Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

NATO PRIORITIES

AFTER THE BRUSSELS SUMMIT

Franklin D. Kramer
Hans Binnendijk
Lauren M. Speranza

NATO PRIORITIES

AFTER THE BRUSSELS SUMMIT

Franklin D. Kramer
Hans Binnendijk
Lauren M. Speranza

This publication has been produced under the auspices of a broader project in partnership with the Royal Norwegian Ministry of Defense focused on Adapting the Alliance.

ISBN-13: 978-1-61977-569-5

November 2018

CONTENTS

EXECUTIVE SUMMARY

At the July 2018 Brussels Summit, NATO sought to enhance its deterrence capacity, warfighting posture, and responses to unconventional challenges in today's complex and evolving security environment. These commitments are comprehensive, and included meeting the allies' 2-percent spending pledge, but the results of these decisions will depend on their implementation. This paper sets forth a policy and programmatic framework for that implementation, proposing four sets of actions that NATO should undertake. To be most effective, these actions should be adopted as part of a broader, coordinated strategy that includes diplomatic, information, and economic efforts, and could be incorporated into the new 2019 NATO Political Guidance. But, as the Brussels Summit concluded, the enhancement of conventional military and counter-hybrid capabilities, including measures to be taken left of crisis, are pressing elements and should be prioritized accordingly.

1. ENHANCING CONVENTIONAL FORCES AND READINESS

NATO's conventional-force upgrade—the "Four 30s" or NATO Readiness Initiative (NRI) announced at the Brussels Summit—should be built around an eastern scenario, with Russia as the adversary. It should also include

- the designation of specific land, sea, air, and enabling forces (including designated combat brigades and fighter aircraft sourced from France, Germany, the United Kingdom, and the United States); and
- a system, established by NATO, for reporting and evaluating key readiness parameters for the units designated to meet the NRI requirements.

a. Land Domain

Military mobility remains a significant concern for effective reinforcement. To address these challenges, the new Joint Support and Enabling Command must strengthen collaboration between military command structures, national governments, and civilian and private-sector authorities by

- establishing a logistical task force to create preplanned infrastructure requirements to support rapid movement, taking into account the significant infrastructure-related actions of the United States through the European Deterrence Initiative (EDI);
- enhancing interaction among Supreme Headquarters Allied Powers Europe (SHAPE) planners and logistics and combatant commands from key nations, such as the United States' European Command (EUCOM) and US Transportation Command;
- supporting and collaborating with the European Union's (EU) ongoing infrastructure program, which may be able to bear significant costs, wherever possible;
- enhancing the military-mobility initiative by creating a diplomatic "green-light" approach, initiated by an official NATO determination to move forces, which will then allow movement via pre-planned routes with pre-planned support, without further national action; and
- coordinating with the civilian sector to develop plans to support rapid movement of forces and equipment. (This could be based on existing models, such as the US Civilian Reserve Air Fleet and the Voluntary Intermodal Sealift Agreement.)

b. Sea Domain

Maritime lines of supply, transit, and communication from the United States to Europe will be an important part of NATO's reinforcement strategy in a sustained contingency with Russia. In this regard, NATO should

- clarify the relationship between Maritime Command (MARCOM) and NATO's three Joint Force Commands (Bursum, Naples, and Norfolk), particularly during a transition to wartime;
- enhance air-sea doctrine and planning mechanisms to provide the Alliance with a multidomain strategy in the North Atlantic Ocean, Baltic, Arctic, and Mediterranean Seas; and
- develop anti-submarine warfare (ASW) and unmanned underwater vehicles (UUV) capabilities and planning to protect sea lines of communica-

tion, including deployment of forces and protection of undersea cables.

c. Air Domain

The Alliance's air power represents the quickest source of deployable firepower. NATO should enhance its capacity in the air domain by

- creating an integrated multidomain approach including sensors, robotics, and other advanced technology, supported by required infrastructure, adaptive basing, and logistics;
- procuring sufficient stocks of precision-guided air-launched anti-armor and anti-cruise-missile munitions;
- enhancing air-sea planning and doctrine; and
- coordinating with civilian authorities to expand shared access to airspace and infrastructure.

2. STRENGTHENING CYBER DEFENSE AND RESILIENCE

Enhancing the resilience and defense of allies' operational and informational networks and critical infrastructure is a key priority for the Alliance, as outlined at the Brussels Summit. To improve NATO's cybersecurity for hybrid scenarios and conventional contingencies, NATO should

- encourage key cyber-capable framework nations, such as the United Kingdom, Germany, Canada, and the United States, to provide support to frontline states to improve the resilience of the critical infrastructures key to mission assurance;
- designate cyber resilience as a critical mission of the Joint Support and Enabling Command to support transportation and logistics mission assurance;
- integrate cyber into NATO's overall set of capabilities, through the development of the Cyber Operations Center; and
- establish a Combined Joint Task Force (CJTF) of nations providing cyber effects with a three-part mandate: capabilities coordination; operational-concept development, including interaction with non-cyber capabilities; and establishment of doctrine to include legal requirements.

3. COUNTERING HYBRID CHALLENGES

As NATO meets the challenge of enhancing its conventional-deterrent posture, Russia is already increasingly concentrating on hybrid attacks. To optimize the capacity to respond to hybrid challenges, NATO should:

- undertake planning to include the potential for significantly increased hybrid attacks at what might be called "Level 2" hybrid (i.e., still short of "armed attack" under the Washington Treaty, and yet more substantial than ongoing hybrid activities that might be called "Level 1").
- fully resource the Counter Hybrid Support Teams (CHSTs), established at the Brussels Summit, to undertake preparation and response activities. To ensure the new initiative is utilized to its full potential, NATO should
    - develop a command-and-control mechanism to coordinate CHSTs, NATO special-operations forces, and, as appropriate, national and EU counter-hybrid capabilities;
- ensure increased awareness through the development of intelligence and a system of indications and warnings focused on hybrid;
- elevate energy security and critical-infrastructure protection as core elements of NATO and NATO-EU exercises, with an enhanced focus on chemical attacks; and
- create a playbook of potential collective countermeasures that could be undertaken by allies in hybrid scenarios, based on the law of countermeasures.

4. UPDATING STRATEGIC PLANNING

To continue the NATO adaptation efforts emphasized at the Brussels Summit, NATO's two strategic commanders, namely the Supreme Allied Commander Europe (SACEUR) and Supreme Allied Commander Transformation (SACT), should be tasked with updating strategic planning to reflect today's security environment.

- SACEUR should be tasked with developing a comprehensive plan for the defense of NATO territory, including a review of whether, and how, force postures should be enhanced to counter threats to NATO's east and south. SACEUR should deter-

mine the requirements of the greatest need—for example, whether enablers such as air defense or prepositioned equipment, structural requirements such as airfields, and resilience for critical infrastructures would be most valuable, and/or if permanently stationing land-combat formations should be a strategic focus. The strategic response might differ between geographic areas, but the following elements should be considered, particularly regarding NATO's posture to the east:

  - The United States' EDI is already providing substantial funding for land- and air-force enablers, and there appear to be strong reasons for NATO to continue to station land-force enablers in the east and implement the concept of adaptive basing for air forces as important elements of NATO's strategy of reinforcement.

  - The US Congress has required the Secretary of Defense to report on the value of increased presence in the east, and the SACEUR, in his role as commander of European Command, will presumably provide analysis on these issues.

  - While nations can undoubtedly agree on a bilateral basis for the stationing of forces, and the United States has significant forces stationed in various places across the Alliance, there are potential political issues—particularly regarding the possibility of stationing substantial permanent forces in the east.

  - Accordingly, if the Secretary of Defense and/or the SACEUR determined that, as a matter of military judgment, forces should be expanded in the east or south, this would provide the basis for consultations, both at NATO and bilaterally, with a focus on enhancing deterrence through both military capabilities and Alliance unity.

  - SACEUR should also evaluate the impact of Russian capabilities in the Arctic, Atlantic, and the south, including in the Mediterranean and Syria, and the implications for force posture and warfighting capabilities.

- SACEUR should analyze and develop tactics, techniques, and procedures (TTPs), focusing on the potential transition from hybrid conflict to armed attack. TTPs should include indication-and-warning systems, flexible deterrent options, and responses to unconventional actions such as an adversary's use of chemical weapons and special-operations forces. Once developed, such TTPs would be transitioned for use.

- SACT should utilize Allied Command Transformation's (ACT) force-planning and training capacities to integrate transformational technologies into the Alliance's warfighting capabilities. SACT should utilize gaming, simulation, and training opportunities to determine how to establish asymmetrical capabilities, as well as TTPs that will allow the Alliance to overmatch Russia or other peer or near-peer competitors.

INTRODUCTION

At the July 2018 Brussels summit, NATO sought to enhance its deterrence capacity, warfighting posture, and responses to unconventional challenges in today's complex and evolving security environment. In doing so, NATO built upon a foundation laid at the Wales and Warsaw Summits. In Brussels, allies committed not only to increased spending to meet the NATO 2-percent pledge, but to important improvements in readiness and reinforcement for air, land, and naval forces.[1] They also agreed to adopt an increased focus on the challenges of cyber and hybrid conflict. The commitments are comprehensive, but the results of these decisions will depend on effective implementation. This paper sets forth a policy and programmatic framework for that implementation, proposing four sets of actions that NATO should undertake. To be most effective, these actions should be adopted as part of a broader, coordinated strategy that includes diplomatic, information, and economic efforts, and could be incorporated into the new 2019 NATO Political Guidance. But, as the Brussels Summit concluded, the enhancement of conventional military and counter-hybrid capabilities, including measures to be

1 NATO, press release, "Brussels Summit Declaration," July 11, 2018, paragraph 3, https://www.nato.int/cps/en/natohq/official_texts_156624.htm.

taken left of crisis, are pressing elements and should be prioritized accordingly.

