Joint Force Experimentation for Great-Power Competition

Sean MacFarland

The war game at the Naval War College came to a frustrating conclusion for the "blue" players representing the U.S. Their attempted dash across the Pacific with powerful naval forces to reinforce positions near the enemy homeland had been stopped well short of their destination by shore-based airpower. Friendly losses due to the enemy's pre-war investment in anti-access/area denial capabilities had been staggering. A quick American victory would not be possible, and a new strategy would be needed to defeat this potential adversary.

Although the location of this war game might not surprise you, the date and opponent might. It took place in 1934, and the adversary was Japan ("Orange" in the war game). Fortunately, the U.S. Navy, informed by the results, changed its war plan in time, and the rest, as the saying goes, is history. In fact, the war game was so prescient that after the war, Fleet Admiral Chester Nimitz said that "the war with Japan had been enacted in the game rooms at the War College by so many people and in so many different ways that nothing that happened during the war was a surprise—absolutely nothing except the kamikaze tactics toward the end of the war. We had not visualized these."[1]

War games and large-scale exercises like those conducted before the Second World War played an important role in our military history, and they are poised to do so again. At the direction of the Chairman of the Joint Chiefs of Staff, General Mark Milley, the Naval War College recently war-gamed a real-world scenario against potential adversaries. It was a good start, and more such war games are expected to follow as are other forms of experimentation. If they do, these opportunities to learn will once again play a vital role in the development of a joint doctrine that supports our National Defense Strategy, addresses the challenges and opportunities created by technological change, and responds to rising threats to both national and global security. If fully supported, they will help America's defense establishment to make cost-effective investments and reduce strategic risk by tapping into America's greatest asymmetric advantage: our ability to innovate.

Global Challenges

In his article "The Thucydides Trap," Graham Allison observed that a rising power and a dominant power do not usually exchange places peacefully. This is the trap into which Athens, as a rising power, and Sparta, as the dominant power, fell.[2] How can the United States, as the world's dominant power, avoid the fate of Sparta, which defeated Athens but was so weakened that it also soon collapsed? The first requirement, of course, is to recognize threats and—just as important—their nature.

The fastest-rising power in the world today is China, which has embarked on what Michael Pillsbury calls a "hundred-year marathon"[3] to

displace the United States as global hegemon. Although most observers agree that Beijing does not wish to use direct force to overthrow the American order and establish itself as the new "sun in the sky," China is clearly arming itself in a way that is meant to challenge American power in the Western Pacific. It is also seeking to compete with the United States through diplomatic, information, and economic means. The implications of these efforts are profound not just for the United States, but also for the entire world.

From the end of the Cold War until recently, we have lacked a clearly defined pacing threat: a nice problem to have had but a problem no longer. A resurgent Russia and a rising China took note of how the U.S. rapidly overwhelmed the Iraqi military in conventional warfare in 1991 and again in 2003. Since then, both nations have embarked on acquisition strategies designed to neutralize our joint warfighting advantages, now enabled by new technologies like unmanned aerial systems and stealth aircraft. By investing in relatively low-cost systems that are designed to prevent us from projecting our forces, our adversaries are now challenging our ability to achieve overmatch against our opponents on the battlefield. This asymmetric approach is called anti-access/area denial (A2/AD).

This renewed geostrategic competition is unfolding amid a revolution that has the potential to rival the Industrial Revolution in its impact. The technological revolution driving these changes in the character of war will change the 21st century battlefield as much as the Industrial Revolution changed the battlefield in the 20th century. Space, which became accessible in the latter half of the 20th century, is growing ever more congested and contested in the 21st.

America, which pioneered space travel, no longer enjoys assured access to it, removing it as one of our asymmetric advantages over our enemies. Cyberspace, which the United States also pioneered, is now shared by the entire world and has joined space as a new domain of warfare along with the more traditional domains of air, sea, and land. As our dependence on space and cyberspace has grown, so too have our vulnerabilities. The globe-spanning reach of these new domains has expanded the battlefield to the homelands of our adversaries as well as to our own "forts and ports," rendering our Atlantic and Pacific moats ineffective.

Advances in weapon technology are potentially game-changing as well. Stealth, or low-observable technology, directed energy for weapons, sensors and communications, remote-controlled vehicles, and hypersonic weapons are accelerating the speed of war from supersonic to hypersonic and beyond, to the speed of light. As if this were not mind-boggling enough, advances in artificial intelligence (AI), powered by big data and information operations that exploit social media platforms, are creating additional challenges and opportunities.

The ability of the human mind to close the OODA (observe, orient, decide, act) loop in a timely manner in response to these technological changes is increasingly at risk. The "cognitive domain" of war is not new, but its character has changed along with the other domains, perhaps making it the most significant domain of all.

To undermine U.S. power, our adversaries are employing other asymmetric means that stop short of traditional acts of war, blurring the line between peace and conflict. The so-called Russian gray zones, China's civil–military integration, Iran's proxy forces, and cyber-attacks by non-state actors have thickened the fog of war. Doctrinal discussions have moved away from the "pre-conflict phase" in favor of a continuum of conflict that encompasses competition and hostilities. We are competing with our peer adversaries and have been for a while, whether we realized it or not. Twenty-first century conflict, then, has expanded not only spatially, but also temporally.

Our Doctrinal Response

Our adversaries have reacted to our actions, and now it is our turn to counteract by

developing a new doctrine that leverages our asymmetric strengths to degrade, penetrate, and ultimately disintegrate A2/AD measures and restores our strategic reach and ability to fight on favorable terms. Our response must address both geostrategic and technological changes. It must be sufficiently compelling to achieve broad support both among U.S. policymakers and among our allies. It must also be affordable. The U.S. used a cost-imposition strategy to defeat the Soviet Union during the Cold War. We cannot allow ourselves to be driven down an unsustainable path in a similar way, as A2/AD would have us do.

To answer all of these challenges, the U.S. Department of Defense (DOD) is developing a doctrine called Joint All Domain Operations (JADO). It is still only a concept, but it builds on the work started by the U.S. Army, joined by the Marine Corps, in developing the warfighting Multi-Domain Operations (MDO) concept. It will also incorporate subsequent work done by the Air Force on the Joint All Domain Command and Control (JADC2) concept and eventually will include concepts from the Navy and Space Force as well. JADO recognizes the new domains of conflict and is intended to exploit them with cross-domain effects and will leverage our armed forces' unique and proven ability to orchestrate joint operations at all echelons.

But choosing the right doctrine is only the beginning. Multi-domain effects, by definition, transit through more than one domain. To fight and win in all domains, our joint doctrine must achieve harmony across all services and across all elements of doctrine, organization, training, materiel, leadership, personnel, and facilities (DOTMLPF) as well as policy (as in "DOTMLPF-P"). As we modernize our forces, new platforms and systems must be designed with cross-domain effects in mind.

As former Secretary of Defense Donald Rumsfeld famously observed, "You go to war with the army you have, not the army you might want or wish to have at a later time."[4] We need to ensure that the Joint Force we have is the one we want. The policy aspect is also important, particularly in the space and cyber domains where management of the electromagnetic spectrum and networks in the competition phase of conflict will mean striking a balance between civil and military requirements.

Getting the services to align doctrines and acquisition programs and to integrate operationally across domains is hard but not impossible. We came close in the final years of the Cold War under the rubric of AirLand Battle (ALB). The Army aligned all elements of DOTMLPF to support ALB, and—critically—so did the Air Force, making the vision of a seamless dual-domain operational concept a reality. Although we did not have the benefit of sophisticated computer modeling tools then, we were able to test some ALB assumptions during the massive annual REFORGER exercises in Europe. We also benefitted from the very real and bloody lessons gleaned from the 1973 Arab–Israeli War. Acquisition efforts in the Army were tailored to ALB and vice-versa.

Thus, the "Big Five" Army weapons programs still widely in use today were ideally suited to the doctrine, and the integration of joint effects in training and exercises became the norm. In the end, we were able to catch doctrinal lightning in a bottle, as proven in Operation Desert Storm against a combat-seasoned, Soviet-trained, and Soviet-equipped enemy.

The Role of Joint Experimentation

America's armed forces are again racing to refashion themselves and adjust to technological innovations, just as they did before World War II when the U.S. shifted from a constabulary Army mounted on horseback and a battleship-centric Navy to a Joint Force that is able to project airpower around the world in support of amphibious and mechanized land forces. Today, we are shifting our focus from counterinsurgency to competition against peer adversaries in peacetime and seeking to achieve overmatch against them in all domains in conflicts.

