Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

TRANSFORMATIVE PRIORITIES FOR NATIONAL DEFENSE

Franklin D. Kramer and Lt. Col. Matthew R. Crouch

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

***Forward* Defense** helps the United States and its allies and partners contend with great-power competitors and maintain favorable balances of power. This new practice area in the Scowcroft Center for Strategy and Security produces *Forward*-looking analyses of the trends, technologies, and concepts that will define the future of warfare, and the alliances needed for the 21st century. Through the futures we forecast, the scenarios we wargame, and the analyses we produce, *Forward* Defense develops actionable strategies and policies for deterrence and defense, while shaping US and allied operational concepts and the role of defense industry in addressing the most significant military challenges at the heart of great-power competition.

Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

TRANSFORMATIVE PRIORITIES FOR NATIONAL DEFENSE

Franklin D. Kramer and Lt. Col. Matthew R. Crouch

ISBN-13: 978-1-61977-181-9

This report is written and published in accordance with the Atlantic Council Policy on Intellectual Independence. The authors are solely responsible for its analysis and recommendations. The views and opinions expressed here are those of the authors and do not necessarily reflect the official policy or position of the Unites States Marine Corps, Department of Defense, or any other agency of the US government or other organization. The Atlantic Council and its donors do not determine, nor do they necessarily endorse or advocate for, any of this report's conclusions.

June 2021

TABLE OF CONTENTS

I. INTRODUCTION AND SUMMARY

This report sets forth key transformative priorities required for an effective national defense strategy. It is not intended to address all elements of a national defense strategy but rather to highlight those areas where transformative changes are necessary to make the strategy successful.

The report proposes such changes because the global context itself has significantly changed. The United States faces multi-theater and multi-domain challenges different from any presented since World War II—and, in fact, ever. The US homeland has itself become an active defense theater, and China and Russia present major concurrent defense challenges in the Indo-Pacific and European theaters, respectively. Within this context, the combination of stealth, precision-guided munitions, network-centric warfare, and sea and space control that gave the United States battle dominance for many years will no longer suffice. The defense battlespace has changed, and the defense domain has expanded. Cyber and supply chain resilience have become key requirements necessitating active inclusion of the private sector. Emerging technologies including unmanned vehicles, cyber offense and directed energy, and hypersonic missiles are changing operational and tactical engagements. With two highly competitive forward theaters, allies are ever more important.

Accordingly, the paper has two main sections: 1) the role of defense in the United States itself—the "American theater"; and 2) the establishment of a tailored forward defense strategy, which gives simultaneous recognition to China as the "number one pacing challenge"[1] and Russia as a "self-identifie[d] ... antagonist to the West."[2] The major recommendations include the following:

A. The American Theater: The United States itself has become an active operational defense theater. Continuous adversarial intrusions have generated the concomitant necessity for greater defense, intelligence community, and private sector engagement in defense of the American theater. Successfully meeting the challenges requires a strategy of "effective resilience/defend back" including the following:

1) Developing and implementing cybersecurity resilient architectures for key critical infrastructures through a "zero trust"-plus approach, starting with pilot programs that the Defense Department could organize and oversee in cooperation with the relevant sector-specific departments including the Department of Homeland Security (DHS) and with highly capable participants from the private sector

2) Creating an integrated national cyber defense center headed by the national cyber director with outreach to the private sector

3) Coordinating government engagement with private sector key critical infrastructures including

a) establishing private sector i) "Sector Analysis and Defense Centers" and ii) certified active defenders for enhanced cyber resilience; and

b) utilizing active cyber defense measures to create an integrated "defend back" capability (i.e., within the United States)

4) Expanding the National Guard's cybersecurity roles, which would have immediate high value for states/localities and key critical infrastructures as well as for Defense Department missions in the event of a high-end conflict

5) Ensuring the resilience of the supply chains for defense and other key critical infrastructures required for defense mission assurance by

a) excluding China from national security supply chains;

b) barring Chinese software from key critical infrastructure supply chains; and

c) requiring a "China plus one country" diversified approach for materials and components for key critical infrastructures

B. The Forward Theaters: China and Russia each present major defense challenges. As a consequence, the United States needs to establish a tailored multi-theater force posture, with an appropriate balance between the

[1] Secretary of Defense, "Message to the Force," Memorandum for All Department of Defense Employees, US Department of Defense, March 4, 2021, https://media.defense.gov/2021/Mar/04/2002593656/-1/-1/0/SECRETARY-LLOYD-J-AUSTIN-III-MESSAGE-TO-THE-FORCE.PDF.

[2] German Federal Ministry of Defence, *Position Paper: Reflections on the Bundeswehr of the Future,* February 9, 2021, https://www.bmvg.de/resource/blob/5029396/a83129815c00e3638302ba3630478987/20210211-dl-positionspapier-en-data.pdf, 2.

Indo-Pacific and Europe.[3] An important element in each theater is an increased role for allies. Cybersecurity and supply chain resilience are as required in the forward theaters as they are in the American theater. Emerging technologies, effective combat formations, and multinational command and control will be key elements for success in a changing battlespace.

For the Indo-Pacific, successfully meeting the challenges requires the following:

1) Japan, Australia, the Republic of Korea, and NATO allies committing to support the United States in the event of a conflict with China including over Taiwan

2) Establishing multinational force capabilities including

   a) with Japan and Australia, a combined naval task force, combined air operations center, and multi-domain command and control system; and

   b) with allies and partners, a combined joint task force for maritime support including freedom of navigation, fishing rights, counter-piracy, search-and-rescue, humanitarian assistance and disaster relief, and a common maritime picture

3) Establishing cybersecurity and supply chain resilience with allies

4) Utilizing emerging technologies and naval mining capabilities including

   a) unmanned vehicles;

   b) cyber and directed energy;

   c) hypersonic missiles; and

   d) expanded mine clearing and mine laying capabilities

For Europe, successfully meeting the challenges requires the following:

1) Establishing cybersecurity and supply chain resilience with allies including by developing and implementing NATO "continuous response" cyber capabilities

2) Making the NATO Readiness Initiative (NRI) effective by

   a) organizing, training, and exercising the national forces called for by the NRI in effective combat formations;

   b) integrating the NRI forces into an effective command and control structure with the US European Command land commander in command of NATO land forces; and

   c) terminating the current NATO Response Force structure as redundant to the NRI forces and ineffective against the Russian threat, but maintaining the Very High Readiness Joint Task Force

3) Enhancing NATO's mobility capabilities and increasing European and US forward presence

[3] The United States has significant defense interests in other theaters, including the Middle East, Africa, and Afghanistan, but those can generally be met through an economy of force approach supported by the capacity to reinforce promptly. Deterrence on the Korean peninsula is also a major requirement, but the United States and the Republic of Korea have a well-established collective defense strategy.

II. THE AMERICAN THEATER

Critical defense challenges in the American theater include cybersecurity, resilience of supply chains, and redefining the roles of the private sector in defense. Strategically, "effective resilience/defend back" in the American theater needs to be added to the long-standing national security strategic pillars of overseas engagement and forward defense.[4]

A. "Effective Resilience/Defend Back" Is a Critical Defense Priority: A critical change to the international environment is that the United States itself has become an active operational theater with significant ongoing adversarial activity, particularly in the cyber and information operations domains. The People's Republic of China (PRC), Russia, Iran, and North Korea are each aggressively undertaking cyber activity against US institutions and individuals. As one example, the recent SolarWinds cyber intrusions by Russia not only provided espionage information, but also simultaneously amounted to preparation of the cyber battlefield inasmuch as it provided the capability for further intrusions.[5] Battlefield preparation is a key element of military operations, and adversarial actions can have significant consequences for mission assurance including command and control, mobility, and operational effectiveness. Accordingly, for the United States, "effective resilience/defend back" needs to be established as a foundational objective of US national security strategy and explicitly included in a national defense strategy.[6]

In the context of a national security strategy, effective resilience has been defined to mean the "capacity to prepare for and withstand shocks of the magnitude of a major pandemic or equivalent such as a major cyber attack with any resulting disruption significantly less than that caused by COVID-19."[7] For the Department of Defense (DOD), effective resilience needs to encompass both cybersecurity and supply chain resilience. "Defend back" means taking appropriate actions in the American theater to defend and/or ensure the resilience of key governance and critical infrastructures including cyber networks and supply chains.

> "A critical change to the international environment is that the United States itself has become an active operational theater"

Heretofore, homeland cybersecurity has largely been the province of the Department of Homeland Security and the private sector, but as the SolarWinds and recent Microsoft "Hafnium" attacks demonstrate,[8] that approach has not been successful. Consequently, not only are US defense capabilities at significant risk, but key institutions and entities have been successfully penetrated including the federal government itself, as well as critical infrastructures such as the electric grid. Concomitantly, as demonstrated in the context of the coronavirus, inadequate attention has been provided to supply chain security. In light of ongoing and continuous adversary activities, the United States needs to undertake a much more effective whole-of-government and public-private approach including by engaging the Department of Defense, the intelligence community, and the private sector, along with the Department of Homeland Security, in generating effective homeland cyber defense and supply chain security. Defending back is a critical requirement. The specifics of an integrated multi-department effort coordinated with the private sector are discussed below.

B. Cybersecurity Requires Major Corrective Actions: While the United States must be effective in all defense domains, currently there are particularly significant

[4] This section draws directly from Franklin D. Kramer and Robert J. Butler, *Cybersecurity: Changing the Model,* Atlantic Council, April 2019, https://www.atlanticcouncil.org/wp-content/uploads/2019/04/Cybersecurity-Changing_the_Model.pdf, and Franklin D. Kramer, *Effective Resilience: Lessons from the Pandemic and Requirements for Key Critical Infrastructures,* Atlantic Council, October 2020, https://www.atlanticcouncil.org/wp-content/uploads/2020/10/Effective-Resilience-Latest.pdf.

[5] "When there is a compromise of this scope and scale, both across government and across the technology sector … (that could) lead to follow-on intrusions. It's more than a single incident of espionage." Anne Neuberger, deputy national security adviser for cybersecurity, quoted in Gopal Ratnam, "Biden Likely to Take Executive Action on SolarWinds Hack," Government Technology, February 18, 2021, https://www.govtech.com/security/Biden-Likely-to-Take-Executive-Action-on-SolarWinds-Hack.html.

[6] Kramer, *Effective Resilience,* 5.

[7] Ibid.

[8] National Security Agency, Cybersecurity & Infrastructure Security Agency, and Federal Bureau of Investigation, *Russian SVR Targets U.S. and Allied Networks,* Cybersecurity Advisory, April 2021, https://media.defense.gov/2021/Apr/15/2002621240/-1/-1/0/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF; "HAFNIUM Targeting Exchange Servers with 0-Day Exploits," Microsoft, March 2, 2021, https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/.

deficiencies in the cyber domain, including especially inadequate resilience, that require major corrective efforts. Those efforts are necessary not only for the defense-specific requirement of mission assurance, but even more importantly for the effective working of American governance, the economy, and individual activities. As the recent executive order on cybersecurity states, "The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy."[9] Defending back in cyberspace to meet these challenges requires establishing cybersecurity resilient architectures; an integrated cybersecurity defense center; private sector "Sector Analysis and Defense Centers" and certified active defenders; and an expanded role for the National Guard.

1) Cybersecurity Resilient Architectures: A "Zero Trust"-Plus Approach

The greatest defense deficiency currently facing the United States is the ability of capable adversaries such as Russia and China to penetrate information and communications technology systems, including operational technologies utilized to run electric grids, pipelines, and other critical infrastructures as well as the defense industrial base.[10] The country's highest defense priority is to establish cybersecurity resilient architectures—which will require a "zero trust"-plus approach.[11] This point is particularly salient in light of the Russian-generated SolarWinds breach and China's Hafnium attack on Microsoft servers, each of which has created cascading adverse effects across the information and communications technology (ICT) sector and other critical infrastructure sectors as well as for government civil networks.[12]

The executive order on cybersecurity has begun a process that could lead to the widespread implementation of cybersecurity resilient architectures. The order is mostly focused on the federal civil departments. Most relevantly, each department is required to "develop a plan to implement Zero Trust Architecture," as well as a plan for the use of cloud technology.[13] The order also requires that threat information be shared among the federal civil agencies and their contractors, provides guidelines for enhancing the security of software, authorizes threat hunting within the federal agencies by the DHS Cybersecurity and Infrastructure Security Agency (CISA), and sets forth a number of specific cybersecurity measures such as two-factor authentication and data encryption.[14]

> "The country's highest defense priority is to establish cybersecurity resilient architectures—which will require a "zero trust"-plus approach."

Congress, through the fiscal year (FY) 2021 National Defense Authorization Act (NDAA), likewise has taken some valuable steps toward the goal of establishing cybersecurity resilient architectures. Specifically, section 1736 requires a DOD assessment of an "architecture" to "remotely monitor the public-facing internet attack surface of the defense industrial base."[15] Additionally, section 1739 authorizes threat hunting by the DOD in the defense industrial base as does section 1705 within the federal information systems, and section 1737 focuses on enhanced information sharing.[16]

While the executive order is directed at the federal civil departments and the congressional requirements largely apply to the federal government and the defense industrial base, the actions called for by the executive order and the NDAA will also provide guidance that could be utilized to establish cybersecurity resilient architectures for additional key critical infrastructure sectors. In addition to the federal government and the defense industrial base, as noted in the Atlantic Council report *Effective Resilience and National Strategy,* "cybersecurity resilient architectures should be developed and implemented for the key critical infrastructures of" energy, finance, food, health,

[9] White House, *Executive Order on Improving the Nation's Cybersecurity*, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[10] Kramer and Butler, *Cybersecurity: Changing the Model*, 9-11.

[11] Kramer, *Effective Resilience*, 26-28.

[12] National Security Agency et al., *Russian SVR Targets U.S. and Allied Networks*; "HAFNIUM Targeting Exchange Servers with 0-Day Exploits," Microsoft.

[13] White House, *Executive Order on Improving the Nation's Cybersecurity*, Sections 3(b), (c).

[14] Ibid., Sections 2, 4, 7(c), 3(d).

[15] US Congress, *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*, H.R. 6395, 2020, https://www.govinfo.gov/content/pkg/BILLS-116hr6395enr/pdf/BILLS-116hr6395enr.pdf, Section 1736.

[16] Ibid., Sections 1705, 1737, and 1739.

information and communications technology, transportation, and water.[17] As a starting point for such an effort focused on key critical infrastructures, the Department of Energy has begun an "electricity subsector industrial control systems cybersecurity initiative '100-day sprint' . . . intended to enhance the integrity and security of priority sites' control systems by installing technologies and systems to provide visibility and detection of threats and abnormalities in industrial control and operational technology systems."[18]

The essence of a cybersecurity resilient architecture is to

> organize and coordinate an integrated set of capabilities that will work as a system to provide effective cybersecurity. Key elements of a resilient architecture should include use of private sector cloud technology; zero-trust architectures for effective access management; development of secure hardware capabilities; expanded use of formal coding; and artificial intelligence-augmented cyber defenses. The architectures need to be flexible to incorporate emerging technologies as they are developed and structured to allow for continuous risk mitigation as adversaries change their methods of attack. While there would be commonality in terms of underlying capabilities, different key critical infrastructures will require somewhat different architectures.[19]

As the SolarWinds attack demonstrated, in the area of cyber supply chain resilient architectures, there is a need for artificial intelligence–enabled approaches to more comprehensive monitoring and anomaly characterization that move across interconnected suppliers and customers, and for inspection controls to be incorporated in software development and deployment.

It is reasonably straightforward to identify the components of a cybersecurity resilient architecture. An analysis by the Massachusetts Institute of Technology's Lincoln Laboratory set forth the key elements of zero trust (ZT):

> The core principles behind ZT are: 1) Universal authentication of all users, devices, and services; 2) Access segmentation, allowing no single entity access to more than a small portion of the organization's resources; 3) Minimal trust authorization, keeping access to resources only to those entities that 'need-to-know' and can be trusted; 4) Encryption everywhere to protect information in flight and at rest, whether inside or outside the organization's networks; and 5) Continuous monitoring and adjustment to detect issues early and adjust access accordingly.[20]

It is, however, much more difficult to establish such architectures in practice. Despite agreement on general principles, there is no simple cookie-cutter approach to effective cybersecurity resilience. The Lincoln Laboratory study identified three generic models as well as four real-world commercial architectures. The study states:

> [R]ealizing the concept of ZT has some critical shortcomings. Neither a universally agreed-upon definition of what exactly makes up ZT, nor a set of criteria on when ZT is implemented properly exist. . . . Choosing technologies is difficult due to the wide range of different product choices, as well as a lack of independent analysis into their effectiveness. Vendor's proprietary interfaces prevent integrating capabilities. No metrics for measuring success exist. . . . The scale of the data to be monitored and analyzed is difficult to manage and beyond the capabilities of many current solutions.

