentionally blur the line between peace and conflict—*the spectrum of conflict is only useful up to a point as a framework for guiding interpretations of hybrid actions and possible responses*.

Relatedly, there is a conceptual debate within policy communities over whether "deterrence," which traditionally stems from nuclear and conventional contexts, applies to hybrid threats in the same way. One school of thought, which is supported in this paper's analysis, argues that deterrence typically refers to preventing conflict from occurring in the first place, whereas with hybrid, the conflict is under way and a perpetual activity. Given that the threat environment is not likely to reduce to "zero" in the hybrid space, this line of thinking asserts that conventional wisdom and assumptions related to deterrence can be misleading. In this vein, it is also difficult to apply deterrence, which tends to be actor-centric, against irregular groups or social forces that are employed throughout hybrid activities. Even when Russia or China are behind a particular hybrid operation, they strive to maintain plausible deniability, making attribution challenging. In reconceptualizing how to change an adversary or competitor's behavior or calculations with respect to hybrid, it is perhaps more useful to refer to *dissuasion* instead of deterrence. In other words, how can transatlantic nations *dissuade* Russia or China from using additional or more intense hybrid actions in the future, or *persuade* them to reduce current actions? This is not just a rhetorical adjustment; it also challenges the way transatlantic policymakers think about escalation and shaping norms, which has significant implications for any counter-hybrid strategy.

Another school of thought argues that deterrence can be used as a framework for influencing a state actor's antagonistic hybrid behavior. Under this paradigm, persuasion and dissuasion fall lower on the traditional escalation ladder of state-to-state relations and cannot replace deterrence. Some in this camp use the term "modern deterrence" for hybrid threats, but only with a focus on building resilience (the hybrid equivalent of deterrence by denial). Yet, this paper argues that approach does not go far enough to sufficiently contain, counter, or stem the hybrid threats facing the transatlantic community.

Despite these differences, officials and thought leaders should work toward an interim consensus that traditional deterrence can at least be adapted for the hybrid context to enable short-term policymaking. The Hybrid CoE's recent report, "Deterrence – Proposing a more strategic approach to countering hybrid threats," makes a valuable contribution to this debate toward that end.[35] Going forward, it will be important for transatlantic policymakers to align their thinking on this issue as much as possible to facilitate coherent counter-hybrid efforts.

2) Forge a common, in-depth understanding of the impact of hybrid activities. There is a pressing need to further investigate the impact of hybrid activities on transatlantic societies in order to understand how best to counter them. Across the policy, civil-society, and academic ether, there is indeed a great deal of description of the hybrid set of issues, including the actors, tools, and examples of actions. But there is not yet a comprehensive understanding of the follow-on effects of these activities on both the target and the adversaries, how they are connected, and what they have actually achieved. Nor is any such understanding shared across countries. For example, to what extent has Russian disinformation actually shaped views toward NATO and the EU in the populations of the western Balkans? As another example, if Russia shuts down a gas pipeline to Ukraine, what does that mean for the economy in Slovakia or Germany in the short and long terms? Understanding these questions will be key to designing a strategy that reduces the impact of hybrid activities and keeps transatlantic societies more resilient and secure.

3) Articulate clear strategic goals for countering hybrid threats. The transatlantic community needs to clearly define its strategic goals and desired end state vis-à-vis hybrid threats. In other words, what does it want to achieve in countering hybrid activities, and what is realistic? This is not yet clearly defined in most national or institutional plans, using common language. While preventing or eliminating all hybrid activities by Russia and China is not feasible, these overarching goals could be broad (for instance, a Russia whose hybrid actions are more limited to non-EU and non-NATO nations, or a China who generally plays by the international rules when it comes to trade and intellectual property laws). To supplement those broad goals, key objectives could be more specific—for example, limiting

35 See Vytautas Kersanskas, "Deterrence: Proposing a More Strategic Approach to Countering Hybrid Threats," Hybrid Centre of Excellence, March 2020, https://www.hybridcoe.fi/wp-content/uploads/2020/03/Deterrence.pdf.

foreign direct investment in *strategic* sectors to no more than 10 percent in all transatlantic countries. Transatlantic policymakers need to consult on these goals, announce them, and codify them in unclassified text to the degree possible. Outlining these aims will be critical to building an effective counter-hybrid strategy.