Experiments like the recent war game in Newport, Rhode Island, will play a vital role

in helping America's military to reshape itself effectively and efficiently. Experimentation through war games and exercises is conducted in a mixture of live, virtual, or constructive environments. In virtual environments, live people interact with simulated systems, as in a flight simulator. In a constructive environment, simulated people interact with simulated systems, as in a command post exercise. The degree to which each environment is present in a war game or exercise depends on the purpose of the exercise. Each form has advantages and disadvantages, and when used for the purpose for which it is best suited, each form can provide useful insights for the development and implementation of JADO.

In the past, each service conducted its own experiments, developed its own respective warfighting concepts or doctrines, and then acquired the capabilities required to execute them—and, of course, it sometimes happened the other way around. In either case, the role played by the Joint Chiefs and the Office of the Secretary of Defense (OSD) resembled that of a referee, ensuring that the services played by the rules. To fulfill the promise of JADO, the role of the Secretary of Defense and the Chairman of the Joint Chiefs should be more like that of a coach, directing the game plan for the services' modernization efforts. The playbook, however, must be informed by the lessons learned through experimentation, and those must be properly resourced. In addition, as any coach will tell you, there is no gain without pain.

As important as modernization might be, the Secretary of Defense and the Joint Chiefs of Staff have many other responsibilities and cannot devote their full attention to it. Since the 2011 inactivation of the United States Joint Forces Command (USJFCOM) as a cost-saving measure, the Joint Staff Directorate for Joint Force Development (J7) has assumed many functions related to modernization. It is responsible for doctrine, education, concept development and experimentation, training, exercises, and lessons learned. But as a staff directorate, it has no forces of its own, nor does it have teams of experienced observers schooled in joint doctrine or dedicated opposing forces ("red teams") trained to think differently. To the extent that these assets exist, they reside for the most part in the services. Nevertheless, by leveraging two initiatives called Globally Integrated Exercises and Globally Integrated Wargames, the J7 is doing a great deal to innovate and validate joint warfighting concepts.

Any attempt to achieve change, however, will encounter resistance. To help overcome parochial service perspectives, the Joint Chiefs have created a cross-functional team to study JADO. The Joint Chiefs have also tasked the services with examining "orphan" functions. The Air Force is studying command and control, the Navy has the lead for fires, the Marines are responsible for Joint Concept for Information Advantage, and the Army is analyzing the logistics requirements for this Joint Warfighting Concept. The intent of this division of labor is to help break down stovepipes and create consensus.

Exercises as Experiments. The results of these studies must be tested somehow. Despite the growing cost associated with deploying live forces, exercises conducted under realistic field conditions are still the best way to test some theories, particularly organizational designs. This will remain true as long as our ability to simulate cross-domain effects in the constructive environment is limited.

As with war gaming, America has a history of organizational experimentation during exercises that goes back to the years preceding its entry into the Second World War. Perhaps the most famous example from this time period would be the Louisiana Maneuvers (LaM), which the Army conducted to test the doctrine and weaponry it would need to face modern adversaries such as Germany. This massive exercise placed experimental armored and mechanized units and the Army Air Corps into a scenario that helped leaders understand the potential of mechanized warfare and how to integrate airpower over vast operational distances.

Large-scale exercises like the LaM provide an unmatched opportunity to fully understand the capabilities and limitations of experimental organizations and new systems. However, the larger the exercise, the greater the competition to prioritize exercise goals. Such goals might include validating a portion of a war plan, improving interoperability with regional partner forces, demonstrating a new capability as a deterrent to adversaries, or all the above. Sometimes, that does not leave much room for experimentation.

A more recent example of a large-scale experimental exercise is Millennium Challenge 2002 (MC02), sponsored by the then newly formed JFCOM. MC02 featured emerging doctrinal concepts such as "dominant battlespace knowledge" and "rapid decisive operations." It also introduced "leap ahead technologies" that were not yet fielded to the force, such as the V-22 Osprey. The director of the exercise said that it would be a key to military transformation. It cost approximately $250 million and involved over 13,000 servicemembers at nine live-force training sites and 17 simulation centers. To justify the expenditure and the commitment of so many forces, additional exercise objectives were added. Not surprisingly, the exercise was unable to fulfill all of them.

MC02 was supposed to be a free play exercise, but when red (enemy) asymmetric tactics inflicted unexpectedly heavy losses on blue (friendly) forces in the opening turn of the game, the director had to intervene. Most of the U.S. naval task force was "re-floated" so that the rest of the exercise could continue and achieve other objectives such as unit live-fire training. In other words, experimentation had to give way to training. Many lessons were learned from this experience, but perhaps the biggest is that it is difficult for large exercises to achieve every goal.[5]

Organizational Experimentation. This is not to say that large exercises are not useful for experimentation. Combatant Command (COCOM)–level exercises such as DEFENDER-Europe and Pacific Sentry have served as valuable opportunities for the development or validation of concepts and capabilities. For example, the Army created the Multi-Domain Task Force (MDTF) in the Pacific to test MDO doctrinal concepts. It combined units capable of long-range precision fires with a provisional Intelligence, Information, Cyber, Electronic Warfare, and Space (I2CEWS) Battalion. The MDTF then participated in the most recent Rim of the Pacific (RIMPAC) exercise. This went well enough that another MDTF is being created in Europe.

The services are experimenting with organizational designs in a variety of exercises, large and small. Each service has multiple examples, but two of them indicate their diversity and level of investment. The 88th Air Base Wing at Wright Patterson Air Force Base in Dayton, Ohio, is researching how the Air Force can best defend its strategic infrastructure—our homeland "forts and ports"—against attacks in the emergent domains of warfare. Meanwhile, the Navy's Surface Development Squadron ONE (SURFDEVRON ONE) will experiment with unmanned surface vessels and *Zumwalt*-class ships. Vice Admiral Richard Brown, Commander, Naval Surface Force, U.S. Pacific Fleet, described SURFDEVRON ONE's role as "developing warfighting capabilities and experimentation." It will also "[d]evelop material and technical solutions to tactical challenges" and "[c]oordinate doctrine, organization, training, material, logistics, personnel and facilities requirements for unmanned surface systems."[6]

Sometimes, an operational environment is the only way to stress test a concept or capability. Last year, the Navy embarked a full squadron of Marine F-35B Joint Strike Fighters on the amphibious assault ship USS *America*, converting it into a mini-aircraft carrier, or "Lightning Carrier," capable of conducting sea-control operations.

Service-Led Experimentation. After numerous unsuccessful attempts to find a solution to an experiment, Thomas Edison said, "I have gotten lots of results! I know several thousand things that won't work!"[7] Many live, virtual, and constructive exercises are conducted around the globe each year. They can and do

serve as laboratories; their results help us to find out more efficiently what will or will not work. Smaller-scale exercises sponsored by the services provide low-cost opportunities to generate feedback from lower echelons. Some of these are done primarily for training and readiness; others are intended as experiments with collateral training benefits. In either case, if the number of objectives is manageable, they can all generally be achieved.

For example, the Baltic Operations (BALTOPS) fleet exercises led by the recently reactivated U.S. Second Fleet have helped to iron out interoperability issues with allied navies and have enabled experimentation with concepts for Arctic operations and trans-Atlantic convoy tactics, among other benefits. Although these are not new types of operations, the Navy is learning how to conduct them in a multi-domain environment and in the more accessible Arctic Ocean.

Each year, the Air Force brings units from around the world to participate in its Red Flag Exercise at Nellis Air Force Base, Nevada. Against a tough, well-trained "aggressor" unit, the Blue forces learn how to employ space, cyberspace, and stealth to defeat integrated enemy air defenses such as those that characterize A2/AD environments. These exercises do a good job of combining training with concept development even though they are not specifically designed for the latter.

The Army conducts an annual exercise called the Joint Warfighting Assessment (JWA) that is designed specifically for experimentation. As the commander of 1st Armored Division at Fort Bliss, Texas, I have seen its value firsthand. JWAs are coordinated by the Joint Modernization Command, formerly known as the Brigade Modernization Command. As an aside, it is noteworthy that the word "Army" does not appear in the title of the exercise or its sponsoring agency. This makes sense, however. The purpose of the JWAs is to find solutions to multi-domain operational challenges in a joint context.

For several years, an entire Brigade Combat Team (BCT) was dedicated to experimentation, testing new equipment and doctrines in harsh field conditions at Fort Bliss and White Sands Missile Range. Cyber operations by and against a sophisticated and robust cyber opposing force were a recurring feature of these exercises. The cyber warriors tested the participants to their limits—and sometimes beyond them—because failure is often a better teacher than success. Although it was not the principal reason for the exercise, the rest of the division gained training value from supporting and participating in the JWAs, particularly because the Air Force, Marine Corps, and our allies were also involved. Today, the JWAs have moved from Fort Bliss and alternate between Europe and the Pacific and are now "coming to a theater near you" in order to test concepts and capabilities in possible theaters of operation against peer adversaries.