Moreover, as the National Security Agency (NSA) has stated, "Implementing Zero Trust takes time and effort: it cannot be implemented overnight. . . . [I]mplementing Zero Trust should not be undertaken lightly and will require significant resources and persistence to achieve."[21] In addition to the effort needed to achieve zero trust, a move to using cloud architecture is likewise a nontrivial effort. Similarly, as described by recent DOD testimony, "Threat hunters are a scarce resource. We don't have the ability to put them

[17] The NDAA provisions amount to a recognition that the DOD's Cybersecurity Maturity Model Certification (CMMC) is a first step, but it is not sufficient in and of itself. Apart from top-tier contractors, most defense industrial base contractors and subcontractors do not have the capacity to meet the cybersecurity threat posed by key adversaries including China, Russia, Iran, and North Korea. Contractor cybersecurity resources—both personnel and financial—are too limited. Making DOD and its contractors and subcontractors capable of defeating the numerous and continuing attacks faced daily will require not only objectives, as the CMMC provides, but capabilities that would be delivered by resilient cybersecurity architectures. Focusing on their prompt development and implementation is a critical element for national security.

[18] Office of Electricity, US Department of Energy, "Department of Energy Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure," *Federal Register* 86, no. 76 (April 22, 2012), https://www.govinfo.gov/content/pkg/FR-2021-04-22/pdf/2021-08482.pdf, 21309.

[19] Kramer, *Effective Resilience*, 27.

[20] K.D. Uttecht, *Zero Trust (ZT) Concepts for Federal Government Architectures*, Lincoln Laboratory, Massachusetts Institute of Technology, July 30, 2020, https://apps.dtic.mil/sti/pdfs/AD1106904.pdf, Executive Summary, v.

[21] National Security Agency, *Embracing a Zero Trust Security Model*, February 2021, https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF, 5, 6.

everywhere and have them be there all the time monitoring everything."[22]

As the foregoing underscores, establishing a cybersecurity resilient architecture will take significant effort. The Department of Defense—which has had success in protecting its networks (recent testimony described "no indications of compromise" from SolarWinds or Hafnium[23])—is nonetheless moving to more fully implement zero trust. However, greater challenges face the federal civil networks and the key critical infrastructures, which are necessary to both defense mission assurance and national resiliency, but have neither the DOD's level of resources nor its cyber expertise.

> "Establishing a cybersecurity resilient architecture for the federal civil agencies and the key critical infrastructures should be undertaken through a combined public-private approach"

Establishing a cybersecurity resilient architecture for the federal civil agencies and the key critical infrastructures should be undertaken through a combined public-private approach, engaging high-end expertise from key elements of the federal government including the Defense Department and the intelligence community as well as the information and communications technology sector, and the critical infrastructures themselves for which the architectures would be developed.[24] There is a great deal of existing expertise, but it has not been focused on developing overall architectures.

For the federal civil agencies, the executive order has set forth an initial way forward including the establishment of agency plans. Much more will be required—as the discussion above demonstrates—but the order does provide a useful, if perhaps implicitly overoptimistic, start. Given the degree of complexity required to establish a full-fledged cybersecurity resilient architecture, including the zero trust aspects discussed above, a useful way to proceed would be for the agencies to utilize a pilot program approach. DOD has developed three "pilots as proof of . . . ZT efficacy," while noting that full departmental implementation will be a "considerable but essential" approach.[25] It seems extremely unlikely that any federal civil department would be able to go directly to an effective cybersecurity resilience architecture without undertaking a similar pilot program, or a "crawl, walk, run" effort. Moreover, adequate resources will need to be provided for threat hunting within the federal civil agencies. As currently resourced, CISA would be hard-pressed to undertake extensive threat hunting;[26] use of private sector certified active defenders, as described in Section II(B)(3), will likely be a requirement.

In contrast to the activities required of the federal agencies as a result of the executive order, there is not a comparable effort yet being undertaken for key critical infrastructures with the exception of the DOE 100-day sprint. But such infrastructures are the backbone for defense mission assurance as well as for national resilience—and there should be a determined effort to enhance their cybersecurity resilience. For the key critical infrastructures, the road is even less clear than that for the federal civil agencies inasmuch as there is no regulatory requirement for most companies to comply with nor, as described above, are there approved standards to adhere to, although the DHS has just undertaken to begin to enhance pipeline security in light of the Colonial Pipeline attack.[27] While not directly relevant, the experience of vaccine development for the coronavirus demonstrates how multiple concerted efforts can achieve desirable results in a relatively short period if appropriate incentives, including necessary resources, are utilized. There is every reason to believe that a wide-ranging and

[22] US Senate, *Stenographic Transcript before the Subcommittee on Cybersecurity, Committee on Armed Services, United States Senate, to Receive Testimony on Future Cybersecurity Architectures*, April 14, 2021, https://www.armed-services.senate.gov/imo/media/doc/21-21_04-14-2021.pdf, 20.

[23] Ibid., 28.

[24] Ibid.; "[C]apabilities will come from both the private sector and the government. The use of private-sector cloud technology, automation, and artificial intelligence can be key for the provision of cybersecurity . . . Additionally, appropriately using highly effective available technology from major government security agencies, including the Department of Defense and the intelligence community, may provide significant benefits to key [critical infrastructures] CIKR." Kramer and Butler, *Cybersecurity: Changing the Model*, 7.

[25] US Senate, *Statement by David W. McKeown, Deputy Chief Information Officer for Cybersecurity and Chief Information Security Officer; Robert Joyce, Director, Cybersecurity Directorate, National Security Agency; and Rear Admiral William Chase III, Deputy Principal Cyber Advisor to the Secretary of Defense, before the Senate Armed Services Committee, Subcommittee on Cybersecurity, on Future Cybersecurity Architectures*, April 14, 2021, https://www.armed-services.senate.gov/imo/media/doc/Joint%20Opening%20Statement.FutureCybersecurityArchitectures2.pdf, 6.

[26] Eric Geller, "America's Digital Defender Is Underfunded, Outmatched and 'Exhausted,'" *Politico*, March 3, 2021, https://www.politico.com/news/2021/03/30/cisa-cybersecurity-problems-478413/.

[27] Ellen Nakashima and Lori Aratani, "DHS to issue first cybersecurity regulations for pipelines after Colonial Hack," *Washington Post*, May 25, 2021, https://www.washingtonpost.com/business/2021/05/25/colonial-hack-pipeline-dhs-cybersecurity/.

fully resourced effort to build cybersecurity resilient architectures for the key critical infrastructures could likewise be accomplished (though likely in a more extended timeframe than for vaccine development). To move forward effectively, both the Joseph R. Biden, Jr. administration and Congress have important roles to play.

An effective way to begin would be for the Department of Defense, in cooperation with the relevant sector-specific agencies as well as DHS and the intelligence community, to organize and oversee pilot programs for four critical infrastructures—the defense industrial base, the electric grid, pipelines, and transportation (air, rail, and ports)—that provide key capabilities to the DOD. The DOD could make participation in such efforts a condition of contracting, along the lines of what is required by the cybersecurity executive order relating to sharing threat information.[28] Congress should provide the resources needed for such a program, both for the federal participants and private sector companies, as there undoubtedly would be costs associated with such an effort. The pilot programs should include multiple highly capable participants from the private sector working with the government and focused on developing cybersecurity resilient architectures. Congress could support such an effort by including in the next National Defense Authorization Act a requirement for such a fast-prototyping effort, and by appropriating the necessary resources.

2) Integrated Cybersecurity Defense Center and the National Cyber Director

A fundamental issue facing the administration and Congress is the role of the national cyber director (NCD)—and, most importantly, whether the NCD will oversee an integrated cybersecurity defense center that will have responsibility for interagency planning and operations including engagement with the private sector.

There have been multiple calls to establish an integrated cybersecurity defense center.[29] An integrated cybersecurity defense center should have both campaign planning and operational roles that would allow it to organize and operate cyber resilience capabilities prior and in response to cyberattacks, similar to the planning and operational activities of "joint interagency task forces" used in other arenas. Such a center would support both the federal government itself and key critical infrastructures, in the latter case working with relevant private sector entities. Given the multiplicity of roles to be effectuated and entities engaged, such a center should be a stand-alone entity along the lines of the highly effective National Cyber Security Centre in the United Kingdom (UK).[30]

> "An integrated cybersecurity defense center should have both campaign planning and operational roles"

An integrated cybersecurity defense center should include the national cyber director and designated personnel and capabilities from the Department of Homeland Security, the Department of Defense, the intelligence community, the Federal Bureau of Investigation (FBI), the Department of Justice (DOJ), the Department of Energy, the Department of Treasury, and the Department of State. The DHS National Cybersecurity and Communications Integration Center and hunt and incident-response teams and the DOD national protection teams from Cyber Command should generally operate as part of the center when focused on domestic cybersecurity resilience. The center should work with the federal civil departments to support their cybersecurity efforts and should closely coordinate with the Department of Defense's cyber "defend forward/persistent engagement" strategy as part of establishing cyber deterrence and resilience within the United States. As an additional core element of an effective strategy, the center should also work with key critical infrastructures in the private sector as described below as well as coordinate with the National Guard in its state cybersecurity role.

Section 1731 of the FY21 NDAA takes a first step in this direction with the requirement of a report to "addres[s] . . . the creation of an integrated cybersecurity center within the [DHS] Cybersecurity and Infrastructure Agency" that potentially would include the National Security Agency, Cyber Command, the Office of the Director of National Intelligence (DNI), and the FBI.[31] While this is only an initial reporting requirement, establishing such a center is long overdue. Moreover, while not specifically linked, section 1731 implicitly builds on section 1715, which established within DHS CISA a joint cyber planning office that would

[28] White House, *Executive Order on Improving the Nation's Cybersecurity*, Section 2.

[29] Kramer and Butler, *Cybersecurity: Changing the Model*, 14-15; James N. Miller and Robert Butler, "Making the National Cyber Director Operational with a National Cyber Defense Center," Lawfare, March 24, 2021, https://www.lawfareblog.com/making-national-cyber-director-operational-national-cyber-defense-center.

[30] The National Cyber Security Centre, https://www.ncsc.gov.uk/.

[31] US Congress, *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*, Section 1731.

also include representatives from Cyber Command, the NSA, the FBI, the DOJ, and the DNI. Section 1731 does not, however, reference the NCD.

The position of the national cyber director was established by section 1752 of the FY21 NDAA. The NDAA focuses the NCD's role on strategy development and the coordination of departmental cyber activities. However, the NCD is appropriately positioned to head a stand-alone, integrated cybersecurity defense center. Former Under Secretary of Defense for Policy James Miller and former Deputy Assistant Secretary of Defense for Cyber and Space Policy Robert Butler have set forth a detailed analysis as to how such a center would operate.[32] As they have described,

> The NCDC [National Cyber Defense Center] would conduct cyber defense campaign planning and coordinate U.S. government actions below the level of armed conflict, while also conducting contingency planning for cyber defense in the event of crisis or war. In support of each of these roles, the NCDC would plan and coordinate four intertwined lines of effort: cyber deterrence, active cyber defense, offensive cyber actions in support of defense, and incident management.[33]

As Miller and Butler have written, a stand-alone, integrated cyber defense center under the NCD "in the Executive Office of the President is needed to make this work."[34] Miller and Butler recommend that the CISA director be dual-hatted as a deputy director to the NCD so as to align section 1715 with the value of having a more fully developed, stand-alone, integrated center.[35]

The importance of a fully integrated effort cannot be overstated. Only a comprehensive government effort would have the integrated capabilities required. The DHS does have excellent connectivity with many elements of the private sector; the DOD has unmatched planning and operational capabilities; the intelligence community has a view of the cyber threat picture; and entities like the FBI and the Treasury Department can most effectively work within a joint center to coordinate investigations, indictments, and sanctions. In sum, an integrated cybersecurity defense center would be significantly more valuable than a far less resourced and significantly less comprehensive entity within a single agency.

3) The Private Sector: Sector Analysis and Defense Centers and Certified Active Defenders

As the discussion above indicates, a key change for the cybersecurity defense of the United States should be moving from the long-standing approach of public-private information sharing to one of public-private coordinated defense. In addition to cybersecurity resilient architectures and an integrated cybersecurity defense center, two key elements of the effort would be establishing "Sector Analysis and Defense Centers" for key critical infrastructures and implementing private sector "certified active defenders" to complement government capabilities.

The key point of creating Sector Analysis and Defense Centers is to go beyond information sharing[36] to engage key private sector entities in activities relevant to cybersecurity defense. Bringing key companies in a sector together would add to the cumulative impact of public-private coordination. An "SADC" would have a sector-specific focus (though it might encompass compatible sectors) and be designed to coordinate the most significant entities within a sector, thereby generally following the organizational model of the Analysis and Resilience Center for Systemic Risk (ARC).[37] The ARC brings together the members of the Financial Systemic Analysis and Resilience Center and significant companies in the energy arena.[38] The ARC undertakes risk analysis and "operational collaboration between ARC's member companies, sector partners, and the U.S. government."[39] It "conduct[s] analysis of critical systems, assets and functions; monitor[s] and warn[s] against threats to those systems, assets, and functions; and develop[s] measures to make them more resilient."[40] The SADCs would act in coordination with the proposed integrated cybersecurity defense center to help effectuate cybersecurity resilience through risk reduction activities for those sectors. The SADCs could be a locus for information/intelligence exchange and could help

[32] Miller and Butler, "Making the National Cyber Director Operational with a National Cyber Defense Center."

[33] Ibid.

[34] Ibid.

[35] Ibid.

[36] As is currently undertaken by Information Sharing and Analysis Centers and Information Sharing and Analysis Organizations. See Jaikumar Vijayan, "What Is an ISAC or ISAO? How These Cyber Threat Information Sharing Organizations Improve Security," CSO, July 9, 2019, https://www.csoonline.com/article/3406505/what-is-an-isac-or-isao-how-these-cyber-threat-information-sharing-organizations-improve-security.html.

[37] Analysis & Resilience Center, https://www.systemicrisk.org/; see "Announcing the Formation of the Analysis & Resilience Center (ARC) for Systemic Risk, *BusinessWire*, October 30, 2020, ttps://www.businesswire.com/news/home/20201030005462/en/Announcing-the-Formation-of-the-Analysis-Resilience-Center-ARC-for-Systemic-Risk.

[38] Currently twenty-seven entities. "Who We Are," ARC, accessed May 21, 2021, https://systemicrisk.org/who-we-are/#members.

[39] "Announcing the Formation of the Analysis & Resilience Center (ARC) for Systemic Risk," *BusinessWire*.

[40] "What We Do," ARC, https://www.systemicrisk.org/what-we-do/.

coordinate planning for responses in the event of a significant cyberattack. A recent report by the New York Cyber Task Force recommended "organizational partnerships that enable coordinated responses to severely disruptive cyber crises . . . allow[ing] the private and public sectors to conduct coordinated cyber defense actions through highly synchronized planning and operations, as well as develop[ing] joint cyber capabilities to respond to adverse cyber events."[41]

An important element of the operational aspects of effective cybersecurity is the requirement for "active cyber defenses" that can create resilience even when an attacker has breached cyber protections. Active cyber defense includes threat hunting capabilities, sandboxing, and in-network deception.[42] Accomplishing active cyber defense effectively requires highly developed cyber capabilities dedicated to the task. Understanding what the adversary is doing both forward and in the American theater adds to the capacity to accomplish active defense.

Congress recognized the importance of active defense in the provisions, noted above, authorizing threat hunting in government networks and in the defense industrial base. The latter (per section 1739) authorizes the secretary of defense "to establish the defense industrial base cybersecurity threat hunting program" if the secretary makes a "positive determination . . . of the feasibility and suitability of establishing a defense industrial base cybersecurity threat hunting program."[43] Among the important considerations that the secretary is directed to consider is which type of entities should conduct such a threat hunting program, with the statute providing several options: "(A) qualified prime contractors or subcontractors; (B) accredited third-party cybersecurity vendors; (C) with contractor consent— (i) United States Cyber Command; or (ii) a component of the Department of Defense other than United States Cyber Command."[44]

The full defense industrial base is very large, including more than one hundred thousand firms,[45] so an effective threat hunting strategy will necessarily require engaging the private sector—and an important issue will be how much of the defense industrial base to include, which will likely turn in part on the feasibility of widespread use of automated systems. The use of private sector certified active defenders—which could include both prime contractors, subcontractors, and qualified third-party cybersecurity vendors—to provide active defense for the defense industrial base would be an important element of an effective resilience/defend back strategy. "Certified active defenders" could be drawn from private sector entities with high-level cyber capabilities including high-end ICT firms; support might also come from federally funded research and development centers and university-affiliated research centers.[46] Both SolarWinds and the Microsoft Hafnium attacks are illustrative of the value that the private sector can bring as the original detection of each of the intrusions was accomplished by a private sector firm.