4) Adopt a more proactive campaign approach to counter-hybrid. To meet the hybrid challenges of today and tomorrow, the transatlantic community must move toward a more proactive campaign approach**.** Thus far, many of the steps undertaken by NATO, the EU, and nations have been largely reactive in response to Russian and Chinese actions against the transatlantic community. But simply reacting and building resilience against those threats is insufficient. Policymakers need to recognize that Russia and China are utilizing widespread, targeted *campaign* approaches that require more forward-leaning *campaign* responses. In that spirit, the transatlantic community should think about how it can create insurmountable obstacles for its adversaries and competitors in their hybrid pursuits. How can it force them to change their behavior against their key objectives in a sustained and long-term way? In practical terms, US Cyber Command's concepts of *persistent engagement* and *defend forward* provide good examples of how nations can adopt a more proactive campaign approach in the cyber domain, but more thought should be dedicated to how these concepts can be applied across the four categories of hybrid activities outlined at the beginning of this paper.[36]

To implement such an approach, policymakers need to have a serious discussion about whether and how the transatlantic community ought to set up its counteroffensive—a controversial notion in itself. Given political sensitivities and the defensive nature of the Alliance, NATO is likely the wrong vehicle to orchestrate a counteroffensive; instead, these efforts could be undertaken at the national level, in a coordinated manner. Still, NATO can certainly remain the primary platform for discussions and consultations to facilitate that coordination. Even if offensive hybrid is a controversial concept, allies should agree that building a better picture of an adversary's weaknesses is worthwhile.

5) Build clear parameters to support joint attribution and action. To support a more proactive strategy, transatlantic policymakers need to build clearer guidelines to establish joint attribution and, if certain parameters are met, enable joint action. As mentioned above, the very nature of hybrid activities makes attribution difficult. Without attribution, it is even more difficult to catalyze action unilaterally, let alone multilaterally. In this regard, it would be useful for NATO and the EU to start outlining shared preconditions to facilitate collective attribution in complex hybrid scenarios. More specifically, what types of things need to be proven, by whom, and to what degree, in order for NATO, the EU, or a group of nations to attribute different kinds of hybrid activities? While criteria will obviously vary on a case-by-case basis, laying out these types of requirements ahead of time, and socializing them among policymakers and advisors, helps to build a more coherent understanding and lays the groundwork for more timely and effective actions.

When it comes to possible joint actions, NATO, the EU, and the Hybrid CoE in Helsinki have all contributed to building joint "playbooks" of potential responses to hybrid actions. While these are extremely useful efforts, most of the proposed options are indeed responsive and reactive. Beyond sanctions, many of these actions, in practice, have failed to impose costs sufficient enough to change Russian or Chinese behavior. As outlined in a previous Atlantic Council paper, the legal framework surrounding hybrid threats—informed by customary international law and treaty law, as well as the law of countermeasures, pleas of necessity, and the norm of non-intervention—provides the basis for more assertive defensive and offensive actions, provided certain conditions are met.[37] What is needed is a clearer articulation of those conditions, analogous to those suggested above for attribution. This would help build a shared sense of what parameters must be met in hybrid scenarios to enable joint action across NATO, the EU, and nations.[38] From there, more preemptive, forward-leaning countermeasures and "actions of necessity" can be laid out in a robust menu of options.[39] Given the collective nature and impact of hybrid threats across the transatlantic community, these options should leverage NATO's Article 5 (collective defense) and Article 3 (resilience) clauses, and the EU's Article 42.7 (mutual defense) clause, to give these institutions a clear mandate to use their many counter-hybrid tools in a more coordinated, unified, and powerful way.

36 For more, see James Miller and Neal Pollard, "Persistent Engagement, Agreed Competition, and Deterrence in Cyberspace," *Lawfare Blog*, April 30, 2019, https://www.lawfareblog.com/persistent-engagement-agreed-competition-and-deterrence-cyberspace.

37 Frank Kramer and Lauren Speranza, *NATO Priorities After the Brussels Summit, Atlantic Council*, November 2018, 14, https://www.atlanticcouncil.org/in-depth-research-reports/report/nato-priorities-after-the-brussels-summit/.

38 Attribution is likely one such parameter in most cases.

39 For more on this concept, see, for instance, Catherine Lotrionte, "Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law," Cyber Defense Review 3, 2 (2018), https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/CDR_V3N2_ReconsideringConsequences_LOTRIONTE.pdf?ver=2018-09-05-084840-807. For some examples of such response options, see Lyle J. Morris, et al., "Gaining Competitive Advantage in the Gray Zone," RAND, 2019, https://www.rand.org/pubs/research_reports/RR2942.html.

Recommendations

In support of the strategic concept outlined above, there are several practical steps articulated below that Euro-Atlantic nations and institutions can take in the short term. While many of these recommendations address several of the considerations above, each is presented here in correspondence with a particular strategic priority. The recommendations lay out specific suggestions for how to organize at the national and international levels, offer ideas to enhance specific counter-hybrid capabilities, and highlight priority areas and new initiatives deserving more attention and resources.

In the short term, the coronavirus crisis will, of course, affect priorities for transatlantic nations and institutions, making it challenging to focus on a full range of counter-hybrid actions. Nevertheless, key counter-hybrid priorities, such as building resilience, strengthening civil response capacities, and investing in civic education, simultaneously serve priorities for pandemic prevention and response and should be integrated and funded as such.