Even routine training exercises serve as opportunities for experimentation. As commander of the U.S. Army's III Corps at Fort Hood, Texas, I was able to test a concept during a major command post exercise and improve the corps' combat readiness at the same time. We employed a Stryker Brigade Combat Team that had been reorganized and retrained to perform in the role of a cavalry regiment in support of the corps during a Warfighter Exercise. The purpose of the exercise was to train corps-level and division-level staffs and prepare them for upcoming operations, which it did in full. The experimental objective did not hinder our training in the least. In fact, in some ways, it helped. Despite its focus on unit training, the exercise yielded important results by validating the requirement for restoring a corps-level reconnaissance and security brigade or regiment. It did not validate the Stryker Brigade solution, but like Edison, we did not fail; we just found out what did not work.

Collecting the insights from all of this exercise-based experimentation across the Joint Force and then applying them to the joint concept development process is a challenge. Although it is a good problem to have, the J7 has its work cut out for it, sorting through the results to find the golden nuggets. These

exercises are yielding a great deal of innovation, and it is important that this innovation is properly considered and exploited by the appropriate organization.

War Games as Experiments. Although exercises are becoming increasingly joint and have begun to explore cross-domain challenges, the models, simulations, and war gaming (MS&G) that support experimentation offer a better opportunity to test concepts and capabilities rapidly. MS&G is not without risk, however. Professor Robert Rubel of the Naval War College has identified several "wargaming pathologies" that are failures in purpose, politics (for example, preordained outcomes), design, assessment, and analysis.[8] Given the complexity and tempo of all-domain war games as well as what is at stake, it will take a significant effort to avoid such pathologies.

As the noted British statistician George Box put it, "[A]ll models are wrong, but some are useful." If the COVID pandemic has taught us anything, it is that Mr. Box knew what he was talking about. Naturally, the early predictions about how the virus would spread were off, but some of the most influential models were off by an order of magnitude, leading to governmental decisions that could have effects equal to or worse than the disease itself. The medical profession tries to live by the code "first, do no harm." Similarly, military doctrines need not be exactly right, but they must at least avoid being "too badly wrong," as British military historian Sir Michael Howard so memorably put it. As pandemics and military history have proven, failure by either medical or military professionals to heed these cautionary words can have fatal consequences.

Avoiding a joint warfighting doctrine that is "too badly wrong" requires useful models designed to replicate multi-domain conflict as accurately as possible. An apocryphal cautionary tale about the use of computer models circulated during the Vietnam War. In 1969, Pentagon staffers asked a computer when the United States would win based on all measurable military data. It quickly answered: "You won in 1964!"

An actual and well-documented example of the war-game design pathology occurred in 1990 when military models vastly overestimated the number of U.S. casualties during Operation Desert Storm. Once word leaked out, widespread concern led to some changes in the plan. A RAND paper published just before the Gulf War predicted the discrepancy, saying that "in many cases the models are built on a base of sand."[9] Unfortunately, despite significant DOD expenditures on models and simulations—nearly $300 million in 2017 alone—the problem persists.[10]

Some important simulations still rely on Lanchester equations to estimate combat losses. Frederick Lanchester, a British engineer, developed the equations in 1916 to conceptualize aerial combat and warned at the time that they were not applicable to ground combat.[11] Perhaps we should have listened to him. Although updated to account for the effects of modern weapons, Lanchester-derived equations used by pre–Desert Storm modelers failed to fully appreciate the dynamics of AirLand Battle and the use of precision-guided munitions in a desert environment. This led to a miscalculation of *multiple* orders of magnitude (fortunately, in our favor). Presumably, the equations' accuracy will not improve when applied to non-kinetic cross-domain effects against logistics or command and control functions.

Obviously, this is an area begging for research and development, and DOD is not blind to the need. In February 2015, then-Deputy Secretary of Defense Robert Work issued a memorandum titled "Wargaming and Innovation" in which he argued that war games can "spur innovation and provide a mechanism for addressing emerging challenges, exploiting new technologies, and shaping the future security environment."[12] Later that year, he coauthored an article with then-Vice Chairman of the Joint Chiefs of Staff (VCJCS) General Paul Selva titled "Revitalizing Wargaming Is Necessary to Be Prepared for Future Wars."[13] He also implemented some MS&G innovations, such as forming the Defense Wargame Alignment Group (DWAG), the Wargame

Repository, and the Wargame Incentive Fund (WIF), which was funded at $10 million. These initiatives helped to gain efficiencies across the enterprise, but the sort of fundamental changes required by all-domain joint warfighting will require a larger effort and a new way of doing business on the part of DOD.

Clearly, new MS&G software will be needed to address the challenges of all-domain joint warfare. Unfortunately, as current VCJCS General John Hyten said during his confirmation hearings, the process of developing military software is "a nightmare across the board" compared to the commercial process as practiced by American companies like Google, Amazon, and Microsoft.[14]

Spending money on new simulations is only half the battle, though. To achieve the best designs and avoid the other war-gaming pathologies, the MS&G community will need to be populated and led by a cadre of officers and civilians who fully understand the state of the art and the warfighter's requirements. The Naval Postgraduate School has created a field of study, in which classes in war-game design are exclusively electives, that can serve as a starting point for the rest of the Joint Professional Military Education (JPME) enterprise. Today, the Army is the only service with a career field dedicated to simulations, and Functional Area 57 (FA 57) officers are assigned to all major Army headquarters at the division level and above. This is a best practice that the other services should consider emulating while the Army assesses whether its FA 57 officers are getting the right training.

Ideally, in addition to learning the art of federating simulations for distributed exercises, MS&G leaders would also learn how to avoid or mitigate the other war-gaming pathologies. To do this, they must understand the capabilities and limitations of both software and wetware: that is, the human element. Seminar-style war games known as BOGSATTs (Bunch of Guys Sitting Around a Table Talking), in which a roll of the dice is used as the stochastic method to replicate uncertainty, can play a role in identifying novel concepts, but they are not well-suited to adjudicating (solving) them. The Army's Unified Quest (UQ) seminars have played an important part in helping to identify challenges related to Multi-Domain Operations (MDO), but they have not been used for adjudication. One of the key tasks throughout the UQ 2019 study year was how to operationalize artificial intelligence in support of MDO,[15] but adjudication of this automation-related question will require a more automated war game.

As Alexander Kott, chief scientist at the Army Research Laboratory, has observed, "[t]he actions of human actors teaming with robots and other intelligent agents will be pervasive in the complex operational environments of the future."[16] In other words, human–machine interaction will no longer be limited to training scenarios: We have reached the point at which we will need to use machines to help us learn how to use machines.

The Marine Corps may be leading the way toward this brave new world. War-gaming experts at Quantico, Virginia, are working on what they call the Next Generation Wargame (NGW). The NGW will attempt to leverage narrow applications of artificial intelligence for "in-stride adjudication," which would allow a war game to unfold without the traditional "turns." This would literally be a game changer, allowing war games to replicate the temporal aspects of conflict, which is increasingly relevant in an age of AI, hypersonics, and speed-of-light weapons.

The other services are taking steps in the right direction.

- The Army's Center for Army Analysis (CAA), the Army War College, and The Research and Analysis Center (TRAC) at Fort Leavenworth are leading the Army's war-game innovation efforts. They are incorporating all domains into the Army's models and evaluating various scenarios against potential adversaries.

- The Army Capabilities Integration Center (ARCIC) has been renamed the Futures

and Concepts Center and absorbed into a major new Army Futures Command. Supported by CAA and TRAC, the Futures and Concepts Center has been involved in selecting and war-gaming potential future technologies for ground combat. The results will be used to conduct additional, more detailed modeling.

- The Air Force Research Laboratory and LeMay Center are leading the charge for the Joint Force in the development of Joint All Domain Command and Control (JADC2).

- The Navy's Center for Naval Analysis (CNA) uses the same model as the one used by CAA, which is called the Joint Wargame Analysis Model (JWAM), another indicator of joint thinking among the services.

- The granddaddy of all war-gaming centers, the Naval War College Wargame Center, continues to refine its methods. While it has retained analysis of competing hypotheses as the core of its methodology, the Wargame Center is now using technology to enable joint, semi-autonomous forces.

Another step in the right direction is the Army's attempt to help bridge the gap between the military and industry by repurposing one if its reserve component training commands. The 75th Innovation Command's mission is to drive "operational innovation, concepts, and capabilities to enhance the readiness and lethality of the Future Force by leveraging the unique skills, agility, and private sector connectivity of America's Army Reserve."[17] These efforts can help to connect the civilian gaming "ecosystem" with the military's war-gaming ecosystem. The latter is a robust community of practice spread across the services, which are busily refining their models to include all six domains of warfare and applying themselves to the challenges of future conflict.