> "an effective threat hunting strategy will necessarily require engaging the private sector"

A key differentiation between existing private sector cybersecurity providers and certified active defenders could be potential ongoing access to government intelligence information and a capacity to plan with the government, which will also require the government to determine what rules will be required for certified active defenders. The government could also decide to provide key capabilities to select certified active defenders. Certified active defenders could undertake an ongoing review of system activities for defense industrial base firms, detect anomalies, defeat intruders, and undertake remediation, for example, by deleting malware and closing unnecessary ports. Certified active defenders and chief information security officers of the private sector firms should establish protocols for joint activities. Part of the activities of certified active defenders should be engaging in joint training and exercising with key defense industrial base firms to be ready to respond to high-end cyber incidents if required.

An important issue for consideration is the appropriate procedure to be undertaken when defeating a cyber threat requires taking action outside the network in which the

[41] New York Cyber Task Force, *Enhancing Readiness for National Cyber Defense through Operational Collaboration,* Columbia School of International and Public Affairs, 2021, https://www.sipa.columbia.edu/sites/default/files/embedded-media/NYCTF%20-%20Enhancing%20Readiness%20for%20National%20Cyber%20Defense%20through%20Operational%20Collaboration.pdf, 6.

[42] National Security Agency, Central Security Service, "Active Cyber Defense," August 4, 2015, https://apps.nsa.gov/iad/programs/iad-initiatives/active-cyber-defense.cfm.

[43] US Congress, *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*, Section 1739(e).

[44] Ibid., Section 1739(b)(4).

[45] "Defense Industrial Base Sector," Cybersecurity & Infrastructure Security Agency, accessed April 18, 2021, https://www.cisa.gov/defense-industrial-base-sector.

[46] See descriptions at Marcy E. Gallo, *Federally Funded Research and Development Centers (FFRDCs): Background and Issues for Congress,* Congressional Research Service, updated April 3, 2020, https://crsreports.congress.gov/product/pdf/R/R44629/6.

SPOTLIGHT: Expanding the Role of the National Guard in Cybersecurity

Cybersecurity for key critical infrastructures as well as for state and local governments could be significantly improved if a focused effort were undertaken to expand the cybersecurity capabilities of the National Guard ("the Guard"). In the event of a high-end conflict, the expanded National Guard capabilities could support Department of Defense missions. In substance, the National Guard could be a key part of an "effective resilience/defend back" strategy.

The National Guard generally works under the authorities of the governor of the state but can be federalized by the president when required. In the cyber arena, according to the National Guard Bureau, "There are more than 3,900 Army and Air National Guard personnel serving in 59 DoD cyber units in 40 states."[1] The Guard's cyber missions are wide-ranging and, at the federal level, include "directly support[ing] the U.S. Cyber Command's Cyber Mission Forces (CMF) construct."[2] At the state level,

> 27 states used Guard members in a non-federal status to support state and local agencies in 2019. This support included response and remediation of cyber incidents; cyber defense analysis; cyber incident response planning; election security planning, threat assessment, and interagency planning. . . . National Guard cyber teams responded to ransomware attacks in Texas, Louisiana, California, Colorado and Montana in 2019.[3]

Congress has recognized the contributions that the Guard brings to cybersecurity and has directed the Defense Department to evaluate expanding Guard cyber missions. Section 1725 of the FY21 NDAA provides for analysis of multistate Guard activities, and specifically for a "pilot program" authorizing National Guard units in one state to support the cyber efforts of another state's Guard units.[4] As part of the pilot program, DOD will "conduct an assessment of . . . existing cyber response capacities of the Army National Guard or Air National Guard, as applicable, in each State."[5]

Similarly, section 1729 of the NDAA requires a joint briefing (three hundred days after enactment) by the secretary of defense and the secretary of homeland security to Congress on

> [h]ow the Department of Defense, including the National Guard, and the Department of Homeland Security, including the Cybersecurity and Infrastructure Security Agency and the Federal Emergency Management Agency, will collaborate with each other and with relevant law enforcement, State governments, and other non-Federal entities when responding to and recovering from significant cyber incidents.[6]

Combined, sections 1725 and 1729 give the Defense Department the opportunity to recommend a significantly expanded National Guard cybersecurity role for the nation. Five steps should be taken to enhance cybersecurity for key critical infrastructures and for state and local governments.

—First, the number of National Guard personnel directed toward the cyber mission should be significantly increased. Congress has asked DOD to assess National Guard cyber capabilities, but a reasonable initial step would be to increase Guard end strength by approximately doubling the current number of cyber personnel. That would allow the Guard to do a great deal more assessments and other interactions with key critical infrastructure providers "left of boom" (i.e., before an incident), which would help increase the resilience of entities like the electric grid or water treatment plants, which have become increasingly at risk. Similarly, an increase in Guard cyber personnel could be particularly helpful for states to establish effective resilience programs in support of local governments, which face continuing ransomware and other attacks,

[1] National Guard, *2021 National Guard Posture Statement: Force for the Future*, US Department of Defense, 2021, https://www.nationalguard.mil/portals/31/Documents/PostureStatements/2021%20National%20Guard%20Bureau%20Posture%20Statement.pdf, 6.

[2] Ibid.

[3] Ibid., 23.

[4] US Congress, *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*, Section 1725.

[5] Ibid.

[6] Ibid., Section 1729.

and yet, for the most part, do not have the resources to establish effective cybersecurity for themselves.[7]

—Second, it will be important to determine how best to recruit highly capable people into the Guard's cyber units. This very well might require different "nontraditional" arrangements that Congress has already suggested be considered for the federal government,[8] including perhaps monetary incentives or flexible work arrangements. As a starting point, however, federal and state government leaders could work together to approach chief executives of cybersecurity, cloud, and telecommunications companies about recruiting personnel to the National Guard. Such an effort would help leverage the best of the United States' talent in the private sector to support federal and state cyber protection missions.

—Third, the Guard's capabilities need to be included in established response planning and procedures, which need to be regularly exercised. This is particularly true for the Guard's support to states and localities. The Army Cyber Institute, as a result of a series of exercises that it undertook with state and local governments, has now developed digital tools and processes that state military departments can use to help communities assess and improve their cyber postures.[9] The National Guard could become the maintainer and sustainer of this tool set as part of its expanded National Guard cybersecurity mission ensuring that the capabilities are widely available for homeland defense. As a recent New York Cyber Task Force analysis found:

> [C]ities may not know how to properly use National Guard units deployed to help them in a crisis, due to a lack of knowledge of National Guard capabilities and organizational structure. For the capabilities and expertise of potential response forces, like the National Guard, to be deployed to the greatest advantage in a cyber crisis, these capabilities and integration process must be understood, mapped, and practiced well in advance.[10]

—Fourth, as section 1725 of the FY21 NDAA suggests, it will be important to build regional capabilities between and among Guard units. High-end cyber defense capabilities fall into a category that the Defense Department characterizes as "high demand, low density," which is to say a lot may be needed but not that many providers are available. Generating regional capabilities will help ensure that a critical mass of highly capable cybersecurity professionals will have had the opportunity to train and exercise together prior to a contingency in which their talents are needed. Moreover, like the Washington National Guard, which has deep expertise in industrial control system security,[11] certain Guard units, because of the nature of businesses in their state, may have expertise that could then be more broadly provided. As part of this effort and to meet the needs across state lines, federal and state government leadership should work to develop cross-state agreements for regional support.

—Fifth, several National Guard units currently engage on an ongoing basis on cybersecurity with a number of US allies[12] as part of the Guard's State Partnership Program.[13] Lessons learned and information generated from such activities can usefully be applied to the Guard's role in defending back in the United States and can be shared from one Guard unit to another.

Finally, in undertaking its cybersecurity activities, the state National Guard should engage with the proposed integrated cybersecurity defense center as well as with the newly established "cybersecurity state coordinator" that the FY2021 NDAA established for each state.[14]

This Spotlight section is an updated version of "Expanding the Role of the National Guard for Effective Cybersecurity," by Franklin D. Kramer and Robert J. Butler, which was first published in *The Hill* on April 28, 2021.

[7] Kramer and Butler, *Cybersecurity: Changing the Model*, 9-14.

[8] US Congress, *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*, Sections 1730 and 1739.

[9] "Jack Voltaic 3.0," Army Cyber Institute, last updated March 31, 2021, https://cyber.army.mil/Research/Jack-Voltaic/.

[10] New York Cyber Task Force, *Enhancing Readiness for National Cyber Defense through Operational Collaboration*, 15.

[11] Joseph Siemandel, "New Washington National Guard Cyber Team Stands Up to Protect DoD Infrastructure," US Army, April 26, 2019, https://www.army.mil/article/220983/new_washington_national_guard_cyber_team_stands_up_to_protect_dod_infrastructure.

[12] Maj. Kurt Rauschenberg, "Md. Guard Exercises Cyber Awareness with Estonian Comrades," *National Guard News,* May 18, 2018, https://www.nationalguard.mil/News/State-Partnership-Program/Article/1525147/md-guard-exercises-cyber-awareness-with-estonian-comrades/.

[13] "State Partnership Program," National Guard, accessed April 18, 2021, https://www.nationalguard.mil/leadership/joint-staff/j-5/international-affairs-division/state-partnership-program/.

[14] US Congress, *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*, Section 1717.

threat is initially found. Disabling adversary command and control, for example, could be important to keep an adversary intrusion from spreading and that certainly could be an important defensive measure in the context of a massive cyberattack or an actual conflict. The FBI does, however, have the authority to obtain a warrant to take action against malware if a violation of 18 U.S.C. section 1030 has occurred including unauthorized access, theft, or damage to a computer in interstate commerce.[47] That authority was used recently to seize malware generated by the Chinese Hafnium intrusions,[48] and would likewise be available for comparable future efforts. As the foregoing implies, the benefits from combining defense industrial base threat hunting—undertaken as proposed above by private sector certified active defenders—with FBI seizures underscores the value of an integrated cyber defense center.

Establishing threat hunting in the defense industrial base implicitly raises the important questions of whether there should be comparable programs for other key critical infrastructures. Defense mission assurance relies not only on the defense industrial base, but, in an operational context, equally or even more so on the electric grid, pipelines, transportation, and the information and communications technology sector (and, of course, the impact of disruptions to such key critical infrastructures goes well beyond defense issues). The Biden administration recently launched a one hundred–day effort to "enhance the cybersecurity of electric utilities' industrial control systems (ICS) and secure the energy sector supply chain."[49] In the next NDAA, Congress should require an analysis for key critical infrastructure sectors similar to the analysis the secretary of defense will undertake for the defense industrial base. In undertaking such an analysis, important issues that will arise will include intellectual property protection and, for at least the ICT sector (and perhaps others), there will be questions involving matters of privacy and civil liberties for individuals. The analysis should consider the benefit of using certified active defenders in those circumstances since, as private companies, their utilization would mean that the government would not itself be engaged on critical infrastructure networks, so that issues of privacy and protection of intellectual property from government monitoring or other forms of government involvement would not be directly implicated.

Constitutional limitations and protection of civil liberties and individual rights remain crucially important in a democracy even during wartime. The Biden administration and Congress might direct the Cyberspace Solarium Commission, perhaps with expanded chairmanship so that interests involving civil liberties and individual rights are appropriately represented, to review how cybersecurity for key critical infrastructures, including in high-end/wartime circumstances, might be accomplished in a fashion compatible with constitutional and civil liberty concerns. As part of such a review, the role of certified active defenders might be evaluated as a potential bridging mechanism that could help ensure that government engagement would not inappropriately intrude on private personal information or undercut constitutional and civil liberty interests. A report could then be provided both to the administration and to Congress as a basis for potential legislation.

C. Supply Chain Resilience Requires Limits on China

Supply chain resilience is a necessary component of Defense Department mission assurance. From a defense perspective, a key element will be limiting China's inclusion in defense, intelligence community, and key critical infrastructure supply chains.[50]

The Biden administration has initiated a two-step supply chain review. Though broader than defense issues, the review will cover multiple areas that are critical to defense, as the initiating executive order provides:

> First, the order directs an immediate 100-day review . . . of . . . Critical minerals [which] are an essential part of defense, high-tech, and other products. . . .[including] rare earths . . ., Semiconductors and

[47] 18 U.S. Code § 1030 – "Fraud and related activity in connection with computers," via Cornell Law School, Legal Information Institute, https://www.law.cornell.edu/uscode/text/18/1030.

[48] "Motion to Partially Unseal Search Warrant and Related Documents and [Proposed] Order in the Matter of the Search of: Certain Microsoft Exchange Servers Infected with Web Shells," Case No. 4:21mj755, United States District Court, Southern District of Texas, Houston Division, filed April 13, 2021, https://content.govdelivery.com/attachments/USDOJOPA/2021/04/13/file_attachments/1753980/AUSA%20McIntyre%20Motion%20to%20Partially%20Unseal%20Search%20Warrant.pdf?utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202.

[49] US Department of Energy, "Biden Administration Takes Bold Action to Protect Electricity Operations from Increasing Cyber Threats," April 20, 2021, https://www.energy.gov/articles/biden-administration-takes-bold-action-protect-electricity-operations-increasing-cyber-0.

[50] By contrast, reliance on allies and certain partners is regularly undertaken in multiple areas, and the executive order on supply chain follows that approach, calling for "actions that can successfully engage allies and partners to strengthen supply chains jointly or in coordination." White House, *Executive Order on America's Supply Chains*, February 24, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/, Section 5(d). Congress has likewise authorized including allies and partners in the supply chain in the FY21 NDAA, which provides that "the policy of the United States should be to work with its NATO and other allies and partners to build permanent mechanisms to strengthen supply chains, enhance supply chain security, fill supply chain gaps, and maintain commitments made at the June 2020 NATO Defense Ministerial, particularly regarding pandemic response preparations." US Congress, *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*, Section 1244(9).

> Advanced Packaging . . .[and] Large capacity batteries . . .
>
> Second, the order calls for a more in-depth one-year review . . . [with a] focus on six key sectors: the defense industrial base; the public health and biological preparedness industrial base; the information and communications technology (ICT) industrial base; the energy sector industrial base; the transportation industrial base; and supply chains for agricultural commodities and food production.[51]

National defense supply chains rely on each of these sectors. Generally, the objective of the supply chain review should be to establish a "resilient industrial base" for the relevant sector that could maintain the required capabilities in the face of adversarial shocks as well as over the long term.[52] It will also be important from a DOD perspective for the supply chain review to look to the future. Research and development will be quite important, particularly given China's intent to dominate those technologies.[53]

China is, however, not only a technological competitor, but also significantly incorporated into multiple supply chains. For defense mission assurance and as more fully described below, there are certain sectors from which China should be entirely excluded from the supply chain and others where less stringent requirements such as a "China plus one" strategy could be a satisfactory approach.[54]

"there are certain sectors from which China should be entirely excluded from the supply chain and others where less stringent requirements such as a "China plus one" strategy could be a satisfactory approach"

To begin, "for strategic sectors vital to national security or other critical national objectives, Chinese products, components, and services should be excluded from the supply chain unless the use is approved by the US government. That limitation would encompass the defense sector and the intelligence community."[55] Other sectors could also be included. As of this writing, the Biden administration is keeping in place, while it develops its overall policy, regulations that would allow for limits on supply chains in the bulk power and information and communications technology sectors—which presumably would be used with respect to China.[56] At a minimum, the use of Chinese software in the supply chains of key critical infrastructures should be prohibited. As the SolarWinds and Microsoft Hafnium attacks have demonstrated, supply chains can be utilized to insert maliciously intended flaws that could lead to exploitations posing significant risks.[57]

[51] White House, "Fact Sheet: Securing America's Critical Supply Chains," February 24, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/02/24/fact-sheet-securing-americas-critical-supply-chains/. In the FY2021 NDAA, Congress has required the DOD to focus on supply chain risk management issues including dependencies on strategic and critical materials (such as rare earths and graphite) and on key products and components (such as printed circuit boards and wireless technology (5G)). US Congress, *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*, Sections 841, 850, 851, 9202, and 9413.

[52] An earlier DOD/interagency supply chain review identified multiple types of supply chain risks. Those included risks arising from sole and single-source suppliers; fragile suppliers (financially challenged); fragile markets (cannot meet foreign competition); capacity-constrained markets; foreign dependency; diminishing sources/suppliers of material necessary to components or final products; gaps in human capital; lack of sufficient specialized capital equipment; and insecurity of product, whether physical or cyber. Interagency Task Force, *Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806, Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States*, US Department of Defense, September 2018, https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF; see Kramer, *Effective Resilience*, 21.