To help redefine the conceptual framework for hybrid threats:

Selectively decouple relations with Russia and China in specific sectors to discourage hybrid behavior. National governments should selectively engage and disengage with Russia and China across different policy areas to shape their perceptions around hybrid threats. Though not a novel concept in international relations, this is a useful framework to apply as policymakers reconceptualize hybrid activities outside the traditional spectrum of conflict, and as part of broader competition. In practical terms, Russia and China may undertake illegal or undesirable hybrid activities in one sector, to which the transatlantic community should respond appropriately and decisively; in most cases, however, this should not preclude cooperation with these countries on areas of mutual interest. For example, while the United States may use punitive economic measures against China to limit its unfair trade practices, Washington may simultaneously collaborate with Beijing to address climate change. In line with the EU's strategic outlook for China and the "Managed Competition" strategy proposed by Franklin D. Kramer, this dual-track approach allows transatlantic countries to indicate which specific hybrid actions they deem unacceptable or acceptable without escalating unnecessarily or cutting off cooperation on key shared issues such as climate, environment, water, and health, despite broader tensions.[40] Such selective decoupling should be adopted multilaterally against Russian and Chinese hybrid actions to help to develop norms in the hybrid space, while also providing a path forward for deeper cooperation should Russia or China decide to change their hybrid behavior.

Create a new platform for cooperation between NATO, the EU, their nations, and the private sector. For a transatlantic counter-hybrid strategy to be effective, NATO, the EU, their member and partner nations, and the private sector need to be conceptually harmonized in how they think about hybrid threats. But, as mentioned above, apart from the efforts of the Hybrid CoE, no official forum currently exists to bring these stakeholders together to coordinate this effort. As recommended in a previous Atlantic Council paper, to address this, a new platform could be created in the form of a Euro-Atlantic Coordinating Council.[41] Rather than a rigid bureaucratic structure, this platform would operate as a voluntary, consensus-based organization. This voluntary approach, based on the model of the Financial Stability Board, provides a different forum for engagement to avoid vetoes and political issues that hinder collective progress on countering hybrid threats, without duplicating existing structures. Maintaining maximum flexibility, the organization would focus on oversight, communication, information sharing, and best practices regarding counter-hybrid—leaving NATO, the EU, nations, and the private sector to implement specific actions at their discretion. The Council could form working groups based on the four categories of hybrid activities to determine the participants at each convening and facilitate more focused discussions. As a baseline agenda, the Council could create and adopt a version of the strategic concept outlined in this paper, in addition to developing shared terms of reference with respect to hybrid. Given its unique nature and position, the Hybrid CoE in Helsinki could consider establishing and managing this Council as a dedicated platform under its auspices, building on the CoE's ongoing work in this realm.

To help forge a common, in-depth understanding of the impact of hybrid activities:

Increase transparency and information sharing around Russian and Chinese hybrid activities. An effective counter-hybrid approach must rest upon a shared understanding

40 Franklin D. Kramer, *Managed Competition: Meeting China's Challenge in a Multi-vector World*, *Atlantic Council*, December 2019, https://www.atlanticcouncil.org/wp-content/uploads/2019/12/Meeting-Chinas-Challenges-Report-WEB.pdf.

41 Kramer and Speranza, *Meeting the Russian Hybrid Challenge*, 3.

If Sweden is attacked, resistance is required

We must be able to resist various types of attack directed against our country. Even today, attacks are taking place against our IT systems and attempts are being made to influence us using false information. We may also be affected by conflicts in our region. Potential attacks include:

- Cyberattacks that knock out important IT systems.
- Sabotage of infrastructure (e.g. roads, bridges, airports, railways, electricity cables and nuclear power stations).
- Terror attacks that affect a large number of people or important organisations.
- Attempts to influence Sweden's decision makers or inhabitants.
- Severed transport links that result in a shortage of foodstuffs and other goods.
- Military attacks, for example airstrikes, rocket attacks or other acts of war.

If Sweden is attacked by another country, we will never give up. All information to the effect that resistance is to cease is false.