At the 2018 meeting of the National Training and Simulation Association, Tony Cerri, then Director of Data Science, Modeling and Simulation for the Army's Training and Doctrine Command G2, said that "if we can marry big data and AI with [modeling and simulation]...that's an unbeatable advantage."[18] Cerri is right, of course, but the converse of his statement is also true. Russia and China are investing vast amounts of money in AI with the aim of achieving superiority over the U.S. by 2030 in what they perceive to be a strategically important field. If our adversaries can experiment more realistically, faster, and less expensively than we can, there is no denying that we will be at a competitive disadvantage against them.

As stated previously, Russia has been joined by China as a peer threat to the United States, and we will need more sophisticated models if we are to understand the nature of the challenge that each poses. Chess, which requires the player to think multiple moves in advance to win, is a popular game in Russia. Not so in China, where a game called Go—based on deception and encirclement rather than direct attack—is preferred. In the early days of AI, IBM's Deep Blue learned to play chess well enough to defeat grandmaster Gary Kasparov in 1997. It took nearly two more decades before Google's AlphaGo was able to teach itself how to win against the world's top Go player, Lee Sedol of South Korea. In fact, it learned so well that Lee retired after the match.

Chris Nicholson, founder of a deep-learning startup, said at the time, "You can apply [this software] to any adversarial problem—anything that you can conceive of as a game where strategy matters. That includes war...."[19] It seems the Russians and Chinese have figured this out. We must as well.

A Guiding Hand

The MS&G community is spread across the Department of Defense. In some ways, this is a strength as it has led to a large and diverse community of interest, but it also hinders our ability to share information and act efficiently. Within OSD, the Office of Net Assessment

(ONA) conducts war games to see decades into the future, and Cost Assessment and Program Evaluation (CAPE) uses models to evaluate alternative capabilities and force structures. Responsibility for coordinating the development, validation, and verification of modeling and simulation software rests with a small organization called the Defense Modeling and Simulation Coordination Office (DMSCO). Within the Joint Staff, both the J7 and J8 conduct modeling and simulation. Naturally, each service has its own requirements and capabilities for MS&G.

Meanwhile, our closest allies are experimenting too. The European Defense Agency is studying the applications of AI and big data in training and simulations and using war gaming to analyze how to deal with complex scenarios such as hybrid warfare. There are many other examples.

Unfortunately, we no longer have JFCOM to bring all these efforts together to acquire the necessary resources and make the necessary changes to develop JADO. So who can coordinate interservice MS&G development to enable better, faster, and less expensive experimentation through war gaming? Who can ensure that we are taking full advantage of America's edge in commercial software innovation? Who can find the right applications for big data, artificial intelligence, and cloud computing for MS&G? And who will spearhead the joint DOTMLPF-P effort needed to implement JADO? Important changes that have been made indicate that the Joint Chiefs of Staff, supported by OSD and the services, could succeed in leading the charge. There are at least two reasons for optimism.

First, the J7 is not attempting to experiment alone. The Vice Chairman of the Joint Chiefs of Staff is an essential player in turning JADO into a fully developed and resourced joint warfighting doctrine. In his traditional role as chairman of the Joint Requirements Oversight Council (JROC), the VCJCS has embraced the original intent of the 1986 Goldwater–Nichols Act and is using his position to push more of a top-down acquisition process in support of JADO. General Hyten said that the JROC will set its attributes and "the services will build to those" attributes, flipping the current bottom-up acquisition approach to one in which the Joint Chiefs "send[] a 'demand signal' to the services."

> The service then will be responsible for building the pieces and coming back to us, and then we have to make sure it fits all together.... That's what the JROC is *supposed* to do, [but] that is something we haven't done yet....

The JROC tended to be a receiver of requirements from services, not a generator of requirements for the services to meet.... That's not what was intended by Congress when it was established, by the processes we put in place, but that's what we've come to. And so that's going to require some discipline at the senior level to make sure that we are actually putting the demand signal out.[20]

If General Hyten applies this thinking to MS&G research, design, and development, the U.S. will be able to develop the right capabilities to experiment with JADO concepts and systems.

Second, and just as important, General Hyten said that he will try to steer the JROC away from being overly prescriptive, which can increase program costs and cause delays. Rather, he sees the council's role as blessing "the attributes of the capabilities that we need to have and then monitor[ing] the service's ability to build that."[21]

This is an important acknowledgment, as no one solution fits all domains equally well. The Army and Marine Corps tend to operate in dirtier environments than do the Navy and Air Force, while the Army has the additional requirement that it be able to scale any solutions to accommodate a force that is much larger than the other services. A continuous flow of information and feedback through the JROC members is the only way these concerns can be resolved. The approach will also allow these MS&G capabilities to evolve more quickly.

That said, the VCJCS and J7 will need some help from OSD, the services, industry, and our allies. Recently, the U.S. Army created its first new four-star command in a generation, the Army Futures Command, to lead its modernization efforts. The reactivation of JFCOM is unrealistic and perhaps even unnecessary, but a joint counterpart for AFC, an all-domain experimentation joint task force (ADE JTF) led by a four-star general or admiral, would be able to focus exclusively on acquiring the resources and generating the momentum needed to realize JADO's full potential. It would be able to supervise the efforts of the JADO cross-functional team and the services' studies of its four "orphan" functions. It could address policy issues with interagency partners, collaborate with allies, and coordinate the efforts of OSD with those of the services. It could distribute experiments between exercises and war games, perhaps even sponsoring some of the latter, and serve as the repository for their results. The J7 is already doing much of this, and the purpose of the ADE JTF would not be to replicate its role, but rather to complement and support it.

Conclusion

A radically new approach to joint acquisition is already underway. If it is supported by an organization dedicated to joint experimentation with the necessary resources and authorities, perhaps the U.S. can avoid the multi-domain equivalent of the surprise we encountered at Okinawa. As Admiral Nimitz conceded, the Plan Orange war games failed to anticipate the Japanese kamikaze attacks that cost the U.S. Navy dearly at Okinawa, sinking 34 ships, damaging 368 others, killing 4,900 sailors, and wounding nearly 5,000 more.

Perhaps someday, a future American commander may be able not only to paraphrase Admiral Nimitz and say that our Joint All Domain Operation Doctrine and Plans were enacted in games and exercises throughout the Defense Department and around the world by so many people and in so many different ways that nothing that happened during the war was a surprise, but also to exceed Nimitz's boast and say that this *included* the enemy's asymmetric cross-domain tactics toward the end of the war. More important still, robust joint experimentation may allow the United States to avoid the Thucydides Trap entirely.