[53] As the National Security Commission on Artificial Intelligence stated, "Ensuring U.S. leadership in the manufacturing of key emerging technology platforms will be an essential component of national competitiveness. . . " The commission listed as key technologies, in addition to artificial intelligence itself, biotechnology, quantum computing, semiconductors and advanced hardware, robotics and autonomy, 5G and advanced networking, advanced manufacturing, and energy technology. Each of these will be important factors in future supply chains. See National Security Commission on Artificial Intelligence, *Final Report*, 2021, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf, 257 and 253-266.

[54] Kramer, *Effective Resilience*, 22; Franklin D. Kramer, *Managed Competition: Meeting China's Challenge in a Multi-vector World*, Atlantic Council, December 2019, https://www.atlanticcouncil.org/wp-content/uploads/2019/12/Meeting-Chinas-Challenges-Report-WEB.pdf, 2.

[55] Kramer, *Effective Resilience*, 22. There have been a number of determinations by the federal government limiting the use of products from China including, for example, a rule prohibiting federal agencies from contracting with companies that use in their systems telecommunications equipment produced by Huawei Technologies Company, ZTE Corporation, or their affiliates. US Federal Acquisition Regulatory Council, "Federal Acquisition Regulation: Prohibition on Contracting with Entities Using Certain Telecommunications and Video Surveillance Services or Equipment," July 14, 2020, https://www.federalregister.gov/ documents/2020/07/14/2020-15293/federal-acquisition-regulation-prohibition-on-contracting-with-entities-using-certain.

[56] US Department of Commerce, "ICT Supply Chain," accessed April 23, 2021, https://www.commerce.gov/issues/ict-supply-chain; US Department of Energy, Office of Electricity, "Securing the United States Bulk-Power System Executive Order," April 20, 2021, https://www.energy.gov/oe/securing-united-states-bulk-power-system-executive-order.

[57] Trey Herr, June Lee, William Loomis, and Stewart Scott, *Breaking Trust: Shades of Crisis across an Insecure Software Supply Chain*, Atlantic Council, July 2020, https://www.atlanticcouncil.org/wp-content/uploads/2020/07/Breaking-trust-Shades-of-crisis-across-an-insecure-software-supply-chain.pdf, 6.

Additionally, as detailed in the Atlantic Council report *Effective Resilience and National Strategy,* limitations on

> [h]ardware and other materials from China need to be established in situations where China is the sole or dominant source. Congress has required under section 3112 of the CARES Act that certain pharmaceutical providers have a resilience plan.[58] A resilience plan mandate could be expanded to other key critical infrastructures, with the requirement that designated firms would have to avoid a situation in their supply chains where there is sole or dominant reliance on China. The basic concept would be that a cutoff of supply by China should not cause a sweeping impact on the relevant sector. One way to accomplish this would be to require dual sourcing by adding a mandate for the supply chain to include a 'plus one' country. Companies would, therefore, not be forced to entirely upend their supply chains that rely on China but could be required to expand them to include other countries. Doing so would incur costs but has concomitant assurance benefits for firms, as well as making sectors more resilient as a whole.[59]

The administration should develop a roadmap for key critical infrastructure sectors, and the degree of any needed expansion to "plus one" countries could be increased incrementally in time, allowing smooth adjustment to the capacity of supply chains. The administration should also evaluate the use of tax and other incentives to support required changes. Ultimately, for the key critical infrastructures, supply chain dual sourcing should be required encompassing a "plus one" country, ensuring that the PRC is not in a dominant position as a primary or sole supplier.

[58] US Congress, "Additional Manufacturer Reporting Requirements in Response to Drug Shortages" in *Coronavirus Aid, Relief, and Economic Security Act*, January 3, 2020, https://www.congress.gov/116/bills/hr748/BILLS-116hr748enr.pdf, Section 3112.

[59] Kramer, *Effective Resilience*, 22-23.

III. THE FORWARD THEATERS: A TAILORED MULTI-THEATER STRATEGY

The priority defense theaters for the United States are the American theater (as noted above), and, for forward defense, the Indo-Pacific and European theaters.[60] There is no doubt that China is the pacing challenge facing the United States.[61] However, while China presents the most significant long-term country challenge to the United States and possibly will also have the most effective suite of defense capabilities, Russia likewise presents a major threat in Europe where the United States has vital interests.[62] Accordingly, a tailored multi-theater defense strategy that appropriately balances risks and capabilities between and among the Indo-Pacific and Europe, and which accounts for the changing nature of the battlespace, is necessary.

A. Indo-Pacific

In the Indo-Pacific, US allies are of vital interest to the United States for values, economic, and security reasons, and the United States also has important partners of consequential significance. China presents the key defense challenge, particularly with respect to the defense of Taiwan but also with its claims and incursions in the East and South China Seas and with respect to its border disputes with India.

The United States has long had a defense strategy for the Indo-Pacific as set forth in the Defense Department's *Indo-Pacific Strategy Report*[63] and which has historically been effective in maintaining peace and stability for the region. The combination of growth in Chinese capabilities accompanied by China's generally more aggressive posture has required the United States to evaluate how to enhance its existing military capabilities for the region. Admiral Philip Davidson, commander of Indo-Pacific Command, has testified that the "greatest danger for the United States is the erosion of conventional deterrence."[64] He identified four key priorities for maintaining deterrence as joint force lethality; enhancing the force design and posture; strengthening allies and partners; and modernizing exercises, experimentation, and innovation programs.[65] Congress has supported such efforts including by establishing the Pacific Deterrence Initiative (PDI). The FY2021 NDAA provides that the purpose of the PDI is to

> carry out prioritized activities to enhance the United States deterrence and defense posture in the Indo-Pacific region, assure allies and partners, and increase capability and readiness in the Indo-Pacific region.[66]

Additionally, the NDAA requires that a report be submitted to Congress including required investments "necessary to achieve measurable progress in reducing risk to the joint force's ability to achieve objectives in the region."[67] Media

[60] As noted above, several other areas of consequence including the Middle East, Afghanistan, and Africa will require an economy of force approach, and on the Korean peninsula, the United States and the Republic of Korea have a well-established collective defense strategy. Additionally, counterterror will remain an important defense task but generally does not require large numbers of personnel, though it does need high-end capabilities and support including from the intelligence community. US Senate, "Posture Statement of General Richard D. Clarke, USA Commander, United States Special Operations Command before the 117th Congress Senate Armed Services Committee March 25, 2021," March 25, 2021, https://www.armed-services.senate.gov/imo/media/doc/Clarke_03-25-21.pdf.

[61] Secretary of Defense, "Message to the Force."

[62] Additionally, the United States faces a changing nuclear threat in that Russia and China each are consequential nuclear adversaries undertaking modernization of their forces, North Korea is increasing its capabilities such that it may have the capacity to undertake a nuclear attack on the United States, and the situation with Iran remains unclear. In light of the extension of New START and US nuclear modernization programs, the United States appears well-positioned to generate strategic stability vis-à-vis China and Russia for the near term, but there should continue to be analysis of the requirements for the medium and longer terms including whether arms control may have an important role. With respect to North Korea, deterrence, including extended deterrence for Indo-Pacific allies, will be a requisite; negotiations should always be evaluated, but negotiations with North Korea have been unsuccessful for the past quarter century.

[63] US Department of Defense, *Indo-Pacific Strategy Report*, June 1, 2019, https://media.defense.gov/2019/Jul/01/2002152311/-1/-1/1/DEPARTMENT-OF-DEFENSE-INDO-PACIFIC-STRATEGY-REPORT-2019.PDF.

[64] US Senate, "Statement of Admiral Philip S. Davidson, U.S. Navy Commander, U.S. Indo-Pacific Command, before the Senate Armed Services Committee," March 9, 2021, https://www.armed-services.senate.gov/imo/media/doc/Davidson_03-09-21.pdf, 3.

[65] Ibid.

[66] US Congress, *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*, Section 1251(a).

[67] Ibid., Section 1251(d)(3). Congress has directed that the report cover investments in multiple categories including "investments in— (A) active and passive defenses against unmanned aerial systems and theater cruise, ballistic, and hypersonic missiles; (B) advanced long-range precision strike systems; (C) command, control, communications, computers, intelligence, surveillance, and reconnaissance systems; (D) test range capacity, capability, and coordination; (E) dispersed, resilient, and adaptive basing to support distributed operations, including expeditionary airfields and ports; (F) advanced critical munitions; (G) pre-positioned forward stocks of fuel, munitions, equipment, and materiel; (H) distributed logistics and maintenance capabilities; (I) strategic mobility assets; (J) improved interoperability and information sharing with allies and partners; (K) information operations capabilities; (L) bilateral and multilateral military exercises and training with allies and partners; and (M) use of security cooperation authorities to further build partner capacity."

reports state that the proposed PDI plan for FY2022-2027 is "$4.68 billion in Fiscal Year 2022, . . .[and] $22.69 billion from FY 2023 through FY 2027."[68] While these are not large amounts in the context of the $700 billion-plus national defense budget, the items identified in the PDI report are intended to be complementary to programs included in the larger, regular DOD budget. Nonetheless, despite the amount of resources being devoted to the Indo-Pacific, there remain significant concerns as to the state of the military balance.[69]

The discussion below proposes four major enhancements to the current Indo-Pacific strategy to strengthen deterrence as well as warfighting capabilities: 1) allied commitments to support the United States in the event of conflict with China; 2) establishment of multinational force capabilities for warfighting and for maritime support; 3) establishing cybersecurity and supply chain resilience with allies; and 4) expanded use of unmanned vehicles, offensive cyber and directed energy, hypersonic weapons, and naval mining capabilities.

1) Commitment by Allies to Support the United States in the Event of a Conflict with China

The Indo-Pacific should not present the United States with a "go it alone" military situation. Allies should actively support the United States in the context of a conflict with China—certainly with respect to attacks on one another, but also and importantly with respect to Taiwan. A planned combined effort would be a major geopolitical change and would require several significant decisions on the part of allies. However, the changed context with China—and particularly its aggressive behavior—calls for such a consequential change in the event China precipitates a conflict. Initially, such a commitment could be pragmatic, arising from multiple common approaches and appropriate declaratory policy. Longer term, however, the United States and its allies should seek to undertake defense in the Indo-Pacific as a collective effort.

As noted above, Admiral Davidson has testified that the "greatest danger for the United States is the erosion of conventional deterrence."[70] That danger is equally great—and perhaps even more so—for allied nations in the Indo-Pacific, and any such erosion likewise has worldwide ramifications. Importantly, however, a commitment by allies to support the United States would be a major deterrent to China beginning a conflict. China would face the reality that it would be acting in the face of widespread opposition. The concern that undoubtedly would be raised is that any such commitment would itself be destabilizing and could lead to conflict. There is no doubt that such a commitment would present a challenge to what China sees as one of its core interests. However, failure to keep Taiwan free would be a defeat for the core interests of the United States and its allies. Both security interests in the Indo-Pacific and democratic values worldwide would be undercut by a failure to maintain Taiwan's freedom. A successful attack by China would be fundamentally destabilizing to the democratic world order. It would not only impact the nations of the Indo-Pacific, but have worldwide ramifications including for Europe. In sum, the changed geopolitical circumstances require changed geopolitical responses.

Recent statements in the context of US-Japanese high-level meetings, including by President Biden and Prime Minister Yoshihide Suga, "underscore[ing] the importance of peace and stability in the Taiwan Strait"[71] provide an initial starting point. The United States has not been specific as to the certainty of a response should China attack Taiwan, though the secretary of state recently stated, "We have a serious commitment to peace and security in the Western Pacific. We stand behind those commitments. And in that context, it would be a serious mistake for anyone to try to change that status quo by force."[72] Accordingly, allied statements should focus on support to the United States, and there should be much greater clarity initially from each of Japan, Australia, and the Republic of Korea (ROK) on such a commitment.[73] At a minimum, these allies need to make clear that trade and other economic interactions with China could not continue if China were in a conflict with the United States. Second, it similarly needs to be clear that the United States could utilize the facilities in each of

[68] Mallory Shelbourne, "U.S. Indo-Pacific Command Wants $4.68B for New Pacific Deterrence Initiative," *US Naval Institute News*, updated March 2, 2021, https://news.usni.org/2021/03/02/u-s-indo-pacific-command-wants-4-68b-for-new-pacific-deterrence-initiative.

[69] David Ochmanek, *Restoring U.S. Power Projection Capabilities,* RAND, July 2018, https://www.rand.org/pubs/perspectives/PE260.html.

[70] US Senate, "Statement of Admiral Philip S. Davidson," 3.

[71] White House, "U.S. – Japan Global Partnership for a New Era," U.S.- Japan Joint Leaders' Statement, April 16, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/16/u-s-japan-joint-leaders-statement-u-s-japan-global-partnership-for-a-new-era/; US Department of State, "U.S.-Japan Joint Press Statement," March 16, 2021, https://www.state.gov/u-s-japan-joint-press-statement/.

[72] "Blinken Warns of China's 'Increasingly Aggressive Actions' against Taiwan," Reuters, April 11, 2021, https://www.reuters.com/world/china/blinken-warns-chinas-increasingly-aggressive-actions-against-taiwan-2021-04-11/.

[73] It is notable that, despite the US-ROK alliance, senior ROK officials have stated they have not been asked to choose between the United States and China. "FM Chung: US, China Not Objects of Choice for S. Korea," KBS World, March 31, 2021, http://world.kbs.co.kr/service/news_view.htm?lang=e&Seq_Code=160518. While in the event of a conflict it may well be that the ROK supports the United States, prior commitments may be hard to obtain.

these countries in the event of a conflict.[74] Third, for both security and values reasons, Japan and Australia should each be part of any military response with the particulars subject to military analysis and political oversight (and though the ROK might need to hold its forces generally in reserve because of the threat from North Korea). It is worth noting that any move by the PRC to take Taiwan by force would potentially include striking US forces and facilities in the region including those in Japan and Australia (and perhaps the ROK), and that would, of course, mean an attack that would engage the mutual defense treaties.[75] Finally and concomitantly, the United States would want to assure each of Japan, Australia, and the ROK of the certainty of the US extended nuclear deterrence guarantee. Moreover, since China is likely to take economic coercive actions in response to such commitments by Japan, Australia, and the ROK, the United States should develop in advance with these countries offsetting economic actions should that be required.

Similarly, European nations and Canada individually and through both the European Union (EU) and NATO need to commit to support the United States in the event of a conflict with China. As with Japan, Australia, and the ROK, it needs to be made clear that trade and other economic interactions with China could not continue if such a conflict were to arise. Europe and Canada, through NATO or individually, could also provide some military support including naval and cyber capabilities. Their willingness to undertake such commitments should derive from multiple factors. These include support to democracy; support for deterrence in the Indo-Pacific; and recognition that China is increasingly a security threat to Europe and Canada, a threat that would only increase if China were successful in an attack against Taiwan (or against any US ally in the Indo-Pacific). A multilateral commitment to deterrence—including trade, economic, and military components—would substantially enhance deterrence in the Indo-Pacific.

2) Multinational Forces for Deterrence and Maritime Support

As discussed above, if conflict with China did occur, it would engage the interests of more than one ally, and a combined response by multiple forces would be called for. While it is not possible to predict such events, establishing several multilateral combined efforts could help enhance deterrence. The United States, Australia, and Japan have already been exercising regularly together as with the Cope North 2021[76] event in Guam and the Malabar exercise (which included India) in October 2020.[77] The United States, of course, has also long had extensive bilateral cooperation with each of Japan and Australia as treaty allies, and that cooperation has increased as a result of malign Chinese activities affecting each country. Moreover, Japan and Australia have agreed in principle to a Reciprocal Access Agreement (a basing treaty akin to a Status of Forces Agreement), which awaits approval by both nations' legislative bodies. That will be a valuable step toward a framework that will enable reciprocal defense between the two nations and is a step toward a combined defense strategy for the region.[78]

Accordingly, a valuable next set of actions would be for the three countries to establish a combined naval task force, a combined air operations center, and a combined multi-domain command and control system. Once established, these arrangements would provide for more coordinated execution of trilateral operations in the maritime and air domains, enhance the interoperability among nations on a continuous basis, and provide the opportunity to develop further multilateral security arrangements as part of the broader Indo-Pacific deterrence effort. Other allies, including the Republic of Korea as well as France and the United Kingdom (the latter two being regularly active in the Indo-Pacific), could be encouraged to join especially since, as they are allies of the United States, they already participate in combined activities.