First, NATO's conventional-force upgrade—the so-called "Four 30s" or NATO Readiness Initiative (NRI)—should be built around an eastern scenario, with Russia as the adversary.[2] NATO should designate specific land, air, naval, and enabling forces (particularly from France, Germany, the United Kingdom, and the United States) and have the certified capabilities and readiness to employ those forces to accomplish necessary reinforcement in less than thirty days. NATO Force Integration Units (NFIUs) may need to be upgraded accordingly. The new Joint Support and Enabling Command and the Joint Force Command Norfolk should be structured and resourced, including with the required infrastructure, to ensure that both continental European and North American reinforcement can be achieved. Air and naval power will require an integrated, multidomain approach including sensors, robotics, and other advanced technology supported by required infrastructure, adaptive basing, and logistics.

Second, NATO's cyber defenses and capacity for cyber effects should be strengthened through three initiatives: support to frontline states from the Enhanced Forward Presence (eFP) framework nations—the United States, Canada, Germany, and the United Kingdom—each with advanced cyber capabilities; making cyber resilience a critical mission of the new Joint Support and Enabling Command; and integrating cyber into NATO's overall set of capabilities, through the development of the new Cyber Operations Center and the establishment of a Combined Joint Task Force of nations providing cyber effects.

Third, NATO should enhance its efforts to counter hybrid challenges in five ways: 1) Planning should include the potential for significantly increased hybrid attacks at what might be called "Level 2" hybrid (i.e., still short of "armed attack" under the Washington Treaty, and yet more substantial than ongoing hybrid activities that might be called "Level 1"); 2) fully resource and fully utilize Counter Hybrid Support Teams (CHSTs) to undertake preparation-and-response activities, and develop an appropriate command-and-control mechanism to coordinate CHSTs, NATO special-operations forces, and, as appropriate, national and European Union (EU) counter-hybrid capabilities; 3) ensure increased awareness through the development of intelligence, and a system of indications and warnings focused on hybrid; 4) elevate energy security and critical-infrastructure protection as core elements of NATO and joint exercises between and among NATO, the EU, and the private sector, which should also include an enhanced focus on chemical attacks; and 5) create a playbook of potential collective countermeasures, to complement sanctions, that allies could undertake in hybrid scenarios.

Fourth, each strategic commander—Supreme Allied Commander Europe (SACEUR) and Supreme Allied Commander Transformation (SACT)—should be asked to update strategic planning.

SACEUR should be tasked with developing a comprehensive plan for the defense of NATO territory, including a review of whether, and how, force postures should be enhanced for the east and/or the south. SACEUR should determine the nature of the greatest needs, and how that might differ among potential geographic areas. The United States European Deterrence Initiative (EDI) is already providing substantial funding for land- and air-force enablers, and there appear to be strong reasons for NATO to continue to station land-force enablers in the east and implement the concept of adaptive basing for air forces as important elements of NATO's strategy of reinforcement. The United States Congress has required the Secretary of Defense to report on the value of increased presence in the east, and the SACEUR, in his role as commander of European Command, will presumably provide analysis on these issues. While nations can undoubtedly agree on a bilateral basis for the stationing of forces, and the United States has significant forces stationed in various places across the Alliance, there are potential political issues—particularly regarding the possibility of stationing substantial permanent forces in the east. Accordingly, if the Secretary of Defense and/or the SACEUR determined that, as a matter of military judgment, forces should be expanded in the east or south, this would provide the basis for consultations, both at NATO and bilaterally, with a focus on enhancing deterrence through both military capabilities and Alliance unity.

SACEUR should also analyze and develop tactics, techniques, and procedures (TTPs), including through experimentation, focusing on the potential transition from hybrid conflict to armed attack. These should include indications and warnings, flexible deterrent options, and responses to unconventional actions, such as an adversary's use of chemicals or

2 Ibid., paragraph 14.

special-operations forces. Once developed, such TTPs would be transitioned into use.

SACT should utilize NATO Allied Command Transformation's (ACT) force-planning and training capacities to integrate transformational technologies into the Alliance's warfighting capabilities. SACT should utilize gaming, simulation, and training opportunities to determine how to establish asymmetrical capabilities and TTPs that will allow the Alliance to overmatch Russia or other peer or near-peer competitors.

ENHANCING CONVENTIONAL READINESS

The Brussels Summit Declaration underscored the "strategic importance to increase responsiveness, heighten readiness, and improve reinforcement" in order to "ensure that the Alliance's deterrence and defence posture remains credible, coherent, and resilient."[3] The key approved actions to this end include:

- "Allies will offer an additional thirty major naval combatants, thirty heavy or medium maneuver battalions, and thirty kinetic air squadrons, with enabling forces, at thirty days' readiness or less."[4]
- "Shorten border crossing times and…provide diplomatic clearances for land, sea, and air movement within five days by the end of 2019."[5]
- "[Establish] a Joint Force Command Norfolk headquarters in the United States to focus on protecting the transatlantic lines of communication, and a Joint Support and Enabling Command in Germany to ensure freedom of operation and sustainment in the rear area in support of the rapid movement of troops and equipment into, across, and from Europe."[6]

A good deal of unclassified analysis, much of it by the RAND Corporation, supports the position that a force of approximately thirty heavy or medium battalions and thirty fighter/fighter-attack squadrons would be an effective, prompt reinforcement force against a Russian attack from the east. For example, a 2016 RAND analysis argued, "a force of about seven brigades, including three heavy armored brigades—adequately supported by airpower, land-based fires, and other enablers on the ground and ready to fight at the onset of hostilities—could suffice to prevent the rapid overrun of the Baltic states."[7] In terms of air capabilities, another study indicated that twenty-eight fighter/fighter-attack squadrons would be crucial as early-arriving forces for a large-scale conflict.[8] With respect to naval forces, the Alliance is also determined to "reinvigorate our collective…anti-submarine warfare (ASW), amphibious operations, and protection of sea lines of communications."[9]

With the summit having established NATO's objectives, the fundamental issue now is what actions will be required for NATO forces to achieve those goals, and to sufficiently meet a Russian conventional challenge from the east. To this end, NATO should consider the following six requirements.

First, to move quickly, forces must know where they are going. That means that their destinations should be pre-planned for given scenarios, and the necessary command and logistical arrangements should be established and trained against. The goal should be for these forces to arrive on station and be ready for employment no later than thirty days after a decision is reached—and, preferably, sooner. More specifically, for the eastern scenario, NATO should adopt a designated-force approach, rather than a rotating or force-generation conference "pickup" approach. To accomplish this, lead nations with the greatest capabilities ought to handle particular sectors, and then have other nations integrate with them. Practically, the United States, France, Germany, and the United Kingdom should take the reinforcement lead, with Poland also playing an important role. Smaller nations, or those geographically farther away from the conflict, should then plan to work with the lead nations. All of this should be done under the auspices

3 Ibid., paragraph 12.

4 Ibid., paragraph 14.

5 Ibid., paragraph 17.

6 Ibid., paragraph 29.

7 David A. Shlapak and Michael W. Johnson, *Reinforcing Deterrence on NATO's Eastern Flank* (Santa Monica, CA: RAND Corporation, 2016), pp. 1-2, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1200/RR1253/RAND_RR1253.pdf.

8 David Ochmanek, Peter A. Wilson, Brenna Allen, John Speed Meyers, and Carter C. Price, *U.S. Military Capabilities and Forces for a Dangerous World* (Santa Monica, CA: RAND Corporation, 2017), p. 47, https://www.rand.org/pubs/research_reports/RR1782.html.

9 NATO, "Brussels Summit Declaration," paragraph 19.

of common NATO command and control, and NATO plans should closely align with national planning.

The United States currently maintains three Army brigade combat teams[10] in Europe, with the prepositioned US Marine Corps equipment and rotational presence in Norway potentially providing a fourth.[11] Adding one brigade each from France, Germany, Poland, and the United Kingdom would get NATO close to the designated total. Forces from countries such as the Netherlands, Denmark, and Norway would provide significant additional warfighting capability. Taken together with supplemental US forces that could promptly arrive from the continental United States, the overall force would be capable of blunting an initial Russian challenge, especially if leaders pay attention to strategic warnings, and if they regularize the requirements for prompt movement (as further discussed below). Since speed of movement is critical, it would be particularly valuable if the SACEUR, in combination with the Secretary General, would have pre-delegated authority to move key elements, particularly enablers, necessary to enable prompt reinforcement.

It is important to note that a designated-force approach would require a change in terms of the current NATO Response Force (NRF) and Very High Readiness Joint Task Force (VJTF), as designated forces focused on the east could not simultaneously be available for NRF or VJTF multi-scenario roles. A revised NRF could act as a second-wave force for an eastern scenario, or as a force for use elsewhere. The VJTF could be maintained as a first-wave light force, likely focused on crisis management. This would require forces different from those to be designated as first responders for the east.