Endnotes

1. Chester W. Nimitz, Fleet Admiral, U.S. Navy, speech to Naval War College, October 10, 1960, Folder 26, Box 31, RG15 Guest Lectures, 1894–1992, Naval Historical Collection, Naval War College, Newport, Rhode Island; quoted in John M. Lillard, "Playing War: Wargaming and U.S. Navy Preparations for WWII," PhD dissertation, George Mason University, October 1, 2013, p. 1, http://mars.gmu.edu/bitstream/handle/1920/8747/Lillard_gmu_0883E_10462.pdf?sequence=1&isAllowed=y (accessed August 19, 2020).
2. Graham Allison, "The Thucydides Trap: Are the U.S. and China Headed for War?" *The Atlantic*, September 24, 2015, https://www.theatlantic.com/international/archive/2015/09/united-states-china-war-thucydides-trap/406756/ (accessed June 2, 2020).
3. Michael Pillsbury, *The Hundred-Year Marathon: China's Secret Strategy to Replace the United States as the Global Superpower* (New York: Henry Holt, 2015).
4. Eric Schmitt, "Iraq-Bound Troops Confront Rumsfeld over Lack of Armor," *The New York Times*, December 8, 2004, https://www.nytimes.com/2004/12/08/international/middleeast/iraqbound-troops-confront-rumsfeld-over-lack-of.html (accessed August 14, 2020).
5. Micah Zenko, *Red Team: How to Succeed by Thinking Like the Enemy* (New York: Basic Books, 2015), pp. 52–61.
6. Naval News Staff, "U.S. Navy Sets New Squadron for Emerging Surface Warfighting Capabilities Development," *Naval News*, May 27, 2019, https://www.navalnews.com/naval-news/2019/05/us-navy-sets-new-squadron-for-emerging-surface-warfighting-capabilities-development/ (accessed July 29, 2020).
7. Frank Lewis Dyer, Thomas Commerford Martin, and William Henry Meadowcroft, *Edison: His Life and Inventions* (New York: Harper & Brothers, 1929), p. 200.
8. Robert C. Rubel, Appendix 1, "Wargaming Pathologies," in Christopher A. Weuve, Peter P. Perla, Michael C. Markowitz, Robert Rubel, Stephen Downes-Martin, Michael Martin, and Paul V. Vebber, *Wargame Pathologies*, Center for Naval Analysis, CRM D0010866.A1/Final, September 2004, pp. 45–55, https://www.cna.org/CNA_files/PDF/D0010866.A1.pdf (accessed June 16, 2020), and Appendix 2, "Stephen Downes-Martin's List of Pathologies," in ibid., pp. 57–58.
9. Paul K. Davis and Donald Blumenthal, "The Base of Sand Problem: A White Paper on the State of Military Combat Modeling," RAND Corporation, *RAND Note* No. N-3148—OSD/DARPA, 1991, p. v, https://www.rand.org/content/dam/rand/pubs/notes/2005/N3148.pdf (accessed June 16, 2020).
10. Govini, *Department of Defense Artificial Intelligence, Big Data and Cloud Taxonomy*, 2017, p. 7, https://en.calameo.com/read/0000097792ddb787a9198 (accessed June 16, 2020).
11. Shawn Woodford, "Wargaming Multi-Domain Battle: The Base of Sand Problem," Dupuy Institute Mystics & Statistics Blog, January 11, 2019, http://www.dupuyinstitute.org/blog/2019/01/11/wargaming-multi-domain-battle-the-base-of-sand-problem/ (accessed June 16, 2020).
12. Robert Work, Deputy Secretary of Defense, Memorandum for Secretaries of the Military Departments, Chairman of the Joint Chiefs of Staff, Under Secretaries of Defense, Vice Chairman of the Joint Chiefs of Staff, Chiefs of the Military Services, Chief of the National Guard Bureau, Commanders of the Combatant Commands, Director, Cost Assessment and Program Evaluation, Director of the Defense Intelligence Agency, and Director, Net Assessment, "Subject: 'Wargaming and Innovation,'" February 9, 2015, p. 1, https://news.usni.org/2015/03/18/document-memo-to-pentagon-leadership-on-wargaming (accessed June 16, 2020).
13. Robert Work and Paul Selva, "Revitalizing Wargaming Is Necessary to Be Prepared for Future Wars," War on the Rocks, December 8, 2015, https://warontherocks.com/2015/12/revitalizing-wargaming-is-necessary-to-be-prepared-for-future-wars/ (accessed June 16, 2020).
14. Jared Serbu, "Pentagon's Number-Two Officer Vows to Fix Software Acquisition 'Nightmare,'" Federal News Network, January 21, 2020, https://federalnewsnetwork.com/defense-main/2020/01/pentagons-number-two-officer-vows-to-fix-software-acquisition-nightmare/ (accessed June 16, 2020).
15. Unified Quest, unclassified "Unified Quest 2018 Deep Future Wargame Summary Report," http://arcic-sem.azurewebsites.us/App_Documents/UQ/Unified-Quest-18-Deep-Future-Wargame-Summary-Report_FINAL.PDF (accessed June 16, 2020).
16. Alexander Kott, "The Artificial Becomes Real," U.S. Department of Defense, Defense Visual Information Distribution Service, January 30, 2018, https://www.dvidshub.net/news/263969/artificial-becomes-real (accessed June 16, 2020). See also Alexander Kott, "Intelligent Autonomous Agents are Key to Cyber Defense of the Future Army Networks," *The Cyber Defense Review*, Vol. 3, No. 3 (Fall 2018), pp. 57–70, https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Fall%202018/KOTT_CDR_V3N3.pdf?ver=2018-12-18-101632-597 (accessed June 16, 2020).
17. U.S. Army Reserve, 75th Innovation Command, "Mission," https://www.usar.army.mil/75thIC/ (accessed June 16, 2020).

18. Yasmin Tajdeh, "Big Data, AI to Advance Modeling and Simulation," *National Defense*, January 3, 2018, https://www.nationaldefensemagazine.org/articles/2018/1/3/big-data-ai-to-advance-modeling-and-simulation (accessed June 16, 2020).
19. Cade Metz, "In a Huge Breakthrough, Google's AI Beats a Top Player at the Game of Go," *Wired*, January 27, 2016, https://www.wired.com/2016/01/in-a-huge-breakthrough-googles-ai-beats-a-top-player-at-the-game-of-go/ (accessed June 16, 2020).
20. Colin Clark, "Hyten: All Domain Drives Requirements Shakeup," *Breaking Defense*, February 20, 2020, https://breakingdefense.com/2020/02/hyten-all-domain-drives-requirements-shakeup/ (accessed June 16, 2020).
21. Ibid.

Building Resilience: Mobilizing the Defense Industrial Base in an Era of Great-Power Competition

Jerry McGinn, PhD

Increasing national security concerns about China's military capabilities and mercantilist economic policies, the growth of commercial technologies like artificial intelligence and robotics, and now a global pandemic have put a spotlight on the U.S. defense industrial base. A robust, secure, and resilient defense industrial base has been an important national priority in recent years. High-level reviews, increased investments, new legislative authorities, and efforts to encourage new entrants have been undertaken to grow and strengthen this industrial base.

How are we faring? Does our industrial base have enough capability and capacity for this era of strategic competition? And how resilient would our industrial base be in response to a national emergency?

The response to the current COVID-19 pandemic has given us a partial answer to these questions. Although the public health focus is obviously different from a military threat, the tools and authorities that are available to respond to this national emergency are essentially the same. Despite the glaring weaknesses in our public health supply chain that the pandemic has exposed, and despite the initially chaotic (albeit massive) response from government agencies and companies across the country, the ability of the U.S. to mobilize its industrial base to meet national emergencies has improved significantly. There is, however, still much work to be done.

Examining how the defense industrial base has mobilized to meet crises from the 20th century to more recent efforts, including the response to COVID-19, can help us to separate fact from myth and start to identify best practices for the future.

Nature and Structure of the U.S. Defense Industrial Base

The defense industrial base is an essential element of the country's national security and can even be considered a central component of the military force structure. The industrial base develops and produces systems and provides services that enable our warfighters to protect our homeland and to deter and defeat adversaries on the ground, at sea, in the air and space, and in cyberspace.

The defense industrial base is comprised principally of private and publicly traded companies that range widely in size and composition. In general, these firms fit within three major categories:

- A small number of large companies that serve as prime contractors and integrators on major weapons systems;

- A larger number of mid-tier companies that manufacture major subsystems or provide technical services to Department of Defense (DOD) customers; and

- A very large number of small companies that manufacture spare parts or provide material serving both commercial and defense customers, serve as nontraditional start-ups developing innovative technologies, or are focused on a particular defense segment or customer set.

All told, the number of firms that contribute in some way to the U.S. industrial base likely well exceeds 100,000, according to Vice Admiral David Lewis, director of the Defense Contract Management Agency.[1] These firms all work closely with government customers to field capabilities for the national defense.

In addition to these private and publicly traded companies, there is a much smaller component of government-owned facilities that produce and service systems: the organic industrial base. These facilities include shipyards, arsenals, maintenance depots, and ammunition plants.[2] Their capabilities include the expertise to "perform deep repair, the means to provide repair parts to the shop floor, and the ability to deliver repaired systems to the time and place of the fight [that] accompanies every military ship, plane, vehicle, and weapon."[3]

The "reemergence of long-term strategic competition" with China and Russia articulated in the 2017 National Defense Strategy (NDS) has led to substantial changes in DOD investment priorities that have shaped the efforts and even the composition of the defense industrial base. The NDS further notes that "[m]aintaining the Department's technological advantage will require changes to industry culture, investment sources, and protection across the National Security Innovation Base."[4] The term "National Security Innovation Base" was introduced in the 2017 National Security Strategy to reflect the broad "network of knowledge, capabilities, and people" that "protects and enhances the American way of life."[5]

The NDS definitely reinforced the emphasis on increasing the number of commercial entrants in the defense industrial base that had begun with efforts such as the Defense Innovation Unit (DIU), self-described as a DOD organization that "strengthens our national security by accelerating the adoption of commercial technology throughout the military and growing the national security innovation base." Specifically, "[w]ith offices in Silicon Valley, Boston, Austin, and the Pentagon, DIU connects its DoD partners with leading technology companies across the country."[6] The military departments have launched similar initiatives such as AFWERX and Army Futures Command.[7] The overall thrust of these efforts has been to focus on commercial innovation because that is the nature of such key NDS technology focus areas as artificial intelligence, robotics, autonomy, and quantum computing.