[74] One of the challenges that the United States would face in the event of an Indo-Pacific conflict is the logistical requirement to have sufficient stocks of weapons and supporting materiel promptly available in theater. Prepositioning adequate stocks in advance could have an important impact on the course of a conflict. For example, planning for an influx of Air Force capabilities would be easier if stocks of munitions and other support requirements were already in place.

[75] The Japan-US Security Treaty provides "Each Party recognizes that an armed attack against either Party in the territories under the administration of Japan would be dangerous to its own peace and safety . . ." *Treaty of Mutual Cooperation and Security between Japan and the United States of America*, Article V, via Ministry of Foreign Affairs of Japan, https://www.mofa.go.jp/region/n-america/us/q&a/ref/1.html. The ROK-US Mutual Defense Treaty provides, "Each Party recognizes that an armed attack in the Pacific area on either of the Parties in territories now under their respective administrative control, or hereafter recognized by one of the Parties as lawfully brought under the administrative control of the other, would be dangerous to its own peace and safety." *Mutual Defense Treaty between the United States and the Republic of Korea*, Article III, via Yale Law School Lillian Goldman Law Library, https://avalon.law.yale.edu/20th_century/kor001.asp. The United States and Australia are signatories to the 1951 ANZUS Treaty which provides, "Each Party recognizes that an armed attack in the Pacific Area on any of the Parties would be dangerous to its own peace and safety and declares that it would act to meet the common danger in accordance with its constitutional processes." *Security Treaty between the United States, Australia, and New Zealand*, via Yale Law School Lillian Goldman Law Library, September 1, 1951, https://avalon.law.yale.edu/20th_century/usmu002.asp.

[76] ANI, "US Conducts Military Exercise with Australia, Japan on Guam," Big News Network, February 8, 2021, https://www.bignewsnetwork.com/news/267774090/us-conducts-military-exercise-with-australia-japan-on-guam.

[77] Megan Eckstein, "Australia to Join US, India, Japan for Malabar 2020 in High-End Naval Exercise of 'the Quad,'" *USNI News*, October 20, 2020, https://news.usni.org/2020/10/20/australia-to-join-u-s-india-japan-for-malabar-2020-in-high-end-naval-exercise-of-the-quad.

[78] Euan Graham and Yuka Koshino, "Australia and Japan Inch Closer towards Landmark Defence Agreement," International Institute for Strategic Studies, December 17, 2020, https://www.iiss.org/blogs/analysis/2020/12/australia-japan-landmark-defence-agreement.

> "The Quad nations should establish a combined joint task force (CJTF) composed of both naval and coast guard elements and focused on maritime support including freedom of navigation, counter-piracy, support to fishing rights, search and rescue, humanitarian and disaster relief, and building a common maritime picture."

A second multinational effort would be to build on the ongoing military engagements among the Quadrilateral Security Dialogue (Quad) nations of Australia, India, Japan, and the United States. The Quad nations should establish a combined joint task force (CJTF) composed of both naval and coast guard elements and focused on maritime support including freedom of navigation, counter-piracy, support to fishing rights, search and rescue, humanitarian and disaster relief, and building a common maritime picture. Participation in CJTF activities would be voluntary and include maritime activities in both the Indian and Pacific Oceans. To ensure that the CJTF would work toward developing effective interoperability, command of the CJTF could be assigned on a rotational basis, allowing member nations to take turns at the helm, not just during the artificial environments of exercises, but during routine and crisis operations.[79]

The CJTF would be designed so that other nations could join as their capabilities in (and deployments to) the region allowed with inclusion of coast guards increasing opportunities for partner nations to contribute. Such a format could include Association of Southeast Asian Nations countries with significant maritime interests including Indonesia, Malaysia, Philippines, and Vietnam, and could also capitalize on planned French, UK, and German cruises to the Indo-Pacific.[80] CJTF operations could also be coordinated with the robust exercise schedule that currently exists in the region. Participation by the CJTF could include such events as Talisman Sabre (the US/Australian bilateral exercise that will again include Japan in 2021)[81] and Malabar (the Indian-hosted exercise that included the entire Quad in 2020)[82] and could be expanded to include other events such as the Indonesian-hosted Komodo[83] or an Indo-Pacific version of the Arabian Sea Warfare exercise which included the United States, Belgium, France, and Japan.[84]

Such a Combined Joint Task Force could also be used to support freedom of navigation through patrolling in contested regions as the United States routinely does, but in a bilateral or multilateral manner as was demonstrated in April 2019 when a French frigate passed through the Taiwan Strait following a transit by US ships the month prior.[85] The United States and India have different views regarding military operations in a country's exclusive economic zone, and there would be great value in generating a practical common approach.[86] Similarly, CJTF operations could be undertaken at the request of a host country in protection of its fishing or seabed rights in its exclusive economic zone. The United States and Australia recently undertook patrolling efforts in support of Malaysia undersea exploration, and future such multinational support might similarly be important to a number of nations.[87]

[79] The United States and France have already demonstrated the possibilities of such cooperative actions, for example, through the leadership of the French over CTF-50 during a strike operation against the Islamic State of Iraq and al-Sham in 2015. Michael R. Gordon, "French Ship Commands Naval Task Force in Strikes against ISIS," *New York Times*, December 20, 2015, https://www.nytimes.com/2015/12/21/world/europe/french-ship-is-in-lead-in-strikes-against-isis.html.

[80] Ralph Jennings, "Western Countries Send Ships to South China Sea in Pushback against Beijing," VOA News, February 22, 2021, https://www.voanews.com/east-asia-pacific/voa-news-china/western-countries-send-ships-south-china-sea-pushback-against; Shogo Akagawa, "Germany to Send Naval Frigate to Japan with Eye on China," Nikkei Asia, January 25, 2021, https://asia.nikkei.com/Politics/International-relations/Indo-Pacific/Germany-to-send-naval-frigate-to-Japan-with-eye-on-China.

[81] Seth Robson, "US, Australia Plan to Carry On with Massive Talisman Sabre Exercise Despite Pandemic," *Stars and Stripes*, January 28, 2021, https://www.stripes.com/news/pacific/us-australia-plan-to-carry-on-with-massive-talisman-sabre-exercise-despite-pandemic-1.660096.

[82] Eckstein, "Australia to Join US, India, Japan for Malabar 2020 in High-End Naval Exercise of 'the Quad.'"

[83] Prashanth Parameswaran, "Exercise Komodo 2018 Puts Indonesian Navy in the Spotlight," *The Diplomat*, May 1, 2018, https://thediplomat.com/2018/05/exercise-komodo-2018-puts-indonesia-navy-in-the-spotlight/.

[84] "US, Belgium, France, Japan Hold Mideast Naval Exercise," Associated Press via ABC News, March 2, 2021, https://abcnews.go.com/International/wireStory/us-belgium-france-japan-hold-mideast-naval-exercise-76587879.

[85] Idrees Ali and Phil Stewart, "In Rare Move, French Warship Passes through Taiwan Strait," Reuters, April 24, 2019, https://www.reuters.com/article/us-taiwan-france-warship-exclusive/exclusive-in-rare-move-french-warship-passes-through-taiwan-strait-idUSKCN1S027E.

[86] Jeff M. Smith, "America and India Need a Little Flexibility at Sea," *Foreign Policy*, April 15, 2021, https://foreignpolicy.com/2021/04/15/us-india-fonop-maritime-law/.

[87] Ben Werner, "Maritime Standoff between China and Malaysia Winding Down," *USNI News*, May 13, 2020, https://news.usni.org/2020/05/13/maritime-standoff-between-china-and-malaysia-winding-down.

A CJTF might be useful as a means of responding to China's use of its fishing fleet to expand its illegal claims in the South China Sea. As one example, some 220 Chinese fishing vessels supported by ships from the People's Armed Forces Maritime Militia were anchored in the Whitsun (also called Julian Felipe) reef area,[88] in direct provocation of the Philippine government and in defiance of the 2016 United Nations Convention on the Law of the Sea ruling declaring Chinese claims to the region unfounded.[89] In such a case, a standing CJTF might accompany Philippine Coast Guard vessels to provide support during law enforcement operations to impound illegally obtained fish or take other measures authorized for the security of an exclusive economic zone—and its multilateral nature might add to its credibility and make it easier for affected nations to take such support.

3) Establishment of Cybersecurity and Supply Chain Resilience with Allies

Cybersecurity and supply chain issues are of as significant concern in the Indo-Pacific theater as they are in the American theater. Critical infrastructures necessary to mission assurance are highly vulnerable to cyberattack in allied and partner countries. Failure to resolve these issues will undercut the warfighting capabilities of US and allied forces—and, consequently, their deterrent effect.

A useful example of the deficiencies in the Indo-Pacific cybersecurity situation is the status of cybersecurity for Japan. In the military, the Japanese Self-Defense Forces Cyber Defense Group is currently being expanded but only to a still small number of approximately one thousand personnel (compared with one estimate of North Korean cyber forces of approximately 6,800).[90] More broadly, as one recent report states:

> Japan's primary cyber capability, the Cabinet Secretariat's National Center of Incident Readiness and Strategy for Cybersecurity, or NISC, has mostly failed at keeping Japan cyber secure. One reason for this is that the centre was designed only to improve the cybersecurity of government agencies. This overly narrow focus not only fails to protect citizens from cybercrime, but also leaves gaping vulnerabilities for the government itself. Government agencies can be targeted through non-government angles. Supply chains, subcontracting and collaboration between private and government sectors all lie beyond the scope of the NISC.[91]

Other Indo-Pacific allies and close partners face challenges broadly comparable to those faced by Japan. While the priorities described by Admiral Davidson and the Pacific Deterrence Initiative will enhance kinetic capabilities and are necessary to achieving stability for the region, their value will be significantly undercut without comparable changes for cyber and supply chain security. A coordinated strategy for cybersecurity and supply chain resilience could make a significant difference.

First, the Defense Department should put cybersecurity for its key Indo-Pacific allies at the top of its priority list for the region. As discussed above, the greatest defense deficiency currently facing the United States is the ability of capable adversaries such as China and Russia to penetrate information and communications technology systems, including operational technologies utilized to run electric grids, pipelines, and other critical infrastructures. This vulnerability applies equally to systems in allied countries. As a consequence, the need for cybersecurity resilient architectures and an effective operational interaction between the private sector and the government, including the military, is critical. A program should be developed to remedy such deficiencies:

—As an initial step, the United States should seek to establish separate high-level, technologically capable task forces with each of Japan, the Republic of Korea, and Taiwan with mandates to generate effective solutions to ensure cybersecurity resilience. Such task forces would need the authority to engage with non-defense governmental agencies as well as with the private sector.[92]

—The United States could, with the agreement of the relevant Indo-Pacific host, engage key allies with significant cyber capabilities including Australia, Canada,

[88] Gabrielle Reyes, "Philippine Fighter Jets Flying Daily over Reef Occupied by Hundreds of Chinese Ships," Breitbart, March 30, 2021, https://www.breitbart.com/asia/2021/03/30/philippine-fighter-jets-flying-daily-reef-occupied-hundreds-chinese-ships/.

[89] Andrew S. Erickson and Ryan D.Martinson, "Records Expose China's Maritime Militia at Whitsun Reef," *Foreign Policy*, March 29, 2021, https://foreignpolicy.com/2021/03/29/china-militia-maritime-philippines-whitsunreef/.

[90] Samuel Arnold-Parra, "A Neglected Frontier: Challenges to Japan's Cyber Security," Global Risk Insights, January 23, 2021, https://globalriskinsights.com/2021/01/a-neglected-frontier-challenges-to-japans-cyber-security/.

[91] Hiroki Hunter, "Suga's Focus on Cybersecurity Underscores Importance of Alliances and Reform for Japan," *The Strategist*, Australian Strategic Policy Institute, March 5, 2021, https://www.aspistrategist.org.au/sugas-focus-on-cybersecurity-underscores-importance-of-alliances-and-reform-for-japan/.

[92] The United States does have an ongoing cyber dialogue with Japan—and the two countries are "strengthening bilateral cybersecurity and information security" according to the recent joint statement after the Biden-Suga meeting. White House, "U.S.- Japan Joint Leaders' Statement: 'U.S. – Japan Global Partnership for a New Era,'" April 16, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/16/u-s-japan-joint-leaders-statement-u-s-japan-global-partnership-for-a-new-era/. The proposed recommendation is consistent with the joint statement but more specific, proposing a specific effort directed to establishing the actual capabilities and procedures required for cybersecurity resilience.

France, and the United Kingdom to help support such task forces.

—The objective of the task forces would be, as described in the sections above on cybersecurity, to create pilot programs for the establishment of cybersecurity resilient architectures; to organize effective operational coordination between the government and the key critical infrastructures of each country; and to organize active defense of such key critical infrastructures as a combined effort between the government and the private sector.

—The task forces should have relatively stringent deadlines and report to the "2+2" foreign and defense ministers' meetings that Japan and the ROK each separately have with the United States. A comparable mechanism would be needed to be established with Taiwan.

> "Emerging technologies and naval mining capabilities should play key roles in creating a more desirable military balance in the Indo-Pacific."

Second, in parallel to the cybersecurity effort, supply chain task forces should similarly be established with each of Japan, the Republic of Korea, and Taiwan. The United States' "100-Day" review mandated by the supply chain executive order described above includes semiconductors, high-capacity batteries, and strategic minerals—and each of these is relevant to defense.[93] The one-year review includes the defense industrial base, the information and communications technology sector, and the energy and transportation sectors—again all relevant to defense. Objectives for the proposed supply chain task forces would be similar to those for the United States' supply chain review including, most importantly, exclusion of China from strategic industries, barring Chinese software in key critical industries, and ensuring that China does not have a dominant position in the material supply chain of such industries. The reporting mechanisms and the deadlines for the task forces could be comparable to those for the cybersecurity reviews. As recommended above for cybersecurity, key allies including Australia, Canada, France, and the United Kingdom could be included in such task forces with the consent of the hosts.

4) Emerging Technologies and Naval Mining Capabilities

Emerging technologies and naval mining capabilities should play key roles in creating a more desirable military balance in the Indo-Pacific. Properly utilized, they can change the nature of operational strategies and tactical engagements for the region.

a) Unmanned Vehicles: In the next ten years, development and deployment of multiple types of unmanned vehicles could significantly enhance the military balance as well as beneficially affect resource requirements. Not only do unmanned vehicles have the potential to perform many of the current missions of manned systems, but they are potentially producible at scale and low cost, making them expendable in a way that manned systems are not ("attritable" to use DOD language). Especially in light of potentially constrained budgets, as well as the importance of generating advantage in the battlespace, accelerating the development and deployment of unmanned vehicles is a high-priority requirement. In the Indo-Pacific, both the Navy and Air Force would benefit from extensive use of unmanned vehicles.

Navy investment in unmanned vehicles is necessary to change both the capacity and capabilities of the fleet—which is facing a potential Chinese naval presence (including the China Coast Guard) of some 650-700 ships.[94] Acquisition of unmanned vehicles would allow the Navy to expand to provide the numbers necessary to meet future deterrence and warfighting requirements.[95] As much as it is a cliché, "quantity does have a quality all of its own." According to former Secretary of Defense Mark Esper, the Navy's planned outlay for unmanned systems is between 140 and 240, making them a major portion of

[93] White House, *Executive Order on America's Supply Chains*, February 24, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/, Section 3(a)(i),(ii),(iii).

[94] Ronald O'Rourke, *China Naval Modernization: Implications for U.S. Navy Capabilities—Background and Issues for Congress,* Congressional Research Service, updated March 9, 2021, https://fas.org/sgp/crs/row/RL33153.pdf, tables at 30-32.

[95] Assuming the availability of Japan's and Australia's naval forces to add approximately 150 (including auxiliaries) and fifty ships, respectively. "2021 Japan Military Strength," Global Fire Power, accessed April 22, 2021, https://www.globalfirepower.com/country-military-strength-detail.php?country_id=japan#:~:text=For%202021%2C%20Japan%20is%20ranked,on%2003%2F03%2F2021; Royal Australian Navy website, accessed April 22, 2021, https://www.navy.gov.au/fleet/ships-boats-craft/current-ships.

an expanded Navy envisioned as a counterweight to the Chinese navy.[96]

Unmanned naval vehicles' mission roles can include intelligence, surveillance, and reconnaissance; electronic warfare and strike; anti-submarine and anti-surface warfare; naval mining and mine countermeasures; and multiple logistics activities.[97] The Navy's current unmanned surface and underwater vehicles include three basic types: Large Unmanned Surface Vehicles, Medium Unmanned Surface Vehicles (MUSVs), and Extra-Large Unmanned Undersea Vehicles (XLUUVs). Several systems have already seen significant development including the *Sea Hunter* MUSV for anti-submarine warfare, counter-mine, and strike missions and the *Orca* XLUUV for multiple missions including anti-surface and anti-submarine warfare, mine countermeasures, and electronic and strike missions.[98] Without trying to define exact numbers for these and other unmanned naval systems, the fundamental point is that significant expansion of the fleet and its capabilities through the use of unmanned vehicles is both necessary and achievable.