Second, given most allied forces' low states of readiness, there are high-priority demands for munitions, stores, and other materiel, as well as logistical support. Resolving such deficiencies is straightforward, requiring purchases of needed materiel and programming to meet logistical demands. Still, it is important to recognize that, as indicated in a 2017 RAND report, it would currently take several weeks to a month for France and Germany to send even one brigade to the east, and even more time for the United Kingdom.[12] Similarly, the German parliamentary armed-forces commissioner has repeatedly found a significant lack of readiness for German forces.[13] This lack of speed and readiness undercuts both deterrence and warfighting capacity. While nations must make the purchasing and programming decisions, NATO should establish a system for reporting, evaluating, and certifying key readiness parameters—at a minimum, for the forces that will be designated to meet the NRI requirements—to help ensure that reinforcing forces can actually meet contingency requirements.

Third, transportation and infrastructure requirements must be pre-planned and able to support rapid movement. The United States, through the European Deterrence Initiative, is undertaking significant expenditures for such requirements, including ammunition and bulk storage, airfield enhancements, deployable air-base capabilities, and prepositioning of materiel. In fiscal year 2017-2019 US Department of Defense budgets, such authorized expenditures exceeded $8.7 billion.[14] The Alliance, as a whole, is also taking action through the new command structures and by working with the EU. As noted, the Alliance has determined to establish a Joint Support and Enabling Command in Germany "in support of rapid movement" of forces. NATO and the EU have also collaborated under Dutch leadership on a "military mobility" initiative, with the current target of providing diplomatic clearance for force movements in five days.[15] The EU is also leading a project under Permanent and Structured Cooperation (PESCO) on the creation and utilization of strategic and logistical hubs, for which NATO drives the requirements that are then supported by the EU. Each of these initiatives needs to be further developed and doing so will significantly enhance deterrence. Germany should establish requirements for force-movement planning, including by air, road, rail, and ship, with rail and sea having high priority. In doing so, planners should interact with key nations that will move major forces first, including European Command for the United

10 The US also deploys an Army Combat Aviation Brigade in Europe.

11 One permanently deployed in each Germany and Italy, and a third on a rotational basis, primarily in Poland.

12 Michael Shurkin, *The Abilities of the British, French and German Armies to Generate and Sustain Armored Brigades in the Baltics* (Santa Monica, CA: RAND Corporation, 2017), p. 9, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1600/RR1629/RAND_RR1629.pdf.

13 "Germany's Lack of Military Readiness 'Dramatic,' Says Bundeswehr Commissioner," *Deutsche Welle*, February 20, 2018, https://www.dw.com/en/germanys-lack-of-military-readiness-dramatic-says-bundeswehr-commissioner/a-42663215.

14 US Department of Defense, "Department of Defense Budget Fiscal Year (FY) 2019," February 2018, European Deterrence Initiative' vice Defense , p.1, https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2019/fy2019_EDI_JBook.pdf.

15 NATO, "Brussels Summit Declaration," paragraphs 17-18.

States and US Transportation Command, which have extensive mobility and logistical experience, as well as with planners from NATO Supreme Headquarters Allied Powers Europe. Germany should establish a logistical task force to develop the necessary coordination. If experimentation would be useful, SACT could provide required support.

Beyond that, NATO and the Joint Support command will need to decide upon required infrastructure upgrades. They will need to work closely with the EU, which has an ongoing infrastructure program and may be able to bear significant costs, especially given the substantial overlap of NATO and EU nations. The military-mobility initiative should also be further developed to shorten the time for moving forces, by creating a diplomatic "green-light" approach. Under this approach, once NATO decided to move forces, they could then move without further national action via preplanned routes, with preplanned support. Notably, rapid movement will rely on the civil sector; in this regard, the US Civil Reserve Air Fleet and the Voluntary Intermodal Sealift Agreement programs may be useful models.[16]

Fourth, the Brussels Declaration states, "In the air domain, we have agreed on a Joint Air Power Strategy."[17] While the actual employment of forces in battle requires operational decisions that SACEUR must determine, a successful strategy requires a series of preoperational actions. Those include designation of forces, as noted above, as well as logistical efforts to make the forces effective. As previously proposed, the initial "NATO air presence…[should be] built around the combat capabilities of US, French, German, and UK forces."[18] The combined forces of these nations significantly exceed the thirty-squadron requirement, and other nations can also provide air forces.[19] But, force structure is not enough, as air power must be "fully supported with the necessary ready airfields, sufficient and sustainable munitions and other required logistical capabilities (fuel, storage, etc.), as well as appropriate air and other airfield defenses."[20]

Several actions are already under way in this realm. As noted above, a significant portion of the funding from the US EDI will go to enhanced air capabilities, including increased presence, exercises, and training, as well as infrastructure and prepositioning. European nations should likewise undertake readiness initiatives, with direction coming from SHAPE planners. All air forces will need effective precision-guided anti-armor and anti-cruise-missile munitions. There should be special focus on innovative concepts such as adaptive basing, as exemplified by the Deployable Air Base System (DABS), which provides for quickly upgrading an unimproved field to mission readiness.[21] Similarly, in Europe's crowded environment, one "required capability" set forth in the Joint Air Power Strategy is "enhanced coordination between military and civil authorities, including shared access to airspace and infrastructure."[22] Any airfield to be used in wartime will need at least some capacity for hardened shelters, and will also require effective air defense. The ability to place airpower at multiple locations will greatly complicate any Russian attempt to degrade the force, whether by cruise missile or other attack, and is consistent with the concept of being "operationally unpredictable," as set forth in the US National Defense Strategy.[23]

Overall, a more integrated approach to air power is needed. General Philip Breedlove, a recently retired SACEUR, has elaborated these points, noting, "Effective air defense in northern Europe must start with a thick sensor network and then rely on both ground-based assets and aviation, along with robust command and control, all exercised in a joint setting."[24] His specific suggestions include creating a regional approach for the frontline states, adding an air-defense element to the enhanced-presence forces,

16 US Transportation Command, "Intermodal Programs," https://www.ustranscom.mil/imp/index.cfm; US Air Force Air Mobility Command, "Civil Reserve Air Fleet," April 26, 2017, https://www.amc.af.mil/About-Us/Fact-Sheets/Display/Article/144025/civil-reserve-air-fleet/.

17 NATO, "Brussels Summit Declaration," paragraph 19; NATO, "NATO's Joint Air Power Strategy," June 26, 2018, https://www.nato.int/cps/en/natohq/official_texts_156374.htm.

18 Franklin D. Kramer and Hans Binnendijk, *Meeting the Russian Conventional Challenge* (Washington, DC: Atlantic Council, 2018), p. 2, http://www.atlanticcouncil.org/images/publications/Meeting_Russian_Conventional_Challenge.pdf.

19 Ibid., p. 14.

20 Ibid., p. 15.

21 US Department of Defense, "Department of Defense Budget Fiscal Year (FY) 2019, European Deterrence Initiative" p. 12.

22 NATO, "NATO's Joint Air Power Strategy," paragraph 39.

23 US Department of Defense, *Summary of the 2018 National Defense Strategy of the United States* (Washington, DC: Department of Defense, 2018), p. 5, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

24 General Philip Breedlove was NATO's Supreme Allied Commander Europe (SACEUR) from 2013–2016. See Philip M. Breedlove, *Toward Effective Air Defense in Northern Europe* (Washington, DC: Atlantic Council, 2018), p. 1, http://www.atlanticcouncil.org/images/publications/Toward_Effective_Air_Defense_in_Northern_Europe.pdf.

integrating sea-based air into the air-defense task, increasing the availability of sensors, and undertaking regular exercises.[25] All these elements should be part of implementing the NATO air-power strategy.

Fifth, the establishment of Joint Force Command Norfolk, as well as the focus on ASW, amphibious operations, and protecting the sea lines of communication all underscore the need for an enhanced Alliance naval effort. The resurrection of the US Second Fleet is an important contribution to this effort. Of course, the Alliance has a significant naval-exercise schedule, but several other actions should be undertaken for enhanced deterrence and effective warfighting.[26] First, an integrated battle plan, including a clear chain of command, needs to be established. One important issue to resolve is the relationship of Maritime Command, situated in the United Kingdom, and the three Joint Force Commands (Brunssum, Naples, and Norfolk)—especially in the transition to, and in the context of, a wartime setting, including the allocation of required forces. Second, NATO's Joint Force Commands should be further enhanced to operate as true joint warfighting commands. Accordingly, building on General Breedlove's recommendation of integrating naval forces into air defense, a broader air-sea effort should be undertaken. This is consistent with the Joint Airpower Strategy, which underscores the multidomain nature of warfare and the need to integrate air and sea activities. By way of example, air capabilities can be an element of cruise-missile defense for maintaining the sea lines of communication, and naval capabilities can provide offense against key adversary assets. In a crisis, the Alliance's response would build over time with the requirement to generate forces as promptly as possible. Given the logistical challenges of moving land forces, the need for maritime and air assets, as well as an air-sea approach, becomes even more critical. Third, the new Joint Force Command Norfolk will need the most advanced ASW assets and must develop an operating strategy for their effective use. Such an approach should not only be counterforce, but should also include assurance of resilience for critical undersea cable assets. Funding from EDI has already been designated for "Integrated Undersea Surveillance System (IUSS) infrastructure improvements, operational support, and battlespace preparation…[including] purchasing new, fixed undersea surveillance systems and refurbishment of older, existing systems…[to] greatly enhance surveillance of key threat submarine transit areas within the USEUCOM AOR."[27] Underwater unmanned vehicles operating as sensors, counterforce, and repair may also play key roles, especially as technology advances.[28] Finally, while SACEUR will need to determine battle plans, it will likely be important to plan to fight in the waters of the north—to ensure that adversary forces do not have sanctuary, and to disrupt, as much as possible, long-range cruise-missile and other attack capabilities coming from the sea.