Whatever its ultimate composition, the defense industrial base must have the ability to mobilize to meet the country's national security needs. This mobilization is driven by three principal components:

- **Capability.** Do we have the defense industrial capabilities we need? Are we investing in the right technologies and building the systems necessary to face both current and future national security challenges?

- **Capacity.** How much redundancy and industrial capacity are appropriate? Are we developing enough manufacturing competency to meet surge requirements in the event of protracted conflict?

- **Resilience.** How can the United States fully mobilize the capabilities and capacities of the defense industrial base to meet future contingencies? How quickly, for example, can we ramp up production lines or adjust to emerging industrial requirements in the middle of a major crisis?

All three components are crucial. None of them is fixed, of course. Any of these components can be increased or decreased through attention and resources. At the same time, however, getting the balance of capabilities and capacities right is key because it takes time to change direction. As former Secretary of Defense Donald Rumsfeld famously quipped, "You go to war with the army you have, not the army you might want or wish to have at a later time."[8]

The key outcome of this balance of capability and capacity is resilience. Resilience determines whether the defense industrial base can ultimately produce and deliver in response to a true national crisis. Let us examine how the defense industrial base has performed over time to put that balance in context.

Mobilization in the 20th Century

World War I. By the start of the 20th century, the United States had become a true industrial power. In the early 1900s, U.S. industrial capacity surpassed that of major European powers like the United Kingdom, France, and Germany, but the United States was focused solely on commercial enterprises, and there was very little defense-focused industrial capacity apart from a limited number of arsenals and shipyards.[9] As tensions in Europe grew and war approached, countries formed alliances and began to mobilize their industries to build rifles, trucks, artillery, airplanes, and other vehicles. Barbara Tuchman's riveting account of German and other European military planners' detailed mobilization plans in preparation for war in her famous work *The Guns of August* vividly depicts this mobilization.[10]

This high state of alert was certainly not present in the United States in 1914, when the Army was a very modest force of just over 127,000 soldiers and there was little appetite for war. In fact, President Woodrow Wilson won reelection in 1916 in large measure because of his slogan, "He Kept Us out of War."[11]

That changed in 1917 when the United States entered World War I. Businesses and business leaders stepped forward dramatically to help the war effort. This is illustrated most notably by the War Industries Board (WIB). The WIB was an emergency agency created and largely led by industry executives—so-called dollar-a-year men—on loan from their respective companies to help oversee war production. While private enterprise played a significant role in war mobilization, this rapid effort also included some heavy government intervention such as an "excess profits tax." In addition, the government exercised what historian Mark Wilson calls "government coercion" and assumed control of private enterprises like Smith & Wesson for periods of time to overcome labor disputes or to direct production.[12]

The results of these efforts were significant. The crash mobilization efforts ultimately succeeded in building a sufficient number of cargo ships to move all of the men and materials needed for the war, including 2 million rifles, 80,000 trucks, and 12,000 airplanes, in less than two years. Unfortunately, however, most of this equipment arrived too late. General John J. Pershing's American Expeditionary Forces, totaling almost 2 million men, used a fair number of British rifles and machine guns as well as French airplanes during the Great War. As Arthur Herman notes in his dramatic account (devoted principally to World War II mobilization), "Of the 10,000 75mm artillery pieces the War Department ordered, only 143 ever reached the front—and not one American-made tank."[13]

After the November 1918 Armistice, the United States quickly dismantled the WIB in 1919, and the industrial base returned to its prewar focus. The Great War experience, however, did significantly inform American mobilization efforts in World War II.

World War II. The United States watched during the 1930s as tensions again rose in Europe. Domestic attitudes remained hostile toward involvement in another European war, and American industrial efforts reflected that posture of neutrality. President Franklin D. Roosevelt, who had served as Assistant Secretary of the Navy during World War I, clearly

TABLE 1

Comparing Peacetime and Wartime Production During World War II

Product	Prewar Baseline Output	Wartime Peak Output	Peak/ Baseline
Synthetic rubber	3,200 long tons (1940)	922,000 long tons (1945)	288.1
Aviation gasoline	4,000 barrels/day (June 1940)	520,000 barrels/day (March 1945)	130
Merchant ships	0.3 million dw tons (1939)	18 million dw tons (1943)	60
TNT	100,000 lbs./day (June 1940)	4 million lbs./day (Dec. 1942)	40
Airframes	20.3 million lbs. (1940)	797.1 million lbs. (1944)	39.3
Magnesium	12 million lbs. (1940)	368 million lbs. (1943)	30.7
Aluminum	327 million lbs./year (1939)	2.3 billion lbs./year (late 1943)	7
Electric power	28 million kilowatts (1940)	44 million kilowatts (April 1944)	1.6
Steel	82 million net tons (1940)	96 million net tons (1945)	1.2

SOURCE: Mark R. Wilson, *Destructive Creation: American Business and the Winning of World War II* (Philadelphia: University of Pennsylvania Press, 2016), p. 79.

heritage.org

recognized the domestic political constraints, but he benefited from the need of the British and French governments to buy aircraft and ships in the late 1930s to confront the growing Nazi threat.

Congress passed the $1.1 billion Fleet Expansion Act in May 1938 to address these international orders as well as increasing domestic orders for ships.[14] Although the United States continued to remain neutral after war began in Europe in September 1939, the need for increased industrial mobilization had become clear. In May 1940, General George C. Marshall, the U.S. Army Chief of Staff, convinced President Roosevelt to increase the Army's 1940 appropriation request dramatically from $24 million to $700 million.[15] These significant actions helped to create the conditions for "the great arsenal of democracy" that Roosevelt famously announced as his goal for America in a December 1940 fireside chat.[16]

This arsenal would be built by a diverse set of characters that represented an underappreciated cohort of the Greatest Generation. They included new dollar-a-year men like General Motors President Bill Knudsen, known as the "Big Dane," who resigned his position after a phone call from President Roosevelt in mid-1940 requesting that he come to Washington; industrialists such as the colorful Henry Kaiser, a high school dropout who became a production wizard; government officials such as former cotton broker and head of the Reconstruction Finance Corporation Jesse H. Jones; and even New Dealers such as the President's close adviser Harry Hopkins.[17]

Despite often being at odds with one another, these leaders achieved tremendous results in establishing industrial capacity in such areas as materials, steel, ships, tanks, and aircraft. They directed or oversaw significant government investment through the alphabet soup of government organizations created during the war such as the War Production Board, its successor Office of Production Management, the Reconstruction Finance Corporation, and many more. Success was accomplished principally through public investment to create new shipyards and manufacturing plants that were run by private companies. These

government-owned and contractor-operated (GOCO) facilities were the largest investment in manufacturing capacity during the war and became a successful business model that continues today.[18]

Most important, these GOCOs produced. As Knudsen and his successor, former Sears, Roebuck executive Don Nelson, worked with the President to establish ambitious production goals each year, the base would inevitably meet and exceed these goals. The sheer numbers and scale are breathtaking. Mark Wilson's analysis lays out the magnitude of this increase in Table 1.

This level of production simply swamped that of America's adversaries. "In 1943," notes Arthur Herman, "American war production was twice that of Germany and Japan combined."[19]

The private-sector companies that produced the output of the arsenal represented all aspects of American manufacturing. The largest government contractors were major existing businesses like Bethlehem Steel, Chrysler, General Motors, Ford, Sperry Gyroscope, and Wright Aeronautical, which expanded or modified their production lines to support the war effort.[20] Thousands of other small and mid-size companies similarly converted their operations or were formed to meet the tremendous war demand. Among the most dynamic and innovative sectors during the war was aircraft manufacturing, with such companies as Lockheed Aircraft, the Curtiss-Wright Corporation, the Glenn L. Martin Company, the Allison division of General Motors, Pratt and Whitney, Boeing, and the fledgling Grumman Aircraft in Long Island, New York, producing aircraft and engines throughout the war.[21]

Not surprisingly, though, there were at times significant challenges in this mobilization. Government seizures of companies, labor unrest, and tensions between government and industry over price controls and profit margins were also regular features during the war.[22] Numerous production efforts struggled or spectacularly failed. The B-29 superbomber, for example, was a tremendous struggle for prime contractor Boeing, government program managers, and the defense industrial base, but through the persistent efforts of all involved, the B-29 came into service and at the end of the war played a pivotal role that included dropping atomic bombs on the Japanese cities of Hiroshima and Nagasaki.[23]

The extraordinary results of the overall effort, however, speak for themselves. When the war ended, the United States was undeniably the world's principal industrial power. But the end of the war also led to rapid demobilization of the armed forces and the start of industrial "reconversion." The government disposed of many GOCOs through privatization, a trend that continued across the defense sector.[24] That, plus conflict on the Korean Peninsula and the onset of the Cold War, helped to shape the defense industrial base for the remainder of the 20th century.