The Air Force is taking comparable steps to develop autonomous and semi-autonomous drones that can perform a variety of missions[99] to support combat operations including contesting China's anti-access/area denial capabilities.[100] The potential for this technology to alter the balance of power is evident in the results of AlphaDogfight demonstrations by the Defense Advanced Research Projects Agency (DARPA) in which DARPA used a simulated dogfight environment to test the artificial intelligence (AI) algorithms against an actual F-16 pilot, resulting in victory in five consecutive simulations of the AI algorithm over the human pilot.[101] The Air Force has now awarded contracts for unmanned aerial combat vehicle prototypes[102] that will incorporate artificial intelligence and human machine teaming, be highly maneuverable and stealthy, and work in concert with fifth-generation platforms like the F-22 and F-35[103] to provide collaborative attack and swarming capabilities.[104] Similarly, AI and "small, inexpensive, unmanned aerial vehicles (UAVs) [can] perform a variety of functions, including intelligence, surveillance and reconnaissance (ISR); position, navigation, and timing (PNT); communications; and strike."[105] One such potential approach is to establish a "targeting mesh" through the employment of

> small, lightweight, and inexpensive sensors capable of detecting and observing targets over a very limited area, [but where] the aggregate capability of hundreds of small UAVs can cover a large area with considerable redundancy, meaning that any point within the area covered by the mesh can be observed simultaneously by multiple independent platforms.[106]

[96] Megan Eckstein, "SECDEF Esper Calls for 500-Ship Fleet by 2045, with 3 SSNs a Year and Light Carriers Supplementing CVNs," *USNI News*, October 6, 2020, https://news.usni.org/2020/10/06/secdef-esper-calls-for-500-ship-fleet-by-2045-with-3-ssns-a-year-and-light-carriers-supplementing-cvns#:~:text=Esper's%20Battle%20Force%202045%2C%20which,a%20resource%2Dconstrained%20budget%20environment.

[97] The Department of the Navy Unmanned Campaign Framework demonstrates the wide variety of missions that unmanned systems are already being used for and maps the development of potential applications of emerging technology. Based upon the description of explicit capabilities that have already been demonstrated and the modular payload design concepts being employed, it is clear that the US Navy and Marine Corps intend to fully integrate unmanned naval systems across all warfighting functions. US Department of the Navy, *Department of the Navy Unmanned Campaign Plan*, March 16, 2021, https://www.navy.mil/Portals/1/Strategic/20210315%20Unmanned%20Campaign_Final_LowRes.pdf.

[98] The first *Sea Hunter* is assigned into Surface Development Squadron 1 with a second one planned during 2021. Megan Eckstein, "Sea Hunter USV Will Operate with Carrier Strike Group, as SURFDEVRON Plans Hefty Testing Schedule," *USNI News*, January 21, 2020, https://news.usni.org/2020/01/21/sea-hunter-usv-will-operate-with-carrier-strike-group-as-surfdevron-plans-hefty-testing-schedule. The Navy plans to procure two *Orcas* per year beginning in FY2023 based off the Boeing *Echo Voyager* design. Ronald O'Rourke, *Navy Large Unmanned Surface and Undersea Vehicles: Background and Issues for Congress,* Congressional Research Service, December 23, 2020, https://crsreports.congress.gov/product/pdf/R/R45757, 18.

[99] Tracy Cozzens, "Boeing Loyal Wingman Uncrewed Aircraft Completes First Flight," *GPS World*, March 7, 2021, https://www.gpsworld.com/boeing-loyal-wingman-uncrewed-aircraft-completes-first-flight/; Joseph Trevithick, Thomas Newdick, and Tyler Rogoway, "Stealthy XQ-58 Drone Busts the Networking Logjam between F-22 and F-35," *The Drive*, December 15, 2020, https://www.thedrive.com/the-war-zone/38168/stealthy-xq-58-drone-busts-the-networking-logjam-between-f-22-and-f-35;
"Skyborg," Air Force Research Lab, accessed May 21, 2021, https://afresearchlab.com/technology/vanguards/successstories/skyborg.

[100] Mark Gunzinger, Carl Rehberg, and Lukas Autenried, *Five Priorities for the Air Force's Future Combat Air Force,* Center for Strategic and Budgetary Assessments, 2020, https://csbaonline.org/uploads/documents/Five_Priorities_For_The_Air_Forces_Future_Combat_Air_Force_Web.pdf, 46.

[101] Oriana Pawlyk, "Rise of the Machines: AI Algorith Beats F-16 in Dogfight," *Military News*, August 24, 2020, https://www.military.com/daily-news/2020/08/24/f-16-pilot-just-lost-algorithm-dogfight.html#:~:text=An%20artificial%20intelligence%20algorithm%20this,simulated%20dogfight%2C%20DARPA%20officials%20revealed.&text=Then%2C%20Heron's%20system%20on%20the,organization%20said%20following%20the%20finals.

[102] Boeing, General Atomics, and Kratos have each received contracts to deliver prototypes for the Skyborg program. The project will produce low-cost attritable drones that can operate in contested airspace and conduct combat missions too dangerous for human pilots. Unlike previous programs, Skyborg is using artificial intelligence to facilitate autonomous operations and learning. Deliveries are anticipated for initial flight testing no later than May 2021. Valerie Insinna, "These 3 Companies Will Build Prototypes for the Air Force's Skyborg Drone," *Defense News,* December 7, 2020, https://www.defensenews.com/air/2020/12/07/these-three-companies-will-build-prototypes-for-the-air-forces-skyborg-drone/.

[103] In the Skyborg/Valkyrie program, the Kratos XQ-58A Valkyrie and the Boeing Loyal Wingman have shown significant progress in intraflight communications and semi-autonomous flight operations. Cozzens, "Boeing Loyal Wingman Uncrewed Aircraft Completes First Flight"; Trevithick, Newdick, and Rogoway, "Stealthy XQ-58 Drone Busts the Networking Logjam between F-22 and F-35."

[104] Gunzinger, Rehberg, and Autenried, *Five Priorities for the Air Force's Future Combat Air Force*, 46.

[105] Thomas Hamilton and David Ochmanek, *Operating Low-Cost, Reusable Unmanned Aerial Vehicles in Contested Environments,* RAND, 2020, https://www.rand.org/pubs/research_reports/RR4407.html, viii.

[106] Ibid., 3.

b) Offensive Cyber and Directed Energy Weapons: Offensive cyber and directed energy weapons can be key elements for generating advantage in the Indo-Pacific military balance. With proper preparation, offensive cyber capabilities can provide prompt "electronic mass" against critical targets.[107] Cyber could be a powerful tool, for example, in retarding the operations at Chinese ports and on rail lines to stymie People's Liberation Army logistics and sequencing of forces that would be necessary for an invasion of Taiwan. Similarly, an effective capability to deny and degrade China's ability to operate in space will be critical in shaping the strategic environment. The capacity for doing so with directed energy weapons was highlighted by the recent French AsterX exercise (in which US Space Force participated), which demonstrated that lasers could be used to destroy or damage adversary satellites.[108]

Directed energy weapons, including laser, high-power microwave, and radio frequency weapons systems, may also be able to be employed as defensive systems[109] including against ballistic and hypersonic missiles, manned aircraft, unmanned aerial vehicles, and artillery.[110] For example, high-power microwave and radio frequency weapons systems have shown potential as defensive systems to counter hypersonic cruise missiles and drone swarms.[111] Other systems under development by the Navy and the Air Force[112] are potentially capable of attacking adversary electronics communications and computer networks,[113] while still others[114] may provide short-range defense of bases.[115] As these technologies are further developed, they could also provide means to disrupt adversary command and control networks, thereby providing significant advantage for US forces on both offense and defense.

c) Hypersonic Missiles: Admiral Davidson has identified requirements for "increased quantities of ground-based missiles and improved air and long-range naval fires capable of ranges over 500 km [kilometers]," and a joint fires network.[116] Long-range fires are obviously an important component of warfighting. As the vice chairman of the Joint Chiefs of Staff has stated, "if someone shows up to the battle and they don't have long-range fires and the adversary does, you can't effectively operate in that theatre."[117] Long-range fires can be delivered by conventional artillery and missiles, but hypersonic weapons, which travel at speeds in excess of Mach 5, could also be an important element in meeting the long-range fires requirement for fires beyond a 500 km range. There are three variations

[107] Both the Israeli use of offensive cyber techniques to defeat the Syrian air defense network in 2007 and the Russian distributed denial of service attack on Estonia of the same year stand as examples of how cyber "fires" can manifest in mass across a broad network, be it command and control for air defense or commercial communications networks. The 2008 invasion of Georgia by the Russians featured similar denial of service features that limited the ability of the Georgians to conduct command and control for their forces and cut off information flow from outside news sources while simultaneously forcing Georgian government networks to shift to servers outside of the country. Major Angel Torres, "Offensive Cyber Fires, a Case for MAGTF Integration," Marine Corps University, US Marine Corps, March 28, 2012, https://apps.dtic.mil/sti/pdfs/ADA601532.pdf, 7-9. Similar methods were employed in Crimea in 2014. Ongoing offensive cyber operations by the Russians in Ukraine highlight the potential to use cyber to have an outsized effect using non-kinetic means to render infrastructure ineffectual in the midst of a broader kinetic campaign. Laurens Cerlus, "How Ukraine Became a Test Bed for Cyberweaponry," *Politico*, February 14, 2019, https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/.

[108] Anthony Cuthbertson, "France Conducts First Ever Military Exercise in Space," *Independent*, March 11, 2021, https://www.independent.co.uk/life-style/gadgets-and-tech/space/france-space-military-b1815718.html.

[109] Henry Obering III, "Directed Energy Weapons Are Real…and Disruptive," *Prism*, vol. 8, no. 3 (2019): 40-41, https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3.pdf.

[110] As suggested by the success of the Airborne Laser to destroy missiles in testing in 2010 and subsequent performance of other similar systems such as the Navy's LaWS and HELIOS systems, the Army's Stryker-based Mobile Expeditionary High Energy Laser demonstrator, and the Air Force's Self-Protect High Energy Laser Demonstrator. Rachel S. Cohen, "Some Directed-Energy Weapons Show Promise while Others Slow," *Air Force Magazine*, July 7, 2020, https://www.airforcemag.com/some-directed-energy-weapons-show-promise-while-others-slow/.

[111] The Air Force demonstrated in 2019 the capability of both mobile high-powered microwave and high-energy lasers against drone swarms at a test in White Sands, New Mexico, downing dozens of drones in a capability demonstration. These systems are designed to be employed by operators while mounted on small all-terrain vehicles such as the Polaris MRZR. Oriana Pawlyk, "Raytheon Directed-Energy Weapons Down Drones in Air Force Demonstration," Military.com, May 1, 2019, https://www.military.com/daily-news/2019/05/01/raytheon-directed-energy-weapons-down-drones-air-force-demonstration.html. The Missile Defense Agency has developed a very high-power laser capable of eventual deployment on a space-based platform. This type of application would allow effective targeting of missiles during the boost, ascent, and midcourse phases. The anticipated range of the weapon is in the hundreds of miles. Obering III, "Directed Energy Weapons Are Real…and Disruptive," 40-41; Cohen, "Some Directed-Energy Weapons Show Promise while Others Slow."

[112] Such as the AFRL's Counter electronics High Powered Microwave Advanced Missile Project (CHAMP) and its follow on High-power Joint Electromagnets Non-kinetic Strike (HiJENKS). Details on CHAMP are covered in J.R. Wilson, "The New Era of High-Power Electromagnetic Weapons," Military & Aerospace Electronics, November 19, 2019, https://www.militaryaerospace.com/power/article/14072339/emp-high-power-electromagnetic-weapons-railguns-microwaves, 5. Discussion of HiJENKS can be found in Sydney J. Freedberg Jr., "'A Golden Age for Collaboration' on Lasers and Microwaves: But Watch the Cheetos!" *Breaking Defense*, July 7, 2020, https://breakingdefense.com/2020/07/a-golden-age-for-collaboration-on-lasers-microwaves-but-watch-the-cheetos/.

[113] Obering III, "Directed Energy Weapons Are Real…and Disruptive," 40-41; Jack McGonegal, *High Power Microwave Weapons: Disruptive Technology for the Future*, Air Command and Staff College, May 2020, https://apps.dtic.mil/sti/pdfs/AD1107488.pdf.

[114] Such as the Tactical High Power Operational Responder built by the Air Force with BAE Systems, Verus Research, and Leidos.

[115] Cohen, "Some Directed-Energy Weapons Show Promise while Others Slow."

[116] US Senate, "Statement of Admiral Philip S. Davidson."

[117] Patrick Tucker, "US Army's Not Stupid for Wanting Long-Range Fires — but More Analysis Needed, Hyten Says," *Defense One*, April 6, 2021, https://www.defenseone.com/technology/2021/04/us-armys-not-stupid-wanting-long-range-fires-more-analysis-needed-hyten-says/173181/.

of hypersonic weapons—"boost-glide," "airbreathing," and "gun-launched"[118]—and the DOD is developing multiple variations of each. The Army and Navy are working in conjunction to develop a common hypersonic glide body, which would serve both as a ground- and submarine-launched system, and the Air Force began flight testing the AGM-183A Air-launched Rapid Response Weapon during 2019 and will complete testing by 2022.[119] The key, of course, is to be able to move from development to actual programs of record and then to full operational capability.

d) Naval Mining Capability: Naval mine warfare can play an important role in the Indo-Pacific.[120] In both the surface and subsurface domains, sea mining offers a low-cost option for shaping the environment. Effective operational planning should account for the use of both mine laying and mine clearing technologies to control the sea lines of communication. The United States should work particularly closely with Japan and Taiwan in enhancing naval mining capabilities. Naval mines could, for example, be an important factor in defeating a Chinese invasion force against Taiwan.

Currently, however, the United States is not adequately postured to conduct the extensive mine operations that would be required in a conflict. As described by Admiral James Winnefeld and Captain Syed Ahmad in 2018, "the nation currently employs only two maritime mines[121] . . . [b] oth use 20th-century technology and are useful only in shallow water directly underneath a target vessel."[122]

Emerging UUV technology does, however, offer potential for a cost-effective and robust offensive mine warfare capability. Soon, Navy submarines could be equipped to launch, recover, and conduct command and control for a series of "mother-and-child" autonomous UUVs. Mothership UUVs could be deployed to critical chokepoints to loiter and then subsequently launch multiple smaller "child" UUVs armed to disable or destroy targets. These systems could effectively augment existing submarine strike capabilities by combining capabilities from both fast-attack submarines and sea mines—including stealth; mobility and sensor-informed pursuit and targeting; affordability; and the presentation of physical and psychological barriers to the adversary.[123]

Similarly, US preparation for mine countermeasures (MCM) is also needed as the "ability to counter sea mines is as equally important as effectively employing them."[124] The United States could expect that China, which has approximately one hundred thousand naval mines, will use them as part of its anti-access/area denial capabilities.[125] As with offensive mining operations, MCM is an area that has been neglected by the US Navy relative to other capability sets and presents a significant vulnerability.[126]

Fleet investments should leverage the emerging technologies of the autonomous systems discussed above to both reduce cost and provide scale to cope with the likely number and variety of adversary sea mines. This should be done on an expedited basis as the Navy's eleven Avenger class mine countermeasure ships and thirty-one MG-53E helicopters are all slated for retirement by 2025. Proposed replacements have insufficient capacity and uncertain capability. The Navy has acquired thirty-one AQS-24C towed mine hunting systems and is developing the AQS-20 and the Barracuda mine neutralizer for use in the Littoral Combat Ship (LSC) MCM module.[127] However, the LCS program has been plagued with issues, and, even if

[118] John T. Watts, Christian Trotti, and Mark J. Massa, *Primer on Hypersonic Weapons in the Indo-Pacific Region*, Atlantic Council, August 2020, https://www.atlanticcouncil.org/wp-content/uploads/2020/08/Hypersonics-Weapons-Primer-Report.pdf, 4.

[119] Kelley M. Sayler, *Hypersonic Weapons: Background and Issues for Congress*, Congressional Research Service, December 1, 2020, https://fas.org/sgp/crs/weapons/R45811.pdf, 6.