Finally, NATO should review the mission and structure of the current NATO Force Integration Units. These units are deployed in eastern allies, with the mission of preparing the way for NATO reinforcements. As the size of NATO's highly ready forces increases, these NFIUS' mission will expand, and should be coordinated with NATO command-and-control arrangements. Their mission might also be augmented to define what they would do in wartime after reinforcements arrive.[29]

STRENGTHENING CYBER DEFENSE AND RESILIENCE

In an armed attack against NATO, Russia would almost certainly utilize its cyber capabilities as part of the onslaught. Those efforts would be directed against NATO military forces, as well as critical-infrastructure capabilities including telecommunications, power, transportation, and reception facilities. A significant cyberattack could, of course, directly disrupt military capabilities. Even a limited incursion could disrupt interoperability if, for example, Russian attackers infiltrated less-capable cyber countries and worked their way through the NATO networks and into other militaries via combined activities (such as a combined air-operations center). Likewise, attacks against critical infrastructure could mean that military capabilities reliant on the electric grid would be disrupted; similarly, transportation and reception facilities depend on critical infrastructure being operational. In sum, having an effective cyber posture is as critical to successful defense as are conventional military capabilities. Currently, NATO and its member countries have not

25 Ibid., p. 5.

26 NATO Allied Maritime Command, "2018 Exercises," https://mc.nato.int/media-centre/news/2018.aspx?cat=133.

27 US Department of Defense, "Department of Defense Budget Fiscal Year (FY) 2019, European Deterrence Initiative" p. 4.

28 At the October 2018 Defense Ministers meeting, thirteen allies signed a memorandum of understanding to promote cooperation on unmanned undersea vehicles. See NATO, "Thirteen Allies to Cooperate on the Introduction of Maritime Unmanned Systems," October 3, 2018, https://www.nato.int/cps/en/natohq/news_158672.htm.

29 Based in part on interviews with NFIU commanders.

reached the necessary level of cyber effectiveness. NATO underscored the importance of cyber at the 2018 summit, taking several steps as "part of NATO's core task of collective defence," including:

> *"Establish[ing] a Cyberspace Operations Centre in Belgium to provide situational awareness and coordination of NATO operational activity within cyberspace" and "integrat[ing] sovereign cyber effects, provided voluntarily by Allies, into Alliance operations and missions..."*[30]

What NATO has done is valuable, but what it has not yet done is far more important for effective defense. As noted above, an attack against NATO would almost certainly include an attack against critical infrastructures, which are extremely vulnerable to cyber intrusions. There are multiple examples of Russian attacks against critical infrastructure (as in Ukraine[31]), or penetration of key assets like the electric grid (as in the United States).[32] For a successful deterrence posture, NATO needs to increase the resilience of critical infrastructures, both in the frontline states and those required for reinforcement elsewhere, as well as to enhance its capacity for cyber effects. To accomplish this, it should undertake three major efforts.

First, for the frontline states, NATO should establish "cyber collective defense, where the framework nations (the United Kingdom, Canada, Germany, United States) leading the eFP in the Baltics and Poland assist those nations in establishing enhanced cyber resilience for their telecommunications, electric grids, and reception facilities that are critical to warfighting and thus a key requirement for deterrence."[33] Those framework nations would work with each of the frontline states to develop the operational procedures to respond to an attack, and put in place advanced capabilities that would limit the consequences of such an attack, through enhanced resilience and the ability to recover.[34] This should be done at the national level, and is fully consistent with the recently released *Department of Defense Cyber Strategy Summary,* which states, "The Department will prioritize...deterring malicious cyber activities that constitute a use of force against the United States, our allies, or our partners."[35] Among other actions, this strategy also asserts, "The Department will work to strengthen the capacity of these allies and partners and increase DoD's ability to leverage its partners' unique skills, resources, capabilities, and perspectives."[36] The US Congress has likewise prioritized such actions, stating in section 1281 of the 2019 National Defense Authorization Act that the Secretary of Defense shall provide a report by March 2019 on US actions at NATO "to build cyber-defense capacity and deter cyber-attacks among Organization member countries."[37] To be clear, nations assisting frontline states would not undertake operational control of any critical infrastructures; these would continue to be run under the framework established by the host nation.

Second, the Joint Support command needs to include cyber resilience as part of its operational concept, with speed of movement and resilience considered together. For example, there is little point in having a plan for rail and air transportation if such a plan can be easily disrupted by cyberattack. Resolving this

30 NATO, "Brussels Summit Declaration," paragraph 20.

31 White House, "Statement from the Press Secretary," February 15, 2018, https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/.

32 US-CERT, "Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," March 15, 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A.

33 Kramer and Binnendijk, *Meeting the Russian Conventional Challenge,* p. 2.

34 For a useful reference setting forth multiple actions that can be taken in the context of the United States, see Paul N. Stockton, *Resilience for Grid Security Emergencies* (Baltimore, MD: Johns Hopkins, 2018), http://www.jhuapl.edu/Content/documents/ResilienceforGridSecurityEmergencies.pdf.

35 US Department of Defense, *Summary: Department of Defense Cyber Strategy 2018* (Washington, DC: Department of Defense, 2018), p. 4, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

36 Ibid., p. 5.

37 Section 1281 provides:
"(a) In General.—Not later than March 31, 2019, the Secretary of Defense shall submit to the congressional defense committees a report detailing the Department's efforts to enhance the United States' leadership and collaboration with the North Atlantic Treaty Organization with respect to the development of a comprehensive, cross-domain strategy to build cyber-defense capacity and deter cyber-attacks among Organization member countries.
(b) Contents. —The report required by subsection (a) shall address the following:
(1) Improving cyber situational awareness among Organization member countries.
(2) Implementation of the cyber operational-domain roadmap of the Organization with respect to doctrine, political oversight and governance, planning, rules of engagement, and integration across Organization member countries.
(3) Planned cooperative efforts to combat information warfare across Organization member countries.
(4) The development of cyber capabilities, including cooperative development efforts and technology transfer.
(5) Supporting stronger cyber partnerships with non-Organization member countries, as appropriate."

problem requires improvements not only in capabilities, but also in bureaucracies. As is regularly recognized, critical-infrastructure assets are owned and regulated by multiple entities—private, governmental, and multinational. While coordination has significantly improved between NATO and the EU, an effective resilience posture will require a combined effort including both organizations, as well as relevant nations and the private sector. The June 2018 EU *Joint Report to the European Parliament, the European Council, and the Council* sets forth a number of ways in which the EU and NATO are cooperating.[38] Given the critical importance of logistics for deterrence and warfighting, and the reliance of logistical assets on cyber capacities, the Joint Support command should spearhead the creation of a joint task force, which would develop pre-crisis cyber requirements. These would focus on high-end conflict and be put in place by the relevant governing entities, including nations, NATO, and the EU. There are several ways in which a joint task force could be established, but, for planning purposes, it would make sense for it to be linked to the new Cyber Operations Center created as part of SHAPE, given that SHAPE will likely have overall strategic responsibility for NATO wartime cyber efforts. The joint task force could also link operationally with the Cyber Operations Center in wartime, if the necessary procedures are put in place. In this context, it would be valuable for the Cyber Operations Center to a) be able to obtain information related to critical infrastructure protection from nations and other relevant stakeholders, including network operators and service providers, and b) have designated points of contacts within each nation responsible for this information. Utilizing such connectivity, the Cyber Operations Center could work with national points of contact to identify, prioritize, and remediate vulnerabilities.

Third, at the Brussels Summit, NATO agreed to establish effective cyber effects by integrating highly cyber-capable nations' capacities into NATO planning and operations.[39] This could include offensive cyber operations as a means of deterrence. For the United States, integrating cyber operations has been done using a joint task force.[40] While NATO could achieve this in several ways, creating such a combined joint task force (CJTF) for cyber—under the auspices of the new Combined Operations Center at SHAPE—would be a good first step, given the need to incorporate multiple national capabilities and to connect offensive and defensive capabilities and actions. If classification issues limited the value of acting at the NATO level, the United States could consider working with close cyber allies, starting with the United Kingdom, and including others as circumstances deem appropriate. Whether at NATO or at the national level, such a CJTF could have a three-part mandate: capabilities coordination; operational-concept development, including interaction with non-cyber capabilities; and establishment of a doctrine to include legal requirements. With respect to the latter, an important legal consideration will be how to respond to adversarial actions that put key assets at risk prior to the onset of armed conflict, such as Russian intrusion into the electric grid and other critical infrastructure. Those issues, including the law of countermeasures, are further discussed in the section on hybrid conflict below.