Total defence

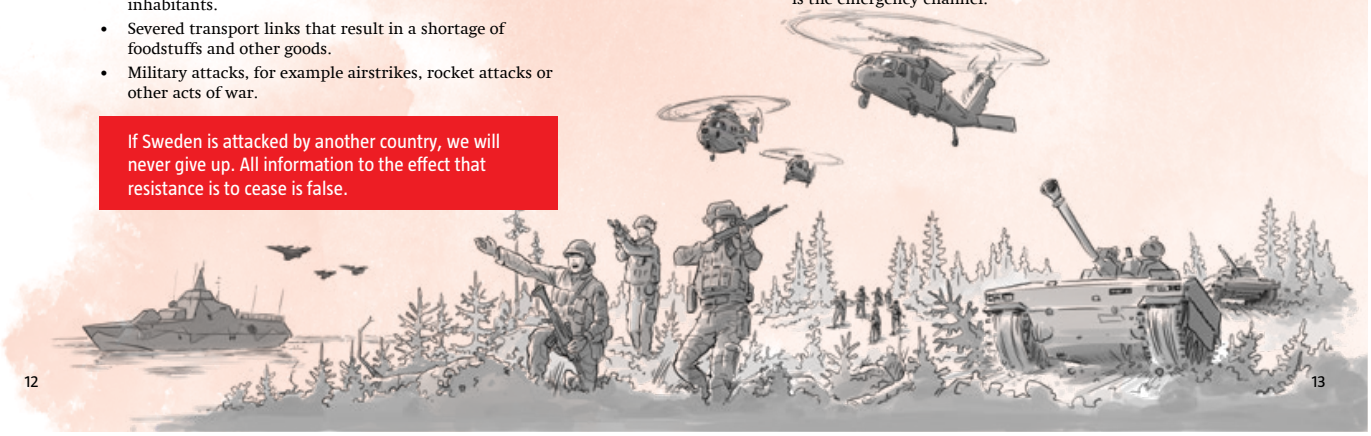
Heightened state of alert

The Government can decide to put the country on a heightened state of alert in order to improve Sweden's chances of defending itself. In a heightened state of alert, peacetime laws apply, but other laws may also be used. For example, the state can requisition private property that is of particular importance to Sweden's total defence.

In a heightened state of alert, the whole of society has to gather its collective forces in order to ensure that vital services continue to function. In a heightened state of alert, you may be called up to help in various ways.

Information about the heightened state of alert will be broadcast on radio and TV. Sveriges Radio's radio station P4 is the emergency channel.

Total defence



12

13

An excerpt from Sweden's 2018 civil defense brochure, "Om krisen eller kriget kommer (If crisis or war comes)," distributed to 4.8 million Swedish households.

of the threat environment. Diverging transatlantic threat perceptions can only be reconciled through greater transparency and information sharing around these issues. Transatlantic countries should be more forthcoming about the hybrid activities they are witnessing to enable collective awareness and response. Whether through NATO, the EU, or regional frameworks; through the Euro-Atlantic Coordinating Council proposed above; through messaging to their publics or media; or through bilateral communication with Russia and China, transatlantic countries should strategically name and shame Russia and China for their specific hybrid actions and demand transparency. Calling attention to these threats and building a shared vernacular around them contributes to a common understanding, promotes cohesion among allies and partners, and paves the way for more consistent responses to these actions. This is particularly crucial for Chinese hybrid activities, which are less understood and pose a significant risk of dividing the transatlantic policy community in the future.

Stand up national hybrid fusion centers. Understanding widespread and diverse hybrid activities requires governments to collect various kinds of intelligence, analyze purposefully ambiguous data and events, and connect them to what may seem like unrelated outcomes. To enable this, nations need to build more integrated analytic and operational capabilities that connect relevant ministries and departments (e.g., defense, foreign affairs, interior, finance) and combine intelligence, planning, and operational functions. This typically requires a dedicated facility, such as a national hybrid fusion center. Hybrid fusion centers should bring together tools and representatives from political, military (including special operations and cyber), civilian authority (including border and law enforcement), economic, and information realms. Ideally, these centers should have a mechanism to coordinate with the private sector and civil society, especially for civil preparedness and critical infrastructure protection. Such hybrid fusion centers would go beyond existing national cyber security centers, for

example, which are limited to one type of hybrid activity.[42] These centers would help build a shared situational picture and enable officials to plan and execute coordinated counter-hybrid actions in a whole-of-government manner.

Conduct hybrid campaign analysis. Rather than focusing on broad Russian and Chinese objectives with respect to hybrid, which is often the approach of larger nations and institutions, such fusion centers should pool information and resources to study more specific, isolated hybrid campaigns across various domains. This approach would significantly improve the ability to understand the impact of and connections between hybrid activities across the four categories in different contexts. It would also help build out a more robust system of indications and warnings (I&W) for future hybrid campaigns, which are vastly underdeveloped compared to conventional I&W. Over time, this integrated campaign-analysis approach would help build a shared awareness of how to anticipate, reduce, or prevent such activities from succeeding or achieving the desired effects in the longer term. Ultimately, this would support a more proactive overall counter-hybrid approach, as well.