[120] Australia's "2020 Force Structure Plan" identified undersea mines as a method of protecting Australia's sovereignty while Japan is developing technology to leverage unmanned, automated loitering undersea weapons for deployment to high-risk areas. Tate Nurkin, *The Five Revolutions: Examining Defense Innovation in the Indo-Pacific Region*, Atlantic Council, November 2020, https://www.atlanticcouncil.org/in-depth-research-reports/report/the-five-revolutions-examining-defense-innovation-in-the-indo-pacific-region/, 21.

[121] The Quickstrike family, which converts different sizes of air-launched general-purpose bombs into mines by attaching a simple target-detection device, and the submarine-launched mobile mine.

[122] Admiral James Winnefeld Jr., US Navy (Ret.), and Captain Syed Ahmad, Judge Advocate General Corps, US Navy (Ret.), *The Other Mine Warfare Will Work,* USNI Proceedings, July 2018, https://www.usni.org/magazines/proceedings/2018/july/other-mine-warfare-will-work.

[123] Commander Erich Frandrup, US Navy, *Embracing Underseas Robots: A US Strategy to Maintain Undersea Superiority in an Age of Unmanned Systems,* Atlantic Council, October 2020, https://www.atlanticcouncil.org/in-depth-research-reports/report/embracing-underseas-robots/, 5. While there is less development in the field of UAVs for use in offensive mine warfare, with appropriate resource support aerial drone technology (such as the current US Navy MQ-25 Stingray platform) could be adapted to provide for delivery of mines. Christopher R. Desanto, Jenna L. Drummond, Russell A. Helger Jr., Ryan P. Mcdonough, and David Perry, *Operational Analysis for Offensive Mine Warfare*, Calhoun Institutional Archive of the Naval Post Graduate School, June 2020, https://calhoun.nps.edu/bitstream/handle/10945/65501/20Jun_Desanto_et_al_Needs_Supplemental.pdf?sequence=1&isAllowed=y, 8.

[124] Frandrup, *Embracing Underseas Robots*, 8.

[125] Rob Wittman, "The US Navy's Modernization Rush Must Not Harm Mine Countermeasures," *Defense News*, May 8, 2020, https://www.defensenews.com/opinion/commentary/2020/05/08/the-us-navys-modernization-rush-must-not-harm-mine-countermeasures/.

[126] Yasmin Tadjdeh, "Navy Invests in New Mine Warfare Technology (Updated)," *National Defense Magazine*, April 6, 2020, https://www.nationaldefensemagazine.org/articles/2020/4/6/navy-invests-in-new-mine-warfare-technology.

[127] Tadjdeh, "Navy Invests in New Mine Warfare Technology (Updated)."

fully implemented, few consider the LCS/MCM module a fully adequate solution for the extensive mine countermeasure requirements of operations in likely scenarios.[128]

B. Europe

Balancing capabilities for the European theater with those required for the Indo-Pacific is a critical task—vital interests of the United States are at stake in each theater. Europe has enormous importance to the United States from values, economic, and security standpoints. Europe has the most democracies, the highest amount of trade and foreign investment with the United States, and in NATO, the most consequential security alliance. Diplomatically and militarily, the nations within the European community are at the core of the rules-based order. Europe faces a significant security threat from Russia, including nuclear, conventional, and hybrid. Europe is also threatened by a growing hybrid challenge from China including cyber espionage and supply chain dependencies.

> "the United States should . . . work with Europe and Canada to increase their defense capabilities so that the continent would not be unduly vulnerable if the United States were engaged in an Indo-Pacific conflict"

In Europe, the United States is an indispensable security provider, and should plan to remain so. However, the United States should nonetheless work with Europe and Canada to increase their defense capabilities so that the continent would not be unduly vulnerable if the United States were engaged in an Indo-Pacific conflict. In different ways, each of France, Germany, and the United Kingdom has indicated an intent to increase its defense capabilities, and the United States should coordinate with those efforts. A common approach to these issues, mainly through NATO but also with the European Union, will be important.

NATO is the critical defense organization for Europe, providing an overall strategic approach for allies including through its Defense Planning Process, which undertakes to "identify and prioritize the capabilities required for full-spectrum operations,"[129] and the planning and execution of "combined, joint, effects-based operations" under the command of the supreme allied commander Europe (SACEUR).[130] However, in light of the increasingly challenging international context, the deterrent and warfighting capabilities of the Alliance would be substantially improved if the following four initiatives were adopted and implemented.

1) Establish NATO Cybersecurity and Supply Chain Resilience

a) Cybersecurity "Continuous Response"

Cyber raises the same very significant issues for the European theater as it does for the American and Indo-Pacific theaters. In the European theater, however, the United States can work through NATO to establish an effective cyber posture.[131] As noted in the Atlantic Council post "NATO Needs Continuous Responses in Cyberspace," "While the cybersecurity of infrastructure and government systems is a national responsibility, a breach of cybersecurity at the national level can have collective consequences."[132] Accordingly, that same article identifies three important steps that should be undertaken with NATO:[133]

> First, as is true of other theaters, the development and implementation of resilient cybersecurity architectures is important for NATO, its members' forces, and its key critical infrastructures. NATO itself cannot develop such architectures. It can, however, underscore their necessity and require its members to do so, using the NATO Defense Planning Process (NDPP), acquisition procedures, standards and targets, and innovation from Allied Command Transformation to support a comprehensive research and development effort.
>
> Second, NATO, in coordination with its nations, should undertake active cyber defense that can create resilience even when an attacker has breached cyber protections. As a key element of active cyber defense, NATO must be capable of hunting for adversaries within cyber systems critical to defense.

[128] Wittman, "The US Navy's Modernization Rush Must Not Harm Mine Countermeasures."

[129] "NATO's capabilities," NATO, June 19, 2020, https://www.nato.int/cps/en/natohq/topics_49137.htm.

[130] "Vision and Mission," NATO, Supreme Headquarters Allied Powers Europe, accessed March 13, 2021, https://shape.nato.int/visionmission.

[131] The United States does work on cyber issues directly with allies and those efforts should be continued.

[132] Franklin D. Kramer, Lauren Speranza, and Conor Rodihan, "NATO Needs Continuous Responses in Cyberspace," *New Atlanticist*, Atlantic Council, December 9, 2020, https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-continuous-responses-in-cyberspace/.

[133] This section is drawn directly from Kramer, Speranza, and Rodihan, "NATO Needs Continuous Responses in Cyberspace."

The Alliance should develop highly capable expert hunt teams to review system activities, detect anomalies, and defeat intruders, for example by deleting malware and closing unnecessary ports. NATO can significantly enhance Allies' active defense efforts by establishing an NDPP requirement for national cybersecurity hunt teams, along with command arrangements for those teams in both hybrid and Article 5 contingencies. It should also establish several NATO Standing Cybersecurity Hunt Teams that would operate with the consent and active partnership of national governments and critical infrastructure network operators to provide cybersecurity for such key critical infrastructures. Standing Cybersecurity Hunt Teams, with a focus on active defense, would expand on the capabilities of NATO's current Cyber Rapid Reaction teams which are limited in numbers and operate reactively.

Third, NATO should coordinate a strategy of persistent engagement to reduce Russian and Chinese activities to undercut the Alliance in cyberspace. NATO should leverage its collective nature to help Allies coordinate a strategy of persistent engagement as a key element of its overall deterrence and defense strategy. NATO should focus its persistent engagement efforts in three areas of high consequence to member nations: 1) disruptions of key critical infrastructure (e.g., electric grids, telecommunications networks, energy pipelines, and finance systems); 2) cyber espionage to undermine NATO military capabilities and advanced defense technologies; and 3) manipulation of Allies' democratic processes, such as elections. NATO support to Allies in these areas is fundamental to its core task of collective defense and security.

Persistent engagement involves tracking adversaries, understanding their goals, analyzing the tools used for attacks, and taking actions to degrade their capabilities to blunt ongoing, or prevent future, attacks. Customary international law, including the law of countermeasures, pleas of necessity, and other cyber norms, provides the international legal basis for a strategy of persistent engagement. Because NATO Allies have already been attacked and are continuously being targeted by these adversaries, offensive actions to counter such activities are justified, as long as they are conducted proportionately. While persistent engagement arguably could increase instability in cyberspace, Alliance inaction is far more dangerous. If Russia and China perceive no consequences to their malign actions in cyberspace, they will only continue and even intensify them.

To accomplish persistent engagement effectively in an Alliance context, NATO should leverage its intelligence and defense planning capacities to develop a system for Allies to constantly track cyber threats from Russia and China. Through its Intelligence and Security division, NATO should gather intelligence on which Allied critical infrastructure, military capabilities, or democratic processes are being targeted. Using this information, NATO's Cyberspace Operations Center (CYOC) could outline ways to diminish Russian and Chinese capabilities to execute such attacks. The CYOC should share its analyses with pre-designated Allies who would work with targeted countries and employ their own cyber effects against the identified threats. Nine NATO nations have already volunteered to provide such effects in support of NATO activities. These cyber-capable Allies would be responsible for persistently disrupting adversaries' cyber activities based on NATO's guidance. This model would make NATO's CYOC a planning hub for an Alliance-wide approach to persistent engagement. It would allow NATO to empower its members to take individual or multilateral actions against adversaries' hybrid campaigns in cyberspace.

b) Supply Chain Resilience

NATO needs to work with the United States and all its member nations on the same set of supply chain issues identified in Sections II and IIIA on the US and Indo-Pacific theaters, respectively. NATO should perform a supply chain analysis that focuses on military capabilities and the vulnerabilities that arise from an overdependence on unreliable sources. A NATO effort could be especially valuable for smaller nations that cannot easily undertake a comprehensive supply chain review on their own. While the United States will work with NATO on supply chain issues, there will also be benefits in working with the European Union, where the European Commission has already done its own study on raw materials (including identifying rare earths as a sector on which Europe is overly dependent on China).[134] The objective should be an effective transatlantic strategy to reduce undesirable dependencies. In the transatlantic context, establishing a "Transatlantic Coordinating Council" has previously been proposed in the context of hybrid

[134] European Commission, *Critical Raw Materials for Strategic Technologies and Sectors in the EU: A Foresight Study,* September 3, 2020, https://ec.europa.eu/docsroom/documents/42882.

challenges and with respect to China.[135] Supply chain resilience could similarly benefit from utilizing a Transatlantic Coordinating Council. Such a council would be a voluntary organization consisting of the member nations of NATO and the European Union as well as the European Union and NATO as entities.[136] By bringing together all relevant players, this would allow for agreement on policy for supply chains and then implementation by the competent authorities.[137]

2) Enhancing the Effectiveness of the NATO Readiness Initiative Forces

a) NATO Readiness Initiative combat capability: The NATO Readiness Initiative (NRI), approved in June 2018, calls for NATO allies to have thirty battalions, thirty air squadrons, and thirty naval combat vessels ready to use within thirty days.[138] According to NATO documents, allies had "generated more than ninety per cent of the forces required" as of 2019.[139] But while the NRI forces may be designated on paper, they have not been organized into effective fighting structures nor have they been tasked with the type of mission clarity needed for effective warfighting.

In a kinetic conflict with Russia, NATO would need to engage in a multi-domain battle. Within the multi-domain effort, forces that operate from a particular domain will need to be cohesively structured—for example, corps, division, brigade, battalion; fleet, battlegroup; air force, wing, squadron. Further, they need to understand, train, and exercise for their most demanding mission, which, in the NATO context, would be a conflict with Russia. Such organization and training, however, simply has not taken place. This is especially important for multinational formations.

It might be that NATO implicitly is relying on the United States to provide the structure and cohesiveness for its other forces. But while the United States does have the capacity to be a "backbone" force, it cannot do so effectively without regularly working with forces from other nations in support of the required mission. To be sure, NATO and the United States undertake extensive exercise schedules including valuable exercises like Trident Juncture,[140] and the US-led Defender series,[141] but such exercises are not equivalent to exercises specifically focused on preparing for a conflict with Russia. Accordingly, NATO should undertake the requisite organizational, training, and exercising activities to provide the greatest capability—and hence deterrence—for NRI-designated forces focused on a conflict with Russia.

> "NATO should create for land forces the same type of command structure that it has established for air forces where the United States European Command (EUCOM) air commander is also the NATO air commander"

b) NATO Command Structure and NRI Forces: NRI forces require effective command and control to generate the required deterrent and warfighting capabilities. The current NATO command structure is not, however, directly linked with those forces. Further, it lacks the required multi-domain approach, and it needs to engage the US Army as the operational land commander in the same way the US Air Force provides operational air command for the Alliance. NATO should take three steps to resolve these issues.

First, NATO should create for land forces the same type of command structure that it has established for air forces where the United States European Command (EUCOM) air commander is also the NATO air commander[142] The US Army land commander should be double-hatted to be the NATO land force commander. In a conflict, that position could be placed in the command structure below the Joint

[135] Franklin D. Kramer, *Priorities for a Transatlantic China Strategy,* Atlantic Council, November 2020, https://www.atlanticcouncil.org/wp-content/uploads/2020/11/PRIORITIES-FOR-A-TRANSATLANTIC-CHINA-STRATEGY-IB.pdf, 7.

[136] Operating along the lines of voluntary organizations such as the Financial Stability Board or the Proliferation Security Initiative. Kramer, *Priorities for a Transatlantic China Strategy*, 5.

[137] The European Union already uses several forums including the European Council and the Council of Ministers to ensure that national interests are integrated into policy. A Transatlantic Coordinating Council that included supply chain resilience in its mandate would have similar value.

[138] NATO, "NATO Readiness Initiative," June 2018, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_06/20180608_1806-NATO-Readiness-Initiative_en.pdf.

[139] NATO, *NATO: Ready for the Future: Adapting the Alliance (2018-2019),* 2019, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_11/20191129_191129-adaptation_2018_2019_en.pdf, 6.

[140] "Trident Juncture 2018," NATO, October 29, 2018, https://www.nato.int/cps/en/natohq/157833.htm.

[141] Todd South, "Massive, Army-Led NATO Exercise Defender Europe Kicks Off," *Army Times*, March 15, 2021, https://www.armytimes.com/news/your-army/2021/03/15/massive-army-led-nato-exercise-defender-europe-kicks-off/.

[142] "Allied Air Command," NATO, accessed April 18, 2021, https://ac.nato.int/: ("in the event of a joint NATO operation he is the responsible commander of the Air Component").

Force Commanders. The United States would provide key elements for any land battle and having the US land commander dual-hatted would allow for the most effective use of NATO's land forces.[143]

Second, the forces that are designated for the NRI should also have clear chains of command, and the components in the chain should regularly work together including through appropriate periodic exercises.

Third, NATO should plan with the United States for US multi-domain command and control capabilities to be available to integrate with non-US forces. This is, of course, nothing other than saying that NATO needs to be interoperable, a long-standing requirement. However, the United States is pressing forward with advanced concepts and technological capabilities such as JADC2 (Joint All-Domain Command and Control), and it is important to maintain interoperability requirements as part of the development effort. Moreover, while JADC2 is still in development, its central premise—which will be important for NATO warfighting capabilities—is that artificial intelligence will be critical to the future battlefield. As the United States expands its artificial intelligence capabilities through JADC2 or otherwise, it needs to also ensure interoperability with allies.[144]

c) Terminate the NATO Response Force except for the Very High Readiness Joint Task Force: NATO approved the NATO Response Force (NRF) in 2003.[145] At the time, it was intended to be essentially an expeditionary force for contingencies outside NATO. After Russia's 2014 Crimea invasion, NATO increased the size of the NRF to its current size of approximately forty thousand.[146] As a matter of fact, however, the NRF has not been used in any significant NATO engagements.[147] Rather, while NATO annually designates forces and a command structure for the NRF, it instead utilizes force generation conferences where nations offer particular forces for specific missions.[148] Moreover, the NRF would not be fit for purpose to deal with a Russian contingency. Its forces are not organized, trained, or equipped for a high-end kinetic battle—rather, the NRF is billed by NATO as "Any mission, anywhere,"[149] which is hardly the focus needed for what would be a very significant high-end campaign. Moreover, it almost certainly could not arrive in place in a timely fashion. Accordingly, NATO should terminate the NRF as it currently exists,[150] and instead organize the NRI forces as discussed above with a focus on the Russian threat. Since crisis management is also an important NATO task, however, a much smaller Very High Readiness Joint Task Force of approximately five thousand built around a brigade with supporting elements should be maintained.

3) Enhance NATO Mobility Capabilities and Forward Presence

NATO's deterrence strategy depends in significant part on its ability to have sufficient forces promptly available to respond to a Russian conventional attack. Especially with the United States necessarily concurrently focused on two theaters, NATO needs to enhance its mobility capabilities and forward presence to make clear that it has the required prompt capability. Three initiatives are necessary: establishing a NATO funding mechanism to support mobility improvements; establishing effective command and control of certain rear area logistic activities under the Joint Support and Enabling Command; and prepositioning materiel for European heavy forces in the east complemented by some additional US Army capability.