COUNTERING HYBRID CHALLENGES

As NATO meets the challenge of enhancing its conventional-deterrent posture, Russia is increasingly concentrating on hybrid attacks. Russia's actions range from low-level conflict and cyberattacks to disinformation and political and economic subversion and coercion, all of which could be considered strategic intimidation.[41] Recent targeted chemical attacks in the United Kingdom demonstrated a higher degree of aggressiveness from Russia, and resulted in death.[42] In March 2018, the US government announced that Russia had orchestrated cyber operations targeting US critical infrastructure, including nuclear power plants and water and electric systems, potentially enabling Russia to manipulate these facilities.[43] The head of Germany's domestic intelligence service reported

38 European Commission, *Joint Report to the European Parliament, the European Council and the Council* (Brussels: European Commission, 2018), https://eeas.europa.eu/sites/eeas/files/joint_report_on_the_implementation_of_the_joint_framework_on_countering_hybrid_threats_from_july_2017_to_june_2018.pdf.

39 NATO, "Brussels Summit Declaration," paragraph 20.

40 See, for example, Lieutenant General Paul M. Nakasone, commander of United States Army Cyber Command, statement before the Subcommittee on Cybersecurity, Senate Committee on Armed Services, p. 3, https://www.armed-services.senate.gov/imo/media/doc/Nakasone_03-13-18.pdf.

41 Franklin D. Kramer and Lauren M. Speranza, *Meeting the Russian Hybrid Challenge* (Washington, DC: Atlantic Council, 2017), http://www.atlanticcouncil.org/images/publications/Meeting_the_Russian_Hybrid_Challenge_web_0530.pdf.

42 Richard Pérez-Peña and Ellen Barry, "UK Charges 2 Men in Novichok Poisoning, Saying They're Russian Agents," *New York Times*, September 5, 2018, https://www.nytimes.com/2018/09/05/world/europe/russia-uk-novichok-skripal.html.

43 US-CERT, "Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors"; Nicole Perlroth and David Sanger, "Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says," *New York Times*, March 15,

Russian attempts at attacking German critical infrastructure.[44] From March 2018, after losing a Stockholm arbitration court ruling costing Russia's state-controlled energy company Gazprom $2.5 billion, the Kremlin shut off natural-gas supplies to Ukraine, resulting in significant shortages and challenges for Ukraine.[45] Most recently, following Macedonia's invitation to begin accession talks with NATO and ahead of its crucial name-change referendum, Russia undertook a significant disinformation campaign to undercut Macedonia's accession.[46]

While Russia's current activities are substantial, it is important to recognize that hybrid attacks could reach much more significant levels than current cases, without reaching the level of "armed attack" under the Washington Treaty, which calls for an Article 5 response. By way of example, and in comparison, to current adversarial actions—which might be considered "Level 1" hybrid—suppose the Salisbury attack in the United Kingdom had instead involved seven different, but near-simultaneous, instances of chemical attacks across three countries instead of one—or, alternatively, five or six instances in which grid generators were simultaneously disabled in different countries. Those examples might be considered "Level 2" hybrid, with hybrid in the context of armed attack being "Level 3." Given this, NATO, EU, and national planning for hybrid challenges needs to encompass the potential for higher Level 2 attacks that could well be undertaken, in addition to the current Level 1 cases.

The Alliance has recognized the challenge of hybrid and has taken several significant steps. At the Warsaw Summit in July 2016, NATO Secretary General Jens Stoltenberg, European Commission President Jean-Claude Juncker, and European Council President Donald Tusk signed a joint declaration to "boost [the] ability to counter hybrid threats."[47] This was later advanced by concrete proposals for joint action, twenty of which focused on hybrid approaches. Among many other important steps, NATO has supported the establishment of an independent European Center of Excellence (COE) for Countering Hybrid Threats in Helsinki, while also creating its own NATO Hybrid Analysis Branch to focus on these issues.[48]

At the 2018 Brussels Summit, NATO amplified its attention on hybrid, stating that the Alliance is ready "to assist an Ally at any stage of a hybrid campaign."[49] Allies also agreed to a variety of actions to enhance NATO's counter-hybrid efforts, as underscored in three key sections of the Brussels Summit Declaration:

> *"While the primary responsibility for responding to hybrid threats rests with the targeted nation, NATO is ready, upon Council decision, to assist an Ally at any stage of a hybrid campaign. In cases of hybrid warfare, the Council could decide to invoke Article 5 of the Washington Treaty, as in the case of armed attack…We announce the establishment of Counter Hybrid Support Teams, which provide tailored, targeted assistance to Allies, upon their request, in preparing for and responding to hybrid activities."*[50]

> *"Reaffirming NATO's defensive mandate, we are determined to employ the full range of capabilities, including cyber, to deter, defend against, and to counter the full spectrum of cyber threats, including those conducted as part of a hybrid campaign…We continue to work together to develop measures which would enable us to impose costs on those who harm us."*[51]

> *"We will continue to optimize NATO intelligence to facilitate timely and relevant support to Allied decision-making and operations, including through improved warning and intelligence*

2018, https://www.nytimes.com/2018/03/15/us/politics/russia-cyberattacks.html.

44 "German Intelligence Head Warns of Cyber-Attacks on Critical Infrastructure," *Deutsche Welle*, May 14, 2018, https://www.dw.com/en/german-intelligence-head-warns-of-cyber-attacks-on-critical-infrastructure/a-43774802.

45 Bermet Talant, "Russia Retaliates Against Ukraine's Court Win, Shuts Off Natural Gas Supplies Indefinitely," *Kyiv Post*, March 2, 2018, https://www.kyivpost.com/business/russia-retaliates-ukraines-court-win-shuts-off-natural-gas-supplies-indefinitely.html.

46 Helene Cooper and Eric Schmitt, "U.S. Spycraft and Stealthy Diplomacy Expose Russian Subversion in a Key Balkans Vote," *New York Times*, October 9, 2018, https://www.nytimes.com/2018/10/09/us/politics/russia-macedonia-greece.html.

47 NATO, press release, "Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization," July 10, 2018, https://www.nato.int/cps/en/natohq/official_texts_156626.htm.

48 *Third Joint Progress Report on the Implementation of the Common Set of Proposals Endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017* (Brussels: NATO, 2018), https://www.consilium.europa.eu/media/35578/third-report-ue-nato-layout-en.pdf.

49 NATO, "Brussels Summit Declaration," paragraph 21.

50 Ibid.

51 Ibid., paragraph 20.

sharing, particularly on terrorism, hybrid, and cyber."[52]

Responding to hybrid challenges requires a multifaceted effort by nations, NATO, the EU, and the private sector. Still, NATO has several unique strengths, particularly with respect to planning and organizing in the context of potential use of force, both at lower levels and in high-end, armed attacks. To optimize the capacity to respond to hybrid challenges, NATO should undertake five sets of actions.

First, as noted above and further discussed below, NATO should plan with respect to current hybrid activities, as well as more substantial Level 2 hybrid.

Second, NATO should fully resource the Counter Hybrid Support Teams (CHSTs), so that they can take on both planning and response actions. The Brussels Summit Declaration nominally creates these CHSTs; thus far, however, there are very few details regarding how these teams will form or function.[53] While the model of NATO's Advisory Support Teams (ASTs)[54] which assemble only when called upon, is useful, the CHSTs should be created with a core of standing, albeit small, forces that would be supplemented by capabilities from nations. This would allow them to undertake planning and to develop tactics, techniques, and procedures that would be promptly available at the request of an individual allied country, prior to—or at any stage of—a hybrid attack, campaign, or incident. Teams should include specific civilian and military experts, rather than policy advisers, from NATO member countries and NATO institutions. They should also include links to EU institutions and member states (the EU Hybrid Fusion cell and the European Commission in particular), as well as the private sector. Representatives should have expertise and technical skills in, for example, intelligence analysis, strategic communications (European and Russian languages), emergency response, border management, energy security, grid stability, political and economic systems, financial systems, and cybersecurity. On the operation side, particularly to address low-level forcible activities, representatives might be drawn from the European Gendarmerie Force, which comprises trained military police from across European countries, as well as from national border guards. These representatives should be engaged ahead of time, as designated CHST personnel for their areas of expertise. One useful way to ensure that the necessary expertise is available would be for the NATO Defense Planning Process to provide guidance for countries to develop key capabilities that could be engaged as part of CHSTs.

CHSTs should spearhead their own planning efforts and be available to support both national planning and response, if required. To draw on existing resources and competencies, the teams should work closely with NATO special-operations forces. CHSTs should also be frequently exercised for various hybrid contingencies. Some members of the CHSTs would be able to work remotely, depending on the hybrid incident, but others could be forward deployed to particularly susceptible regions, such as the Baltic or Balkan states. These teams could be embedded in NATO eFP battalions, currently in the Baltic States and Poland, or NATO Force Integration Units, where appropriate. Frontline nations and those interested in support from CHSTs should be prioritized first.