To reinforce strategic goals for countering hybrid threats:

Invest in civic education, media training, and civil preparedness. As transatlantic countries define clear objectives for countering hybrid threats, they should communicate them to their publics and media to promote awareness and compliance. A key part of this involves investing in civic education, which plays a vital role in enhancing understanding, creating buy-in, and building societal resilience. Effective examples of these efforts exist across the Nordic and Baltic countries, many of which adopt comprehensive security concepts to involve all parts of government and society. Such efforts include conducting national defense courses, issuing civil-defense brochures for how to spot and handle hybrid contingencies, organizing media capacity-building programs and journalist training workshops, and developing special civilian authorities that receive targeted military training to detect and respond to hybrid activities in local contexts.[43] Building on NATO's seven baseline resilience requirements and EU resilience guidelines, governments should (re)establish and (re)invest in these types of efforts in the post-Cold War era, expanding upon existing materials, adapting them for current hybrid challenges, and tailoring them to national and local environments.[44]

Produce key messages in different languages. Governments should also publish and promote their counter-hybrid goals, documents, policies, and communications in all languages relevant to their populations. Diverse populations, with ethnic minorities or subgroups that speak different languages, are often at higher risk of being targeted by Russian and Chinese disinformation and other hybrid activities that seek to stoke divisions and manipulate government messages. To mitigate this risk and enhance societal resilience, governments must ensure all citizens can understand national goals, principles, values, and policies related to hybrid threats. Institutions, such as NATO and the EU, should supplement translation and dissemination efforts where possible, as they have greater resources and more diverse personnel with multilingual capabilities. Their resources and personnel should also be distributed in support of institutions at all levels of government, as well as grassroots organizations, engaged in countering Russian and Chinese narratives for local populations.

Provide guidance to the private sector to support counter-hybrid goals. To achieve counter-hybrid goals, governments need to work with the private sector in more deliberate ways. As underscored above, the private sector plays a

42 The Foreign Malign Influence Response Center recently proposed in pending US legislation embodies this approach, recommending the establishment of a fusion center under the US Director of National Intelligence designed to counter hybrid activities in a more holistic way among the US interagency. Additional initiatives in this spirit should be supported in each transatlantic country.

43 Finland, for instance, conducts wide-reaching national and regional defense courses, which help to establish a common understanding of the threats facing Finland and improve collaboration between different sectors of society, government, and military in emergency conditions. It also promotes networking and cohesion between people working in different areas of comprehensive security and builds a shared inclination in support of national defense. See "National Defence Courses," The Security Committee of Finland, accessed March 20, 2020, https://turvallisuuskomitea.fi/en/cooperation/national-defence-courses/. Following Russia's illegal annexation of Crimea and growing hybrid activities around Europe, Sweden and Lithuania, among others, issued civil-defense brochures to their populations calling on citizens to ensure they are prepared for a major war or civil emergency. These booklets, which are circulated online and in all schools, libraries, universities, and local government facilities, encourage citizens to make sure they have adequate food, water, shelter, and access to reliable information in the event of a crisis. They also outline tips and guidance for how to spot foreign malign activity in their area, and how to report and react to these scenarios without necessarily taking up arms. See "If Crisis or War Comes," Swedish Civil Contingencies Agency, May 2018, https://www.dinsakerhet.se/siteassets/dinsakerhet.se/broschyren-om-krisen-eller-kriget-kommer/om-krisen-eller-kriget-kommer---engelska-2.pdf; and "Prepare to Survive Emergencies and War," Ministry of National Defense of Lithuania, 2015, file:///C:/Users/LSperanza.ACUS/Downloads/ka%20turime%20zinoti%20en.pdf. Norway also maintains a special force called the Home Guard, whose civilian members complete military training. Their activities include search-and-rescue and natural disaster clean up, but they can also be used as a local response force in case of an attack. Almost all personnel are assigned to their home areas, which makes them uniquely suited to notice and report subtle changes in the environment and hybrid activities missed by most people. See "Home Guard," Norwegian Armed Forces, accessed March 24, 2020, https://forsvaret.no/en/organisation/home-guard.

44 For instance, guidance on how to spot Russian military equipment in the Baltics would not be relevant in the United States, but tips for detecting Russian or Chinese disinformation could be.

crucial role in countering hybrid threats—whether through platform companies (e.g., Facebook, Google, Microsoft) combatting disinformation online or critical infrastructure operators (e.g., electric grids, energy pipelines) ensuring basic functions of society through crises. Yet, without clear guidance from governments and international institutions, private-sector stakeholders are unlikely to sufficiently self-regulate to support specific counter-hybrid goals. Instead of relying solely on a market approach, transatlantic policymakers should provide legislation to ensure the private sector is equipped to help identify vulnerabilities, build resilience, and coordinate with relevant authorities across hybrid contingencies.