The NATO Response Initiative provides that the NRI forces are to be ready to use within thirty days. However, existing constraints with respect to mobility make achieving that goal improbable. There have been two major mobility studies by think tanks in the past year, one co-chaired by a former SACEUR and the other co-chaired by the former US Army Europe commander.[151] Each of the studies reached the same conclusion—that NATO's current mobility is inadequate. As a result, the studies' recommendations included robust funding of infrastructure improvement; improved command and control procedures established and tested through deliberate exercises; enhanced

[143] With this arrangement, NATO's land command in Izmir, Turkey, could continue as a command focused on readiness of the land forces or, alternatively, readiness could be a function of the NATO land commander.

[144] Effective multidomain operations similarly apply to cyber operations and the domain of space, especially as the latter would play a critical role in providing, among other things, sensor-based cueing; communications; and position, navigation, and timing information.

[145] "NATO Response Force," NATO, last updated March 17, 2020, https://www.nato.int/cps/en/natolive/topics_49755.htm.

[146] NATO, *Readiness Action Plan,* March 23, 2020, https://www.nato.int/cps/en/natohq/119353.htm.

[147] The NRF was utilized for summer Olympics support in 2004, Afghan presidential election support in 2004, assistance to the United States in the wake of Hurricane Katrina in 2005, and Pakistan humanitarian aid in 2005-2006. "NATO Response Force," NATO.

[148] John Deni, *Disband the NATO Response Force*, Atlantic Council, accessed March 26, 2021, https://www.atlanticcouncil.org/content-series/nato20-2020/disband-the-nato-response-force/.

[149] "NATO Response Force," NATO.

[150] Deni, *Disband the NATO Response Force.*

[151] The Atlantic Council published *Moving Out: A Comprehensive Assessment of European Military Mobility* in April 2020. It was co-chaired by General Curtis M. Scaparotti, US Army (Ret.). Scaparotti served as the supreme allied commander Europe from 2016 to 2019. CEPA, the Center for European Analysis, published *The CEPA Military Mobility Project: Moving Mountains for Europe's Defense* in March 2021. It was co-chaired by Lieutenant General Frederick B. (Ben) Hodges III, US Army (Ret.). Lieutenant General Hodges was commander, US Army Europe, from 2014 to 2017.

infrastructure resilience; standardization and streamlining of border crossing procedures to create a "military mobility Schengen"; and increased political support and high-level official coordination for the mobility efforts within the EU and NATO.[152]

"NATO should utilize a prioritized list of mobility projects to develop the requirements for a 'mobility infrastructure fund' that nations collectively would support"

The most fundamental obstacle to resolving NATO's mobility challenges is the lack of adequate funding. While the European Union has initiated an "Action Plan on Military Mobility,"[153] the EU's efforts have proven inadequate to provide sufficient resources for NATO to achieve its thirty-day mobility goal. While the United States has recently indicated a desire to join the EU mobility effort,[154] a harmonized approach will not change the reality that the EU five-year budget provides for only 1.69 billion euros,[155] an entirely insufficient amount to meet the full spectrum of mobility requirements. By way of comparison, the European Commission in its proposed budget had recommended a 6.5 billion euro budget for military mobility,[156] and one estimate by the European Court of Auditors—solely for a single proposed rail corridor that would connect Poland, Lithuania, Latvia, Estonia, and Finland—was 7 billion euros.[157] Other mobility projects would obviously add to the cost.

If an adequate level of mobility capability is to be achieved, NATO itself will have to organize the necessary funding. To accomplish this, NATO should utilize a prioritized list of mobility projects to develop the requirements for a "mobility infrastructure fund" that nations collectively would support to accomplish the necessary projects.[158] Such expenditures by nations should be counted toward the NATO 2 percent defense spending goal for nations. NATO would have to decide on the required level of funding from each nation. However, inasmuch as the United States has already established the European Deterrence Initiative, which includes infrastructure funding, the mobility infrastructure fund should receive the bulk of its funding from European NATO members and Canada. A designated fund such as this would provide NATO the necessary funding for its key defense mobility goals.

Even with adequate funding, effective military mobility is not achievable without appropriate command and control. To accomplish this, both think tank reports identify the need for a more clearly defined role for NATO's Joint Support and Enabling Command (JSEC) and for continued and deliberate exercises to test and stress the transportation systems and command and control of movement.[159] JSEC should have rear area authority to effectively bridge national logistics operational centers (including EUCOM for the US forces) to NATO's strategic and operational commands. A key element will be coordinated interaction with the relevant private sector authorities. Future exercises should be used to move the force and member nations toward standard processes that are tailored to support effective military mobility.[160] Such exercises will permit the interaction required to improve mobility capabilities within the Alliance. It will also permit the needed interactions to identify key linkages among civilian and commercial entities crucial to ensuring effective mobility operations during crisis.[161]

[152] Curtis M. Scaparrotti and Ambassador Colleen B. Bell, *Moving Out*, 4-5; Heinrich Brauss, Ben Hodges, and Julian Lindley-French, *The CEPA Military Mobility Project*, 5-11.

[153] European Parliament, *Military Mobility*, 2019, https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/635570/EPRS_ATA(2019)635570_EN.pdf.

[154] Sebastian Sprenger, "US-EU Cooperation Pitch on Military Mobility Gets Positive Response," *Defense News*, March 15, 2021, https://www.defensenews.com/global/europe/2021/03/15/us-eu-cooperation-pitch-on-military-mobility-gets-positive-response/.

[155] "A New Progress on Military Mobility in the EU," Railway Pro, October 20, 2020, https://www.railwaypro.com/wp/a-new-progress-on-military-mobility-in-the-eu/.

[156] European Parliament, *Military Mobility*.

[157] Kristjan Kallaste, "Court of Auditors: Current Rail Baltic Project Not Financially Sustainable," ERR News, June 16, 2020, https://news.err.ee/1102603/court-of-auditors-current-rail-baltic-project-not-financially-sustainable.

[158] Ground mobility requires resource-intensive infrastructure development and standardization of cross-border procedures to meet the thirty-day mobility targets of the NRI. Improvements to the road and rail network are necessary to ensure ground forces can effectively transition from point of debarkation to area of operations. Both studies reflect NATO's need for standardized rail gauges and incorporation of appropriate load-bearing structures into the transportation network. Applicable for ground and air mobility alike is the establishment of properly positioned and adequate stocks of ammunition and petroleum, oil, and lubricants as well as the development of the intermodal connectors between these nodes and the potential fronts. Scaparrotti and Bell, *Moving Out*, 27; Brauss, Hodges, and Lindley-French, *The CEPA Military Mobility Project,* 15.

[159] Scaparrotti and Bell, *Moving Out*, 4; Brauss, Hodges, and Lindley-French, *The CEPA Military Mobility Project*, 8, 54.

[160] Brauss, Hodges, and Lindley-French, *The CEPA Military Mobility Project,* 15.

[161] Scaparrotti and Bell, *Moving Out*, 38-39.

Facilitating the movement of forces would be significantly enhanced if NATO's non-US members would preposition materiel for heavy forces forward. Currently, NATO forces in the Baltics consist of the national forces of each country and the multinational Enhanced Forward Presence battalions.[162] These forces are valuable trip wires and do have a deterrent effect. However, the military balance would be significantly improved if brigade-level heavy forces (including fires) could be very promptly available if required. Prepositioning of European heavy forces forward would allow for such prompt capability to be available. The United States already has prepositioned materiel in Europe for brigade-level forces. One complementary approach would be for the United Kingdom, France, and Germany to preposition materiel for heavy brigades in Estonia, Latvia, and Lithuania, respectively. Such a capability coupled with the United States forces and prepositioning in Poland would substantially increase the deterrent effect and warfighting capabilities for NATO.

> "the United Kingdom, France, and Germany [should] preposition materiel for heavy brigades in Estonia, Latvia, and Lithuania, respectively"

The prepositioned materiel should regularly be used in exercises and deployments by the relevant European forces. In addition to the proposed prepositioned heavy forces, exercises and deployments by the UK-led Joint Expeditionary Force and the French-UK Combined Joint Expeditionary Force (CJEF) would be valuable. The CJEF, in particular, might regularize support to NATO's southeastern flank. As French President Emmanuel Macron has emphasized the importance of European capabilities for defense, those capabilities should be utilized as part of NATO's deterrent efforts vis-à-vis Russia.

The United States could complement European prepositioning by having the Army plan to direct a significant portion of its forces toward Europe and by having the Air Force develop a swing capability so that forces could be promptly available in either Europe or the Indo-Pacific. For the Army, one potential approach would be for the United States to increase the number of armored brigade combat teams (ABCTs) in Europe by one. The precise placement of the ABCT could be determined in conjunction with the review that the Defense Department is undertaking regarding American forces in Europe, although the Defense Department has recently announced adding in Germany a five hundred–person "multi-domain task force, with artillery, air and missile defense, intelligence, cyber, space and electronic capabilities as well as a Theater Fires Command."[163] A further critical step, to offset Russian capabilities,[164] would be fielding enhanced precision long-range fires capability for the European theater.[165] For the Air Force, a swing strategy would be necessary as the requirements for two theaters likely are in excess of the available force. Though it involves risks, a swing approach is possible, but if it is to be undertaken successfully, it will require focus on sufficient basing options and prepositioned materiel. NATO needs to evaluate any needed expansion of airfield capacity as well as key requirements such as properly positioned and adequate stocks of ammunition and petroleum, oil, lubricants.[166] Military construction to "resize existing airfield [and] build new ones to support strategic and tactical airlift" would enhance the ability of NATO forces to practice distributed operations and cold and adaptive basing techniques and create the capacity

[162] Details on the current forces that compose the Enhanced Forward Presence (EFP) are available from NATO in the form of fact sheets at https://shape.nato.int/resources/site16187/General/factsheets/factsheet_efp_2021.pdf. There are currently four EFP battle groups, located in Estonia (led by the UK), Latvia (led by Canada), Lithuania (led by Germany), and Poland (led by the United States). In total, the EFP forces number approximately 4,600 troops.

[163] Robert Burns, "Austin: US Adds 500 Troops in Germany, despite Trump Pledge," Associated Press, April 13, 2021, https://apnews.com/article/joe-biden-europe-lloyd-austin-berlin-germany-201df3ddf8a2b17336c4df2cbf88ef1d.

[164] The 2018 Commission on the National Defense Strategy for the United States identified that the "The United States will need capacity enhancements in the Army. More armor, long-range fires, engineering, and air-defense units are required to meet the ground-heavy challenges posed by Russia in Eastern Europe and while maintaining a robust deterrent to aggression on the Korean Peninsula." Recent Congressional Research Service reporting stated, "Compared with potential adversaries' longer-range systems, wider variety of munitions, and innovative target acquisition techniques, a diminished U.S. artillery capability—based on fewer units, limitations on cluster munitions use, and shorter effective ranges—could present significant battlefield challenges for the U.S. Army, with implications for modernization efforts." Andrew Feickert, *US Army Long-Range Precisions Fires: Background and Issues for Congress*, Congressional Research Service, March 16, 2021, https://crsreports.congress.gov/product/pdf/R/R46721, 2.

[165] Currently, the US Army has two Multiple Launch Rocket System (MLRS) battalions in Grafenwoehr, Germany, as part of the 41st Field Artillery Brigade equipped with the Army Tactical Missile System (ATACMS). Maj. Joseph Bush, "41st Artillery Brigade Comes to Fruition and Changes Command in the Same Day," Defense Visual Information Distribution Service, August 27, 2020, https://www.dvidshub.net/news/377004/41st-field-artillery-brigade-comes-fruition-and-changes-command-same-day. ATACMS range out to only 300 kilometers (km), and the Army is seeking to enhance this capability through the development of the Precision Strike Missile (PrSM). PrSM is compatible with both HIMARS and MLRS and will have an initial range of 500 km, the initial operating capability is expected in 2025, and the Army is already exploring options to increase the range out to 1,600 km. Feickert, *US Army Long-Range Precisions Fires: Background and Issues for Congress*; Sydney J. Freedberg Jr., "Can the Army Triple PrSM Missile's Range?" *Breaking Defense*, April 2, 2021, https://breakingdefense.com/2021/04/can-army-triple-prsm-missile-range/.

[166] Brauss, Hodges, and Lindley-French, *The CEPA Military Mobility Project,* 37.

for higher resupply throughput rates.[167] Additionally, NATO should "[r]amp up procurement of passive protection measures for forward bases (e.g., expedient shelters, fuel bladders, airfield damage repair equipment and materiel, decoy aircraft, and other deception measures) [as] [a]nalysis shows that such measures, in conjunction with active defenses, can significantly enhance force survivability and sortie generation."[168]

[167] Ibid., 36, 38.

[168] David Ochmanek, *Restoring U.S. Power Projection Capabilities: Responding to the 2018 National Defense Strategy,* RAND, July 2018, https://www.rand.org/pubs/perspectives/PE260.html, 11.

IV. CONCLUSION

Establishing an effective national defense strategy will require transformative thinking. In the American theater, sustained and innovative attention will be required. “Effective resilience and defending back” will be necessary components of the strategy. Particular attention will need to be given to cybersecurity and supply chains. An effective interagency operational process will need to be created that engages the private sector and states/localities including through the National Guard. In the forward theaters, a tailored multi-theater strategy focused on China and Russia will be necessary. Working with allies will be key. Cybersecurity and supply chain resilience will be as important in the forward theaters as in the American theater. Multinational capabilities and emerging technologies will be required. Focusing on the transformative priorities discussed in this report will generate both deterrence and the requisite warfighting capabilities necessary to ensure the security of the United States, its allies, and its close partners.

ABOUT THE AUTHORS

Franklin D. Kramer is a distinguished fellow and board director of the Atlantic Council. Mr. Kramer has served as a senior political appointee in two administrations, including as assistant secretary of defense for international security affairs. At the Department of Defense, Mr. Kramer was in charge of the formulation and implementation of international defense and political-military policy, with worldwide responsibilities including NATO and Europe, the Middle East, Asia, Africa, and Latin America.

In the nonprofit world, Mr. Kramer has been a senior fellow at CNA; chairman of the board of the World Affairs Council of Washington, DC; a distinguished research fellow at the Center for Technology and National Security Policy at National Defense University; and an adjunct professor at the Elliott School of International Affairs, George Washington University. Mr. Kramer's areas of focus include defense, both conventional and hybrid; NATO and Russia; China, including managing competition, military power, and China-Taiwan-US relations; cyber, including resilience and international cyber issues; innovation and national security; and irregular conflict and counterinsurgency.

Mr. Kramer has written extensively; in addition to the current report, his publications include, on NATO, *NATO Priorities after the Brussels Summit*, *Meeting the Russian Hybrid Challenge*, and *Meeting the Russian Conventional Challenge*; on China, *Priorities for a Transatlantic China Strategy*, *Managed Competition: Meeting China's Challenge in a Multi-vector World*, and *The China Plan: A Transatlantic Blueprint for Strategic Competition* (chapters on economics and on "one-world" cooperation); on cyber and resilience, *NATO Needs Continuous Responses in Cyberspace*, *Effective Resilience and National Strategy: Lessons from the Pandemic and Requirements for Key Critical Infrastructures*, *Cybersecurity: Changing the Model*, *Cyber and Deterrence: The Military-Civil Nexus in High-End Conflict*, and *Cyber, Extended Deterrence, and NATO*; on innovation and technology, *Innovation, Leadership, and National Security*; and on counterinsurgency, *Civil Power in Irregular Conflict* (principal editor and co-author of the policy chapter) and *Irregular Conflict, the Department of Defense and International Security Reform*.

Lieutenant Colonel Matthew R. Crouch is the academic year 2020 to 2021 Commandant of the Marine Corps Senior Military Fellow at the Scowcroft Center for Strategy and Security at the Atlantic Council. In this role, he has focused his research and writings on defense planning policy and deterrence.

Originally from Sparks, Nevada, Lieutenant Colonel Crouch received his commission from the United States Naval Academy in 2000 with a bachelor of science degree in political science. He was selected for training as a naval aviator upon graduation.

Throughout his twenty-five-year military career, Lieutenant Colonel Crouch deployed four times to the Middle East, including three deployments to Iraq and one to Afghanistan. Having served in a variety of positions of staff and command, he was most recently assigned to the United States Marine Corps Forces Korea staff where he served as the director of operations (G-3).

Lieutenant Colonel Crouch is a qualified MV-22 and CH-46E pilot. He holds a master of arts degree in government and politics from the University of Maryland along with a master of business administration degree from Hong Kong University. He is an Olmsted Scholar.

Atlantic Council

Board of Directors

Atlantic Council

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