CHSTs should be centrally commanded and controlled. NATO should conduct a study to evaluate appropriate command and control in the context of hybrid, similar to the command structure review it completed ahead of the Brussels Summit. This effort should also evaluate how to work with national and EU capabilities. One option would be to have the CHSTs coordinated by team leaders under the Operations Division at NATO Headquarters, acting under the authority of the Secretary General and nations requesting support. This approach would be parallel to NATO's strategic communications function, which is led at NATO Headquarters. However, given the operational nature of hybrid – especially in the Level 2 context, and particularly with respect to cyber, use of chemicals, riots, insurrections, and the like – it would be important to coordinate CHSTs out of SHAPE. Currently, no single division or team is responsible for hybrid overall either at SHAPE or at NATO HQ. Given this, it would be useful to establish an overarching Hybrid Operations Center, similar to the Cyber Operations Center, at SHAPE that would be responsible for coordinating CHSTs, among other counter-hybrid activities; although, certain activities, such as strategic communications might be undertaken at NATO HQ. The Cyber Operations Center and

52 Ibid., paragraph 13.

53 Ibid., paragraph 21.

54 NATO has Resilience Advisory Support Teams (ASTs) to help nations assess and build resilience. For more on this concept see NATO ACT, "Building Resilience: Collaborative Proposals to Help Nations and Partners," 2017, www.act.nato.int/images/stories/events/2017/resilience/resilience-wp.pdf.

a new Hybrid Operations Center would need to be coordinated or combined in some fashion.

Third, NATO should increase its awareness of adversarial hybrid activities by further developing intelligence and establishing a system of indications and warnings focused on hybrid. Better intelligence is, of course, a prerequisite to timely and effective action, and NATO has increased its focus on "improved warning and intelligence."[55] NATO has made significant progress on the development of indications and warning, especially in the conventional realm. Still, greater efforts are required in the hybrid realm, which encompasses many activities that will require political determinations to take collective action—the overall responses to the chemical attacks in the United Kingdom being a good example. Accordingly, having a system that focuses on adversaries' hybrid actions, provides early warning to the degree possible, and allows for coordinated political determinations is an important requirement for the Alliance. There are numerous ways to accomplish this, but the Assistant Secretary General for Intelligence and Security (ASG I&S) should be a leading actor in ensuring that all members of the Alliance are fully advised. The ASG I&S should work with military authorities and nations to make regular information available to the Alliance, including routine briefings to the North Atlantic Council. Additionally, the ASG I&S and NATO's military authorities should work with nations to develop indicators and warnings, cognizant of the possibility that higher-level hybrid attacks might be imminent. To further develop and enhance these indicators and warnings, more specific Russian objectives should be considered. Rather than thinking in terms of Russia's overarching and strategic objectives, such undermining the West and dividing NATO and the EU, warnings and corresponding indicators should be built around potential specific Russian actions or campaigns—as an example, Russia's activities in Macedonia ahead of its name-change referendum, which sought to decrease voter turnout and increase votes against the referendum. Additional resources and personnel to focus on open-source information and coordination with the EU and relevant private sector entities (e.g. finance, energy, telecommunications) should all be part of such activities.

Fourth, NATO should elevate energy security and critical-infrastructure protection (CIP) as a core focus of NATO and combined (NATO-EU-private sector) exercises. Of course, diversifying energy supplies is the most effective way to combat Russian energy manipulation. However, NATO can help with the protection of allies' critical energy and other infrastructure, in terms of both physical and cyber activities. As part of this, NATO should enhance its efforts to train and exercise its forces, including CHSTs, in CIP-centric hybrid scenarios. Some exercises currently include energy, cyber, and other critical-infrastructure elements on the periphery, but they should be elevated to a primary role. Other useful efforts are also underway in NATO and EU circles in the form of scenario-based discussions, training, and best practices sharing.

Currently, CIP-related exercises are planned and executed in a "parallel and coordinated" manner between NATO and the EU; however, they should be conducted as an integrated activity with NATO, the EU, and representatives from the private sector, such as Internet service providers (ISPs) and electric-grid operators. National forces and authorities, such as police and border guards, should also be integrated into these plans and exercises.

NATO should also place a particular focus on the chemical threat in the hybrid context, as demonstrated by the Russian attacks in the UK. National chemical-defense units and clean-up crews—especially those equipped to handle sensitive substances related to energy and critical infrastructure—should also be enhanced and considered in planning efforts. NATO should work to establish clear lines of communication and joint contingency planning across these NATO, EU, and private-sector stakeholders to proactively prepare for hybrid crises that include chemical attacks.[56]

Fifth, NATO should work to develop doctrine for responding to strategic intimidation and hybrid activities, including a playbook of collective countermeasures to be taken by allies in hybrid scenarios, especially those that may not meet a conventional Article 5 threshold.

The Brussels Summit Declaration underscores this requirement, and emphasizes the necessity of having the capability to respond. In particular, the declaration calls for allies to "work together to develop measures which would enable us to impose costs on those who

55 NATO, "Brussels Summit Declaration," paragraph 13.

56 Russia's use of chemicals also underscores the importance of protection-and-response capabilities for nuclear, radiological, and biological threats.

harm us."[57] The legal framework for these actions is informed by customary international and treaty law, including the UN Charter (article 2(4) use of force clause and article 51 armed attack clause), as well as the law of countermeasures, pleas of necessity, and the norm of non-intervention.[58] Under international law, there are actions NATO allies can take, both offensive and defensive in nature, against the perpetrator of a hybrid attack, provided certain conditions are met.

Most importantly, in addition to sanctions—which some Allies have already used in response to Russian hybrid activities—NATO nations may also take "countermeasures" and "actions of necessity."[59] These measures would otherwise not be lawful, but are justified due to a prior wrongful act against the state (for countermeasures) or circumstances that place a state's essential interests in "grave and imminent peril" (for pleas of necessity).[60] There are several requirements and restrictions on these actions; for instance, countermeasures require attribution of the initial act to a state actor, while both countermeasures and actions of necessity must follow the customary principles of necessity and proportionality. Still, allied leaders have a number of untapped options in this realm.[61]

This body of law also supports the use of collective countermeasures, a concept particularly relevant for NATO, which enables multiple nations—even those not directly harmed by the hybrid act—to act together to amplify a response under certain circumstances. Under the accumulation of events doctrine, individual incidents or successive attacks, which alone may not rise to a sufficient level of force to justify the use of countermeasures, can be assessed under the law as connected incidents.[62] Taken together, these may reach a threshold that would justify more severe countermeasures.

Though these options are often not widely understood or utilized by allied policymakers or military personnel, they provide compelling and impactful ways for NATO nations to deter and reply to Russian hybrid challenges – both in the context of pre-crisis vigilance measures and deterrence response options. NATO should begin formulating doctrine and a playbook of countermeasures, which can be taken by its member states if certain triggers are activated. Capitalizing on NATO's strength as a collective defense alliance, these counter-intimidation measures should be adopted multilaterally by several allied member states, whenever possible. Formulation of this playbook should also include cooperation with the EU to explore where and how EU-level responses and capabilities fit in. Such a playbook would not need to include strict, pre-agreed actions, but would provide potential options that advisers could present to NATO or national authorities. A task force, perhaps headed by NATO's Assistant Secretary Generals for Emerging Security Challenges and for Operations, in coordination with SACEUR, should be established to provide such options and recommendations to the Alliance and nations. The ASG I&S should also conduct a more systematic analysis of Russian vulnerabilities to inform the development of these possible options. By catalyzing these conversations ahead of time, this playbook would help to lay the groundwork for timelier political decision-making both to preempt and respond to Russian strategic intimidation efforts as they increase. One additional way to ensure senior decision-makers understand hybrid threats and these potential response options would be to hold a scenario-based discussion focused on Level 2 hybrid at a NATO defense ministers' meeting.

The types of adversarial, sub-Article-5, including Level 2 hybrid, actions that should be considered

57 NATO, "Brussels Summit Declaration," paragraph 20.

58 United Nations, "Charter of the United Nations," June 26, 1945, http://www.un.org/en/charter-united-nations/. See Catherine Lotrionte, "Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law," *Cyber Defense Review* vol. 3, no. 2, Summer 2018, https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/CDR_V3N2_ReconsideringConsequences_LOTRIONTE.pdf?ver=2018-09-05-084840-807.

59 Sanctions under international law are considered "retorsions," which are lawful acts taken at any time by one state upon another, in retaliation for a similar act by the other state. Another example would be expelling another state's diplomats.

60 While there no universally accepted definition for a state's "essential interests," they are generally considered to include issues related to a state's security, preservation of its natural environment, economy, public health, safety, and food supply. See United Nations, *Draft Articles on Responsibility of State for Intentionally Wrongful Acts, With Commentaries* (New York: United Nations, 2001), Article 25, http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.

61 For a full discussion, see Lotrionte, "Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law."

62 Ibid.; see also United Nations, *Draft Articles on Responsibility of State for Intentionally Wrongful Acts, With Commentaries*; see also Colonel Gary Corn and Eric Jensen, "The Technicolor Zone of Cyberspace—Part I and Part 2," Just Security, May 30, 2018, https://www.justsecurity.org/57217/technicolor-zone-cyberspace-part/.

for a playbook or doctrine include: cyber or physical operations to shut down an electric grid or energy pipeline; forcible abduction of individuals; little green men or proxies; targeted killings of single individuals; limited chemical attacks on foreign territory; political or economic subversion or coercion, including election interference; sabotage; intelligence operations; inciting civil unrest or riots; hacking a manufacturing facility to produce faulty and/or dangerous products; and widespread disinformation campaigns originating in a foreign state that significantly affect a sovereign state's internal affairs. The task force could consider appropriate potential responses. These would be tailored to different contexts, but might include: seizure or freezing of an offending state's assets; blocking access to an offending state's bank accounts; disabling Internet access or routers, either of an offending state or within that state's territory; blocking IP addresses of an offending state; rescuing nationals from an offending state's territory; hacking and releasing sensitive information about an offending state; proportional actions against an offending state's critical infrastructure; or hacking an offending system or individual to forcibly remove a source of significant disinformation that endangers a state's sovereign affairs or essential interests.