Because many of these companies are multinational, international institutions have a unique role to play—in particular the EU given its ability to legislate. Building on similar legislation and regulations in other sensitive industries, the EU should work directly with key private-sector stakeholders to develop basic guidelines for how industry leaders and their employees need to be thinking about, preparing for, and responding to hybrid threats. Key focus areas should include

- detecting hybrid threats, campaigns, and incidents;
- identifying and addressing vulnerabilities;
- ensuring adequate redundancy in critical infrastructure;
- communication protocols with governments and citizens;
- mechanisms to transfer authorities to government under necessary circumstances; and
- encouraging cooperation and joint ventures to provide competitive alternatives to foreign technology, equipment, and infrastructure in strategic sectors.[45]

To support a more proactive, campaign aproach to counter-hybrid:

Clarify counter-hybrid standard operating procedures (SOPs). A major factor constraining nations' abilities to be proactive in their counter-hybrid efforts is that no single part of government owns hybrid threats. As a result, it remains challenging to catalyze *responsive* actions within bureaucracies, let alone *proactive* ones. The national hybrid fusion centers recommended above would go a long way in centralizing cross-governmental tools and competencies, but they will only function effectively if there are clear mechanisms for command and control. Consequently, nations should work to clarify standard operating procedures, authorities, and information-sharing protocols across departments and agencies for a wide range of hybrid activities. This would bolster their capacity to effectively communicate, coordinate, and respond in real time to, and ideally in anticipation of, hybrid attacks. One baseline goal should be to provide clear guidance for how forces or actors in the field can detect hybrid activities, report their findings to the government, and respond quickly.[46]

Pair highly capable nations with less capable nations to build counter-hybrid capacities. Nations and institutions cannot proactively address hybrid threats if they do not have well-developed capabilities to do so. Many medium-sized transatlantic nations have developed significant specialized capabilities to address certain sets of Russian and Chinese hybrid activities. For example, Estonia punches above its weight in advanced cyber capabilities, while Denmark has advanced special-operations forces. Drawing on NATO's framework nation model, and either through NATO, EU, regional (e.g., Nordic Defense Cooperation, Visegrád Group), or bilateral frameworks, these capable nations should team up with less capable nations across Europe to conduct training and capacity-building activities now, in anticipation of future hybrid threats. Specific areas of focus should include strengthening capacities in western Balkan and EU Eastern Partnership countries. These efforts would improve capabilities, enhance interoperability, expand situational awareness in different contexts, and eventually equip governments to adopt a more proactive approach. They would also help institutionalize lessons learned and pave the way for deeper coordination during potential crises.

Review resource allocation periodically to support the most effective counter-hybrid capabilities. Another obstacle to proactive counter-hybrid is that it takes time to determine which counter-hybrid capabilities work and secure the necessary resources and personnel. Oftentimes, cumbersome assessment procedures and complex budget requirements also prohibit available resources from reaching desired places. To address this, NATO, the EU, and their national governments should each initiate a detailed review of their budgets. This should include analyses of how funds for specific hybrid-related programs (across the four categories of hybrid challenges) have been used, and the relative impact they have produced. Based on the results, governments and institutions should supplement the most impactful programs with additional resources

45 This is similar to what the US government has tried to do by facilitating cooperation among Dell, Microsoft, AT&T, Nokia, and Ericsson to build an alternative to China's Huawei 5G architecture. See Antonio Villas-Boas, "The US is Making its Own 5G Technology with American and European Companies, and Without Huawei," *Business Insider*, February 4, 2020, https://www.businessinsider.com/5g-huawei-white-house-kudlow-dell-microsoft-att-nokia-ericsson-2020-2.

46 The total defense and comprehensive security concepts adopted by Sweden, Norway, and Finland, as well as Estonia (which channels this approach in a more digitally forward way) provide good examples for other transatlantic countries to emulate where possible, acknowledging constraints on larger and more complex countries.

The 175th Cyberspace Operations Group of the Maryland Air National Guard trains at the Warfield Air National Guard Base. *Photo: US Air Force/J.M. Eddins Jr.*

and expertise, and restructure budget lines as needed to ensure funding flows to untapped areas of potential. Governments and institutions should also explore establishing a common counter-hybrid fund that can be utilized on an as-needed basis by multiple departments working across organizations on hybrid issues. The release of such funds could be contingent upon simple criteria that should incentivize joint efforts among agencies.

Create new legislation and keep it up to date. Proactive approaches are most effective when rooted in strong, pre-existing legal frameworks that guard against hybrid threats. As adversaries and competitors evolve their hybrid activities, governments and institutions must adapt their legislation and legal frameworks accordingly. One good example of this at the national level has been Finland's recent legislation, which requires the Ministry of Defense to review real-estate purchases by nonresidents, to mitigate foreign malign influence based on prior incidents.[47] While NATO, the EU, and nations are making strides, this requires consistent attention. The EU should initiate periodic reviews of hybrid-related legislation to keep it up to date. Though this is difficult to retain over sustained periods of time across bureaucracies facing competing demands and limited resources, national parliaments and the EU should initiate periodic reviews of hybrid-related legislation to keep it updated. Key legislative focus areas pertinent to Russia and China should include:

- creating restrictions on foreign direct investment and engagement in strategic sectors (e.g., energy, telecommunications, electricity, transport, finance);
- mandating governmental review of technology transfers (to China in particular) to reduce pressure on companies;[48]
- creating incentives (e.g., tax write-offs, subsidies) for companies to do business in and with the United States and Europe, as opposed to China or Russia;
- building regulatory standards to encourage the private sector to build resilience, work with governments, and protect and operate critical infrastructures adequately in peacetime and crisis;
- building regulatory standards with the private sector to stem the spread of Russian and Chinese disinformation;
- creating new structures (such as national hybrid fusion centers) and transferring authorities to improve the management of hybrid threats across governments and institutions;
- imposing sanctions in response to Russian and Chinese hybrid actions; and
- fencing off dedicated funds for counter-hybrid efforts, among others.