Korea and the Defense Production Act. The Soviet establishment of puppet regimes in Eastern Europe in the aftermath of World War II and the North Korean invasion of the South in 1950 led Congress to enact the Defense Production Act (DPA), which was modeled on the authorities of World War II. President Harry S. Truman used the DPA principally to prioritize and direct production efforts. He continued, for example, the practice of government seizures of private companies, although this practice came to an end after the Youngstown steel strike of 1952. Concerned about the impact of the strike on the war effort, the President issued an executive order in April to force the steel mills to stay open. The Supreme Court, however, ruled that Truman's seizure of the steel industry was unconstitutional.[25]

Despite the Supreme Court ruling, the DPA took shape over time. The law gave the President broad authority to ensure the timely availability of essential domestic industrial resources to support defense requirements. Congress continued to reauthorize three of the original DPA titles, which were used regularly throughout the Cold War and in the decades following the fall of the Berlin Wall.

- Title I is focused on the distribution and allocation of goods and services. The distribution authority of Title I permits the government to prioritize contracts to meet priority government needs. The Defense Prioritization and Allocation System (DPAS), overseen by the Department of Commerce, uses this authority regularly to prioritize orders and rate contracts to meet government-mandated critical infrastructure requirements.[26]

- The allocation authority of Title I permits the government to prioritize industrial efforts to meet national defense priorities. This authority was rarely used in the aftermath of the 1952 steel strike, but it was central to the establishment of the Civil Reserve Air Fleet (CRAF). CRAF, managed by the Department of Transportation, gave the President the ability to mobilize specific aircraft for government use in the event of national emergency.[27] CRAF planning efforts focused for example, on surge requirements to deploy U.S. troops and equipment to Europe to help the North Atlantic Treaty Organization (NATO) defend Europe in the case of Soviet military aggression.

- Title III focuses on the ability to "create, maintain, protect, expand, or restore industrial base capabilities essential for national defense" through grants, loans, purchases, and purchase commitments.[28] The President delegated authority to the Department of Defense to manage this authority. Over time, Title III became focused almost exclusively on grants—principally congressional earmarks—to increase industrial capacity in areas of industrial base weakness such as complex forgings for naval propulsion shafts and the creation of a domestic production facility for beryllium.[29]

- Title VII focuses on voluntary agreements between the private sector and government to "help provide for the national defense" in times of crisis.[30] Only one voluntary agreement on the maritime industry currently exists, and it is managed by the Department of Transportation. Foreign direct investment is also covered under Title VII and is governed by the Committee on Foreign Investment in the United States (CFIUS). CFIUS is an interagency committee that, led by the Department of the Treasury, reviews foreign investment transactions for national security concerns. CFIUS was added to Title VII in 1988 through the Exon–Florio amendment to the DPA but received little public attention until the Dubai Ports transaction in 2007.[31] This transaction, which proposed the foreign purchase of six U.S. ports, led Congress to pass the Foreign Investment and National Security Act to create CFIUS in statute.[32]

Industrial Base and Industrial Policy Trends. The privatization of the defense industrial base (which President Dwight D. Eisenhower famously dubbed the military–industrial complex in his 1961 farewell address) continued during the Cold War.[33] Throughout decades of East–West confrontation, dozens of major defense contractors developed ships, aircraft, and ground vehicles for the Department of Defense.

The existential threat of nuclear war and the militarized border between NATO and Soviet bloc forces led to a consistently large U.S. defense budget—generally over 5 percent of gross domestic product—throughout the Cold War.[34] This changed dramatically after the fall of the Berlin Wall and Secretary of Defense William Perry's "Last Supper" meeting with major defense company CEOs, which sparked a significant round of industrial consolidation within the defense sector as budgets declined after the Cold War ended.[35]

Inside government, meanwhile, there was little coordinated focus on industrial policy or planning. The Office of War Mobilization, which performed this function during World

War II, was abolished immediately after the war. President Truman created a comparable entity, the Office of Defense Mobilization, during the Korean War, but President Eisenhower greatly reduced the stature of this office in favor of a market approach.[36]

Much of this was purposeful because of long-standing American bias against industrial policy. As the late Jacques Gansler noted, "[t]he U.S. economy is built on the strong assumption of the benefits of free-market operation and has long been averse to industrial planning, even in the defense sector."[37] Unlike Cold War adversaries like the Soviet Union and China, the United States did not put great stock in five-year plans to achieve industrial results. Instead, U.S. leaders believed that, much like the perceived experience during World War II, the dynamic nature of the U.S. economic system and the strength of the overall industrial base would be able to respond to any national crisis.

Mobilization in the 21st Century

As the nation moved into the second decade of the 21st century, national security officials began to rethink many of their assumptions about mobilization and the defense industrial base.

Post-9/11 Conflicts and the MRAP. The conflicts in Afghanistan and then Iraq in the wake of 9/11 spurred industrial mobilization efforts that were substantially different from those that had arisen in response to previous conflicts. During the early 2000s, most of the industrial base focused on developing capabilities to fight insurgents.

Particularly in Iraq, improvised explosive devices (IEDs) became the greatest threat to American forces. U.S. armored vehicles had been very effective in toppling the Taliban and Saddam Hussein regimes but were much less suited to protecting soldiers against IEDs. Large and small companies focused on developing systems to counter IEDs as well as additional force protection for individuals and vehicles. Overall, the defense industrial base was up to the task, developing more advanced body armor for soldiers and additional armor for vehicles. DPA Title I was even used to help prioritize the production of body armor.[38] Despite these improvements in force protection, however, deaths from IEDs continued to mount.

The Mine-Resistant, Ambush-Protected Vehicle (MRAP) ultimately became the force protection solution for American forces, but its development and deployment were not without challenges. As James Hasik points out in his forthcoming book, the foremost challenge with respect to the MRAP was getting it established as a true acquisition priority. The MRAP was a radical departure in armored vehicle design, and it competed with other priorities.

Prioritization changed with the arrival of Robert Gates as Secretary of Defense in 2007, but challenges to the industrial base were not insignificant. There were initial industrial bottlenecks for ballistic glass, axles, tires, and spare parts, but the biggest challenge was steel plate. With extremely limited domestic capacity to produce steel plate for the MRAP, DOD qualified foreign-owned and foreign sources to meet the demand. Secretary Gates also used the highest DPA Title I DPAS rating, DX, to prioritize steel plate procurement. Eventually, these challenges were overcome, and tens of thousands of MRAPs were produced and delivered to Iraq, contributing significantly to the dramatic reduction in IED casualties by 2008.[39]

Sharpening Focus on the Defense Industrial Base. The proliferation of high-tech commercial technology and the shifting of manufacturing and production to meet the demands of the global economy have had tremendous economic benefits for the United States and countries around the world, but they also have given rise to trends and practices that would be problematic in war. The limits of these approaches, which include just-in-time manufacturing and global supply chain optimization, became increasingly visible in the defense industrial base as the country entered the second decade of the new century and troop levels in the Middle East decreased.

While national security priorities and Buy America laws ensured that the vast majority of the development and production of defense

systems occurred in the United States, the production of some critical subcomponents and materials migrated overseas. DOD's annual *Industrial Capabilities* reports to Congress identified many of these weaknesses in the industrial base.[40] They noted, for example, that the production of microelectronics and materials such as rare earth elements as well as specialty chemicals and energetics used in explosives were increasingly produced only outside of the United States—in some cases, almost exclusively in China. These components and materials are used overwhelmingly for commercial purposes in electronics such as computers and smartphones, but they also are essential components in critical advanced defense systems such as radars and precision-guided munitions (PGMs).

The short-lived 2010 Chinese embargo of rare earth elements following the Japanese seizure of a Chinese fishing vessel brought attention to the dominant position that China had achieved, largely through state industrial policy, in rare earth mining and processing. Although the crisis quickly passed, the lack of U.S. domestic rare earth capacity and consequent dependence on a foreign source of supply remained.[41]

DOD's focus on the industrial base sharpened during this period as a result. The Office of Industrial Affairs, which had been demoted in stature in the early 2000s, was elevated and eventually strengthened further in 2013 with the creation of the Office of Manufacturing and Industrial Base Policy (MIBP). In addition to the traditional focus on industrial base assessment, anti-trust reviews of defense-related mergers and acquisitions, and DPA Title III, the responsibility for CFIUS was transferred to MIBP. This reorganization and a direct-report relationship to the Under Secretary of Defense for Acquisition, Technology, and Logistics gave DOD a stronger focal point for industrial base analysis and mitigation efforts across the department.