It is also important to note that the nature or effects of some adversarial hybrid attacks may be such that they reach the threshold for "armed attack" under Article 51 of the UN Charter. In these cases, NATO's Article 5 would come into play.

UPDATING STRATEGIC PLANNING

The July 2018 summit recognized a fundamentally changed security environment, including significant conventional, cyber, and hybrid challenges emanating from the east, but also instability ranging from northern Africa and the Sahel to the Levant and Iraq to Afghanistan, which affects allied nations. Under these circumstances, the Alliance's supreme military commanders should conduct a comprehensive review of the challenges, as well as the opportunities to enhance deterrence, support political efforts to promote stability, and undertake effective warfighting. Three parallel efforts should be considered.

First, SACEUR should be tasked with developing a comprehensive plan for the defense of NATO territory, including a review of whether, and how, force postures should be enhanced for the east and/or the south. SACEUR should determine the nature of the greatest needs—for example, whether additional enablers such as air defense or prepositioned equipment, structural requirements such as airfields, and resilience for critical infrastructures would be most valuable, and/or if land-combat formations should be permanently stationed—and how that might differ between potential geographic areas.

The military value of a comprehensive force-posture review is underscored by the political requirement. The Polish government has proposed that the United States permanently station an armored brigade in Poland. In the 2019 National Defense Authorization Act (NDAA), the US Congress has similarly required a report on the "feasibility and advisability of permanently stationing US forces in the Republic of Poland."[63] The presidents of the United States and of Poland recently discussed the possibility.[64] However, the Alliance does not have infinite resources, and—as the above discussion of conventional readiness and reinforcement shows—there are many demands for those resources. Preliminarily, it seems clear that the Alliance's strategy of reinforcement would be enhanced if there were additional capabilities in the east. Because multiple land and air forces would need to move and fight forward, there are strong reasons to station land-force enablers in the east—in particular, prepositioned equipment for brigade combat teams and/or equipment and support for long-range fires and air defense.[65] The fiscal year 2019 EDI "funds

63 Section 1280 of the NDAA provides, in part, "Not later than March 1, 2019, the Secretary of Defense, in coordination with the Secretary of State, shall submit to the congressional defense committees a report on the feasibility and advisability of permanently stationing United States forces in the Republic of Poland," including an "assessment of the types of permanently stationed United States forces in Poland required to deter aggression by the Russian Federation and execute Department of Defense contingency plans, including combat enabler units in capability areas such as (A) combat engineering; (B) logistics and sustainment; (C) warfighting headquarters elements; (D) long-range fires; (E) air and missile defense; (F) intelligence, surveillance, and reconnaissance; and (G) electronic warfare." The report shall also consider whether "a permanently stationed United States Army brigade combat team in Poland would enhance deterrence," "the actions the Russian Federation may take in response," "the international political considerations…including within the North Atlantic Treaty Organization (NATO)," and "whether such a brigade combat team in Poland would support implementation of the National Defense Strategy." Other report requirements include investments required, changes to the force in Europe, logistical requirements, and Polish support.

64 Alan Cowell, "Fort Trump? Poland Makes a Play for a U.S. Military Base," *New York Times*, September 19, 2018, https://www.nytimes.com/2018/09/19/world/europe/poland-fort-trump.html.

65 The United States is currently planning to deploy a brigade set worth of equipment to prepositioned sites in Poland. Dan Stoutamire, "Army to Move Brigade's Worth of Firepower into Poland," *Stars and Stripes*, April 26, 2017, https://www.stripes.com/news/army-to-

the continued build of a division-sized set of prepositioned equipment that is planned to contain two ABCTs (one of which is modernized), two Fires Brigades, air defense, engineer, movement control, sustainment and medical units."[66] While the initial focus was on Belgium, Netherlands, and Germany, at least preliminarily, "US Army Europe (USAREUR) has identified Powidz Air Base, Poland as a new European Activity Set (EAS) to move prepositioned equipment…to enable US Army Europe to continue military assurance to NATO allies."[67] Additional EDI funding is also designated for ammunition and bulk fuel storage, rail extensions and railheads, a staging area in Poland, and ammunition infrastructure in Bulgaria and Romania.[68] The FY2019 EDI also funds "operating and procurement requirements to enable the purchase and prepositioning of ECAOS DABS Prepositioned War Readiness Material at various locations throughout Europe." This provides a basis for implementing the concept of adaptive basing for air forces as an important element of NATO's reinforcement strategy.[69] Likewise, the congressional statutory language (quoted in the footnote) implies there are strong reasons to conclude that the forward deployment of combat enablers to the east supports both deterrence and warfighting. Still, it would be important for SACEUR (who will have to act in his US capacity as commander of European Command to support the Secretary of Defense regarding the report to Congress, and his NATO capacity as SACEUR for Alliance considerations) to provide a thorough military evaluation of both enablers and permanently stationed combat forces in Poland, and the east more broadly.

Further, while nations can undoubtedly agree on a bilateral basis for the stationing of forces, and the United States has significant forces stationed in various places across the Alliance, there are potential political issues—particularly regarding the possibility of stationing substantial permanent forces in the east. Two of these stand out. First, some members of the Alliance have maintained that the 1997 NATO-Russia Founding Act prohibits permanent stationing of larger formations in the east of the Alliance, in former Warsaw Pact nations. That argument is plainly incorrect when placed against the words of the Founding Act, which provides:

> *"NATO reiterates that in the current and foreseeable security environment, the Alliance will carry out its collective defense and other missions by ensuring the necessary interoperability, integration, and capability for reinforcement rather than by additional permanent stationing of substantial combat forces. Accordingly, it will have to rely on adequate infrastructure commensurate with the above tasks."*[70]

The "current and foreseeable security environment" of 1997 has obviously changed dramatically, as the 2018 Brussels Summit Declaration makes clear. By its own terms, the Founding Act is no bar. However, the fact that certain allies still adhere (even if incorrectly) to the Founding Act, despite Russian behavior, raises the political issue—namely whether, as a policy matter, the Alliance wants to move additional substantial permanent forces farther east. Maintaining Alliance cohesion will be a critical element of any decision to forward deploy additional forces to Poland. From a military perspective, and given the reality of constrained resources, enablers being developed under the EDI have high priority, but SACEUR should provide a full evaluation as to the value of permanent forces. This input from SACEUR, in his role of commander of EUCOM, should feed into the report the United States Congress has required from the Secretary of Defense on the value of increased presence in the east. The report, which will be presented in unclassified form, will be of significant interest to all members of the Alliance. Accordingly, if the Secretary of Defense and/or the SACEUR determined that, as a matter of

move-brigade-s-worth-of-firepower-into-poland-1.465372.

66 US Department of Defense, "Department of Defense Budget Fiscal Year (FY) 2019, European Deterrence Initiative" p. 11.

67 Powidz Air Base, "Base Notice: FY18 Army Prepositioned Stocks Tree Cutting," June 27, 2018, https://mpit.bip.gov.pl/fobjects/download/407411/65-18-pdf.html.

68 US Department of Defense, "Department of Defense Budget Fiscal Year (FY) 2019, European Deterrence Initiative" p. 25.

69 Ibid., p.12.

70 The full text of the relevant paragraph is: "NATO reiterates that in the current and foreseeable security environment, the Alliance will carry out its collective defence and other missions by ensuring the necessary interoperability, integration, and capability for reinforcement rather than by additional permanent stationing of substantial combat forces. Accordingly, it will have to rely on adequate infrastructure commensurate with the above tasks. In this context, reinforcement may take place, when necessary, in the event of defence against a threat of aggression and missions in support of peace consistent with the United Nations Charter and the OSCE governing principles, as well as for exercises consistent with the adapted CFE Treaty, the provisions of the Vienna Document 1994 and mutually agreed transparency measures. Russia will exercise similar restraint in its conventional force deployments in Europe." NATO, "Founding Act on Mutual Relations, Cooperation and Security between NATO and the Russian Federation Signed in Paris, France," May 27, 1997, http://www.nato.int/cps/en/natohq/official_texts_25468.htm.

military judgment, forces should be expanded in the east or south, this, along with the conclusions outlined in the report, would provide the basis for consultations, at NATO and bilaterally, with a focus on enhancing deterrence through both military capabilities and Alliance unity.

Whatever the exact determination, it would be most valuable for any additional presence to be multinational as a matter of Alliance unity, while being undertaken in a manner to maintain military effectiveness. While US capabilities could lead, the inclusion of other allies would most effectively enhance deterrence, as it has with eFP. Should additional forces be forward deployed to Poland, NATO might also consider adjusting the framework-nation assignments of the four NATO Battle Groups. For example, if the Canadian and US framework-nation assignments were to shift, then a US-led NATO battlegroup in Latvia, with some additional enablers, would further enhance deterrence in the Baltic area. Finally, it is important to underscore that a comprehensive plan undertaken by SACEUR should include the South, the Atlantic, and the Arctic, as no armed conflict could be expected to remain confined to a single geographical arena. As recent events underscore, SACEUR should include in this evaluation the impact of Russian capabilities in the south, including the Mediterranean and Syria, and the implications for force posture and warfighting capabilities.