47 "Non-EU Citizens Will Need Permission to Buy Real Estate in Finland," *Foreigner.fi,* October 28, 2019, https://www.foreigner.fi/articulo/moving-to-finland/non-european-citizens-will-need-special-permit-to-buy-real-estate-in-finland/20191028145549003298.html. For examples of prior incidents, see Andrew Higgins, "On a Tiny Finnish Island, a Helipad, 9 Piers — and the Russian Military?," *New York Times*, October 31, 2018, https://www.nytimes.com/2018/10/31/world/europe/sakkiluoto-finland-russian-military.html.

48 Kramer, *Managed Competition: Meeting China's Challenge in a Multi-vector World*.

To support joint attribution and action:

Leverage emerging technologies such as artificial intelligence. Because hybrid activities take so many forms, it is difficult to anticipate, detect, and analyze all possible threats in all environments. This makes it particularly challenging to identify the perpetrator of a specific hybrid action, share that conclusion, and agree on an appropriate response by NATO or the EU. Standing up national hybrid fusion centers and adopting a campaign-analysis model, as suggested above, would help to improve these capabilities in the short term. Looking to the future, emerging technologies, such as artificial intelligence (AI), can help policymakers achieve faster joint attribution and determine appropriate joint action in complex hybrid scenarios. AI has the unique ability to collect massive amounts of data, including actions and events across the four categories of hybrid threats. If employed correctly, AI can analyze patterns and connections across these social, political, cyber, economic, and other sectors, which individually may appear unrelated but together indicate hybrid activities at work. This data, combined with modeling, games, and other theoretical frameworks, can shed new light on Russian and Chinese hybrid behaviors. Such insight can help analysts determine Moscow and Beijing's specific objectives and potentially help reveal their most likely courses of action. This information can then be utilized to retroactively develop I&W in service of a more proactive approach to prevention and response.

Importantly, this can also help experts create signature footprints, or typical characteristics and distinguishing features specific to Russian and Chinese hybrid tactics, which would be a game changer in enabling collective attribution. Beyond attribution, military leaders, civilian authorities, and governments can also use these tools to support decisions around appropriate precautions or response measures in unilateral and multilateral contexts at new levels of speed and efficiency. NATO, the EU, and transatlantic nations should pool resources and expertise among highly capable countries to further invest in innovation efforts in this vein.[49]

Conduct national interagency exercises based on real hybrid scenarios. To be able to quickly attribute and respond to hybrid activities, governments and institutions need to practice and sharpen these competencies. To do this, governments should prioritize a series of trainings and exercises simulating complex, realistic, and diverse hybrid scenarios related to Russia and China. The exercises should involve all relevant government departments and forces, and, in theory, national fusion centers, as well as civil-society and private-sector stakeholders. Importantly, they should test real-world hybrid scenarios that are similar to events that have actually occurred, as opposed to imagined scenarios which lack complexity and nuance. Yet governments and institutions tend to avoid this, fearing that failure to manage such scenarios will result in public embarrassment.[50] As opposed to tactical considerations, these exercises should focus on political and strategic decision-making, civilian-military interaction, underlying assumptions, and thresholds for action.[51]

Conclusion

While the transatlantic community's response to hybrid threats has improved over the last five years, more progress is needed to effectively deter Russia and China from using hybrid actions. Going forward, Euro-Atlantic governments and institutions need to build a more effective and comprehensive transatlantic counter-hybrid strategy. To that end, this paper suggested five fundamental priorities that could form a common strategic concept to guide transatlantic thinking on hybrid threats. In support of that strategic concept, the recommendations outlined above offer several constructive steps that NATO, the EU, and nations can take, in cooperation with the private sector and civil society, to enhance their counter-hybrid capabilities against Russia and China. These actions range from organizational initiatives at the national and international levels to functional efforts related to resourcing, educating, legislating, and exercising. As hybrid threats intensify for the foreseeable future, including in the aftermath of the coronavirus crisis, transatlantic policymakers should consider this agenda as a pressing priority.

49 In the United States, the Defense Advanced Research Projects Agency (DARPA) was commissioned to develop an AI-enabled system for this purpose called the Collection and Monitoring via Planning for Active Situational Scenarios (COMPASS) program, which is still in development at the time of writing. These types of efforts can help experts create signature footprints, or distinguishing features, specific to Russian and Chinese hybrid tactics. Access to such information about hybrid activities would drastically improve collective attribution and decision-making. NATO, the EU, and transatlantic nations should pool resources and expertise among highly capable countries to further invest in similar innovation efforts.

50 NATO and the EU should adopt this approach for their annual crisis-management exercises (CMXs) to make their hybrid components more realistic and effective.

51 In this spirit, the Hybrid CoE has begun training and capacity-building courses for its member governments, which should be expanded and further resourced.

About the Author

Lauren Speranza is the director of Transatlantic Defense and Security at the Center for European Policy Analysis (CEPA). Lauren is responsible for leading and developing CEPA's work on collective defense and NATO, regional security, and cooperation with allies and partners. Her areas of expertise include transatlantic relations, defense and deterrence in Europe, hybrid warfare, and NATO-European Union relations. She has authored and contributed to several articles and reports on Russian and Chinese hybrid threats, NATO adaptation, US force posture in Europe, and Mediterranean security, which have garnered attention in transatlantic policy circles. She has provided analysis and advice to senior policymakers at NATO, in the EU, and in the US government and Congress. Her work has been featured in several publications and media outlets, including *US News and World Report*, *Bloomberg*, *Defense One*, *Newsweek*, and *Real Clear Defense*. Prior to joining CEPA, Lauren was the deputy director of the Transatlantic Security Initiative at the Atlantic Council, where she managed a robust portfolio of European security and defense programming, policy research, government engagement, and business development. Her focus areas included Nordic-Baltic security, Europe's southern neighborhood, and NATO's future. In this capacity, she also played a leading role in managing NATO's official public diplomacy efforts ("NATO Engages") around the Alliance's 70th anniversary and last three summits. Previously, Lauren worked with start-up Horizon Intelligence as a political and security risk analyst. She also worked with the International Affairs Council in Raleigh and several North Carolina state political campaigns. Lauren has also been a fellow with the Atlantik-Brücke program. Lauren graduated summa cum laude and Phi Beta Kappa from Elon University with a BA in Political Science and International Studies. She also earned an MA in International Security from the Brussels School of International Studies in Belgium, where she graduated as Valedictorian.

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

CHAIRMAN EMERITUS
Brent Scowcroft

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

SECRETARY
*Walter B. Slocombe

DIRECTORS
Stéphane Abrial
Odeh Aburdene
Todd Achilles
*Peter Ackerman
Timothy D. Adams
*Michael Andersson
David D. Aufhauser
Colleen Bell
Matthew C. Bernstein
*Rafic A. Bizri
Linden Blue
Philip M. Breedlove
Myron Brilliant
*Esther Brimmer
R. Nicholas Burns
*Richard R. Burt
Michael Calvey
James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
*Helima Croft
Ralph D. Crosby, Jr.
*Ankit N. Desai
Dario Deste
*Paula J. Dobriansky
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Thomas R. Eldridge
*Alan H. Fleischmann
Jendayi E. Frazer
Courtney Geduldig
Robert S. Gelbard
Thomas H. Glocer
John B. Goodman
*Sherri W. Goodman
Murathan Günal
*Amir A. Handjani
Katie Harbath
John D. Harris, II
Frank Haun
Michael V. Hayden
Amos Hochstein
*Karl V. Hopkins
Andrew Hove
Mary L. Howell
Ian Ihnatowycz
Wolfgang F. Ischinger
Deborah Lee James
Joia M. Johnson
Stephen R. Kappes
*Maria Pica Karp
Andre Kelleners
Astri Kimball Van Dyke
Henry A. Kissinger
*C. Jeffrey Knittel
Franklin D. Kramer
Laura Lane
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mian M. Mansha
Marco Margheri
Chris Marlin
William Marron
Neil Masterson
Gerardo Mato
Timothy McBride
Erin McGrain
John M. McHugh
H.R. McMaster
Eric D.K. Melby
*Judith A. Miller
Dariusz Mioduski
*Michael J. Morell
*Richard Morningstar
Virginia A. Mulberger
Mary Claire Murphy
Edward J. Newberry
Thomas R. Nides
Franco Nuschese
Joseph S. Nye
Hilda Ochoa-Brillembourg
Ahmet M. Oren
Sally A. Painter
*Ana I. Palacio
*Kostas Pantazopoulos
Carlos Pascual
W. DeVier Pierson
Alan Pellegrini
David H. Petraeus
Lisa Pollina
Daniel B. Poneman
*Dina H. Powell McCormick
Robert Rangel
Thomas J. Ridge
Lawrence Di Rita
Michael J. Rogers
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Rajiv Shah
Stephen Shapiro
Wendy Sherman
Kris Singh
Christopher Smith
James G. Stavridis
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
Michael G. Mullen
Leon E. Panetta
William J. Perry
Colin L. Powell
Condoleezza Rice
George P. Shultz
Horst Teltschik
John W. Warner
William H. Webster

**Executive Committee Members*

List as of June 30, 2020

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