Second, SACEUR should analyze and develop tactics, techniques, and procedures, focusing on the potential transition from hybrid conflict to armed attack, including: indications and warning; flexible-deterrent options; and responses to unconventional actions, including an adversary's use of chemicals and special-operations forces. Once developed, such TTPs would be transitioned to use.

One of the most uncertain issues facing the Alliance is whether, and how, ongoing hybrid activities might transition to armed attack. Decision-making in this situation may be particularly difficult. The Alliance's establishment of CHSTs, as discussed above, reflects the importance of responding appropriately to such hybrid issues. While there is a good deal of consideration regarding hybrid issues, the transition from hybrid to armed conflict requires clear analysis of the military's role. SACEUR should undertake such a review, working with other elements of the Alliance, and engaging the EU and the Hybrid COE.[71]

In this realm, at least three areas require significant development. The first is indications and warnings, particularly with respect to determining when hybrid activities foreshadow an escalation to armed attack. The intelligence efforts of NATO and the EU are highly relevant, but what needs to be further developed is whether, and how, to analyze an adversary's hybrid actions in the context of an indications-and-warning effort.[72] As noted above, the ASG I&S should play a key role in this arena, and coordination with the military is an important requirement. Second, flexible-deterrent actions are steps that can be taken to increase warfighting capacity, and to also serve as a means of deterrence to an adversary. More thought is needed to determine what possible flexible-deterrent options might look like in the context of hybrid conflict. Third, as the use of chemicals in the UK and "little green men" in Ukraine indicated, Russian actions could likely begin with significant, but unconventional, means.[73] Building an alliance approach to deter and/or respond to such activities is an important priority. As previously emphasized, allied capabilities to respond to chemical incidents need to be reviewed, and likely expanded. Use of Alliance special-operations forces in conjunction with border forces, military police, and law enforcement should also be a focus area.

Third, SACT has an important role in ensuring the Alliance makes effective use of advanced technology. At the 2018 summit, the allies agreed to undertake "necessary increases in defense spending, including on research and development…to foster innovation to maintain our technological edge."[74] This focus on technology is important now, and will become increasingly crucial in the future. For many years, some allies—and the United States, in particular—have overmatched adversaries with capabilities including

71 The European Centre of Excellence for Countering Hybrid Threats (Hybrid COE) provides a single location dedicated to furthering a common understanding of hybrid threats and promoting the development of comprehensive, whole-of-government response at national levels and of coordinated response at EU and NATO levels in countering hybrid threats. For more, see https://www.hybridcoe.fi/.

72 The European Union Hybrid Fusion Cell and NATO's Hybrid Analysis Branch are two such activities. See European Commission, Joint Report to the European Parliament, the European Council and the Council, pp. 3–4, https://eeas.europa.eu/headquarters/headquarters-homepage/46398/joint-report-implementation-joint-framework-countering-hybrid-threats-july-2017-june-2018_en.

73 The term "little green men" refers to the tactic of using unmarked soldiers or unattributable asymmetric forces, as employed by Russia in its illegal annexation of Crimea.

74 NATO, "Brussels Summit Declaration," paragraph 31.

precision-guided munitions, stealth, and network-centric warfare. As the US National Defense Strategy states, however, "our competitive military advantage has been eroding."[75] In the European theater, Russia has accomplished significant development in areas such as cruise missiles, electronic warfare, and cyber. In light of these advances, both the United States and its allies not only need to get to the battle promptly, but also need to maintain some capabilities that provide for overmatch. Some capabilities, such as the F-35, are already reaching the force, but more are needed. The US Defense Department began a serious capability-upgrading program several years ago with the so-called "third offset" and, more recently, has sought to accelerate the development of advanced capabilities, including efforts on artificial intelligence, robotics, hypersonics, directed energy, quantum computing, and man-machine interface.[76]

While a good deal of effort is taking place at the national level, the issue for the Alliance is how to bring those capabilities into a coordinated, innovative military effort. NATO ACT has a well-developed structure with strategic analysis, capabilities development, and training functions, which can be used to help the Alliance focus on generating asymmetric capabilities to offset Russian capabilities. One key area of emphasis should be the use of gaming and simulations to determine which efforts are most valuable. ACT should then interact with the defense-planning process, and organize training to bring advanced asymmetric capabilities into the Alliance's overall warfighting capacity. Such actions should take account of entities such as the Strategic Capabilities Office in the United States, which focuses on innovative capabilities that can be fielded within a five-year period.[77] ACT should undertake an "innovation integration initiative" along these lines, including working with the Defense Planning Process led at NATO headquarters.

CONCLUSION

At the 2018 Brussels Summit, NATO agreed to important steps for enhancing deterrence, strengthening its warfighting posture, and responding to aggressive and unwarranted hybrid actions—a large portion of which come from Russia. As the Alliance undertakes its next steps, including the development of political guidance, the recommendations outlined above will help implement these key objectives and outcomes, bolstering defense and deterrence, and boosting Alliance unity at this critical time for the transatlantic community.

75 US Department of Defense, *Summary of the 2018 National Defense Strategy of the United States*, p. 1.

76 As well as cyber, discussed above.

77 "The SCO identifies, analyzes, and accelerates disruptive and asymmetric applications of existing commercial and government systems and near-term technologies to create operational strategic effects via three mechanisms: crossing or blurring domains, teaming systems, and incorporating enabling commercial technology...[T]he SCO conducts demonstrations, experiments, and prototypes candidate capabilities to reduce upfront risk on potentially game-changing concepts that can be fielded in the near-term (0-5 years) fiscal development period." See US Office of the Secretary of Defense, *Fiscal Year (FY) 2019 President's Budget* (Washington, DC: Department of Defense, 2018), https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2019/budget_justification/pdfs/01_Operation_and_Maintenance/O_M_VOL_1_PART_1/OSD_OP-5.pdf.

Atlantic Council

Board of Directors

INTERIM CHAIRMAN
*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. Mirtchey
*Virginia A. Mulberger
*W. DeVier Pierson
*John J. Studzinski

TREASURER
*George Lund

SECRETARY
*Walter B. Slocombe

DIRECTORS
Stéphane Abrial
Odeh Aburdene
*Peter Ackerman
Timothy D. Adams
Bertrand-Marc Allen
*Michael Andersson
David D. Aufhauser
Matthew C. Bernstein
*Rafic A. Bizri
Dennis C. Blair
Thomas L. Blair
Philip M. Breedlove
Reuben E. Brigety II
Myron Brilliant
*Esther Brimmer
Reza Bundy
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
David W. Craig
Helima Croft
Ralph D. Crosby, Jr.
Nelson W. Cunningham
Ivo H. Daalder
*Ankit N. Desai
*Paula J. Dobriansky
Thomas J. Egan, Jr.
*Stuart E. Eizenstat
Thomas R. Eldridge
*Alan H. Fleischmann
Jendayi E. Frazer
Ronald M. Freeman
Courtney Geduldig
*Robert S. Gelbard
Gianni Di Giovanni
Thomas H. Glocer
Murathan Günal
John B. Goodman
*Sherri W. Goodman
Amir A. Handjani
Katie Harbath
John D. Harris, II
Frank Haun
Michael V. Hayden
Brian C. McK. Henderson
Annette Heuser
Amos Hochstein
Ed Holland
*Karl V. Hopkins
Robert D. Hormats
Mary L. Howell
Ian Ihnatowycz
Wolfgang F. Ischinger
Deborah Lee James
Reuben Jeffery, III
Joia M. Johnson
Stephen R. Kappes
*Maria Pica Karp
Andre Kelleners
Sean Kevelighan
Henry A. Kissinger
*C. Jeffrey Knittel
Franklin D. Kramer
Laura Lane
Richard L. Lawson
*Jan M. Lodal
Douglas Lute
*Jane Holl Lute
William J. Lynn
Wendy W. Makins
Zaza Mamulaishvili
Mian M. Mansha
Gerardo Mato
William E. Mayer
Timothy McBride
John M. McHugh
H.R. McMaster
Eric D.K. Melby
Franklin C. Miller
*Judith A. Miller
Susan Molinari
Michael J. Morell
Richard Morningstar
Edward J. Newberry
Thomas R. Nides
Franco Nuschese
Joseph S. Nye
Hilda Ochoa-Brillembourg
Ahmet M. Oren
Sally A. Painter
*Ana I. Palacio
Carlos Pascual
Alan Pellegrini
David H. Petraeus
Thomas R. Pickering
Daniel B. Poneman
Dina H. Powell
Arnold L. Punaro
Robert Rangel
Thomas J. Ridge
Michael J. Rogers
Charles O. Rossotti
Robert O. Rowland
Harry Sachinis
Rajiv Shah
Stephen Shapiro
Wendy Sherman
Kris Singh
Christopher Smith
James G. Stavridis
Richard J.A. Steele
Paula Stern
Robert J. Stevens
Robert L. Stout, Jr.
*Ellen O. Tauscher
Nathan D. Tibbits
Frances M. Townsend
Clyde C. Tuggle
Melanne Verveer
Charles F. Wald
Michael F. Walsh
Maciej Witucki
Neal S. Wolin
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Harold Brown
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 October 26, 2018

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