This sharpened focus played a significant role in addressing the changing nature of foreign direct investment as the country of origin in CFIUS transactions began to shift substantially after 2010. From 2007–2009, for example, acquisitions originating from companies in the United Kingdom, Canada, France, Australia, and Israel—traditional U.S. allies—accounted for 57 percent of 358 covered transactions. Transactions originating from Chinese firms were less than 4 percent of the total. In less than a decade, those ratios shifted dramatically. From 2016–2018, transactions originating from China were the largest proportion of cases filed: 26.5 percent. Moreover, the nature of the Chinese transactions drew increased scrutiny because the vast majority of these proposed acquisitions (84 percent) were focused on the manufacturing, finance, information, and services sectors.[42]

This shift drew significant bipartisan congressional and executive branch concern about the impact of increased levels of Chinese ownership or control in such critical sectors of the industrial base as microelectronics. On August 13, 2018, the President signed into law the National Defense Authorization Act (NDAA) for Fiscal Year 2019, which included the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA).[43] FIRRMA was the most significant reform of CFIUS since the Foreign Investment and National Security Act (FINSA) of 2007 and helped to modernize national security reviews of financial transactions by "expand[ing] the scope and jurisdiction of CFIUS," refining CFIUS procedures, and requiring "actions by CFIUS to address national security risks related to mitigation agreements."[44]

2017–2018 White House Defense Industrial Base Review. The galvanizing point for sustained action in the defense industrial base was the 2017–2018 whole-of-government review launched by President Donald J. Trump's Executive Order 13806, "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States," signed on July 21, 2017.[45] Initiated by the White House Office of Trade and Manufacturing Policy and led by the DOD Office of Industrial Policy, this interagency effort identified five macro forces shaping the

industrial base that included the decline of U.S. manufacturing capability and capacity as well as U.S. government business practices. These macro forces manifest themselves in what the final report called "risk archetypes" in the defense industrial base, ranging from single and sole sources of supply to fragile suppliers and markets as well as dependence on foreign suppliers and the erosion of U.S.-based infrastructure.[46]

The report reinforced many previous efforts, but one finding in particular—the "surprising level of foreign dependence on competitor nations"—stood out and became the focus for implementation.[47] Of principal concern were areas in which Chinese firms had become single or sole-source suppliers of critical materials well down the supply chain through mercantilist economic policies and general global supply chain trends. In response, the Administration initiated a significant number of DPA Title III and Industrial Base Analysis and Sustainment program projects to address these shortcomings. These resulted in Presidential Determinations and funding opportunities for capabilities such as small unmanned aerial systems, critical chemicals for missiles and munitions, and heavy and light rare earth separation and processing.[48]

Adapting the Defense Industrial Base to Meet NDS Objectives. The defense industrial base has been financially healthy for most of the past two decades with substantial defense budgets and strong market valuations in the wake of the 9/11 attacks, subsequent long-term military operations in the Middle East, and growing security threats from China and in cyberspace. The basic structure of the industry has similarly remained stable with a handful of large prime contractors that enjoy annual revenues exceeding $15 billion, a larger number of mid-tier companies that are major subsystems suppliers, and a much larger cohort of small businesses and component suppliers. Mergers and acquisitions have continued throughout the industrial base with the exception of consolidation among the top system integrators.

The NDS focus on renewed great-power competition led to significant changes in investment priorities across DOD. In addition to high-tech investment, the overall DOD budget increased, and existing major acquisition programs were overhauled to align with NDS objectives. After almost two decades focused on counterterrorism, however, there were questions about whether the defense industrial base would have the resilience for a rapid ramping up of production in complex major systems such as satellites, aircraft, and ships in the event of a crisis. As noted in the White House 13806 report and the annual industrial capability reports to Congress, there are numerous sectors of the industrial base, such as advanced radars, aircraft, shipbuilding, ground vehicles, and rocket motors, where there often are just two prime contractors.[49]

In addition to these efforts to add capability and capacity to the defense industrial base, there have been a number of initiatives to simplify and increase the speed of the DOD acquisition system. Congressional efforts through the NDAA in the past several years have created authorities, for example, to facilitate the greater use of Other Transactions Authority (OTA) contracts[50] and to create a middle-tier acquisition authority approach.[51] The rationale behind these changes has been to encourage greater innovation and more prototyping both in research and development and in major acquisition programs to help build resilience to meet the dynamic challenges of today's security environment. DOD has put together an Adaptive Acquisition Framework (AAF) to outline these and other "pathways" for acquisition professionals "to develop acquisition strategies and employ acquisition processes that match the characteristics of the capability being acquired" in support of the NDS.[52]

Supply chain security has been a persistent challenge in the defense industrial base. Beyond the entry of companies from adversary countries into lower levels of the supply chain, two principal challenges stand out.

The first of these challenges is supply chain visibility. DOD does its business through contracts with prime contractors, and those contracts hold the prime contractors accountable

for having their subcontractors deliver. As a result, DOD does not have direct visibility into the defense supply chain beyond the prime or tier-one or tier-two levels. Similarly, prime contractors do not have tremendous visibility beyond one or two levels further down the supply chain. Most of the time, this is not an issue, but in certain cases, it can be very difficult. In 2017, for example, a fifth-tier supplier that provided a voltage control switch used in PGMs was purchased, and a subsequent end-of-life buy was insufficient to meet operational demands.[53] This resulted in the rationing of PGMs being used in an operational theater at the time until a longer-term solution was devised.

The second persistent challenge is cybersecurity. The threat to U.S. national security secrets and the damage caused by intellectual property theft in the defense industrial base are well documented and have played a central role in the establishment of DOD's Cybersecurity Maturation Model Certification (CMMC) effort.[54] CMMC is being implemented in 2020 with the goal of full implementation by 2025.

With these changes in investment and in how DOD acquires goods and services, the question remained as to whether the defense industrial base could deliver in the event of major conflict. The unexpected COVID-19 pandemic early in 2020 has provided a partial answer.

The Response to COVID-19

In many ways, the current COVID-19 pandemic has been a testing ground for the ability of the U.S. industrial base to respond to a national emergency because, not surprisingly, the challenges to public health supply chains are similar in many ways to those faced by defense supply chains. For example, while innovation and research and development are strong domestically, the production of personal protective equipment (PPE) and many pharmaceuticals has largely moved offshore.

The limitations of this approach were exposed in the early days of the pandemic when media reports revealed that Chinese firms produce over 50 percent of the world's N95 masks and that they had temporarily halted their mask exports as the virus spread in China.[55] Furthermore, there was the troubling revelation that more than 90 percent of the global production of antibiotics also takes place in China.[56] Much like the White House defense industrial base review, the pandemic has demonstrated the problematic nature of dependent economic relationships with nontransparent economies and undemocratic countries like China for items of strategic importance.[57]

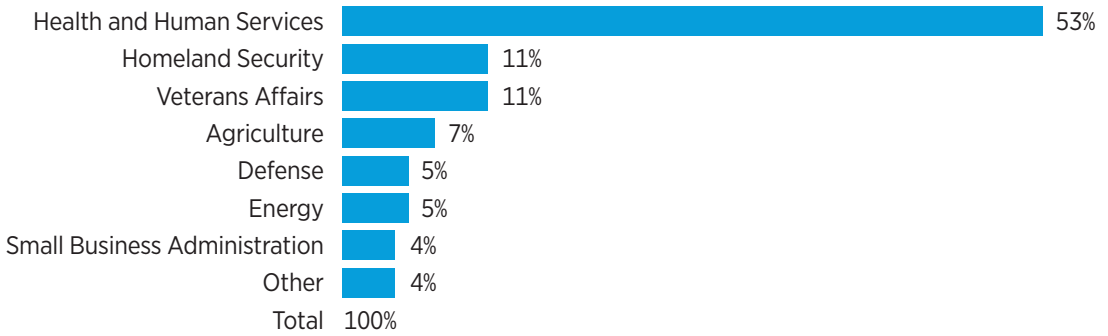
The initial federal response to the pandemic was chaotic, as it would be in any major crisis, but it was clear from the outset that the White House and all U.S. government agencies were pursuing an all-of-the-above approach to acquiring the PPE and equipment needed to treat COVID patients across the country. The Coronavirus Task Force and federal agencies led by the Department of Health and Human Services (HHS) worked with existing producers of ventilators and other health care equipment to surge production to unprecedented levels, and agencies began to release quick-turnaround—even same-day-response—solicitations to purchase PPE from all sources. Some also issued competitions to seek alternative solutions from suppliers that had never before produced health care equipment.[58] Meanwhile, White House advisers such as Director for Trade and Manufacturing Policy Dr. Peter Navarro got on the phone with leaders of commercial firms to find companies willing to adjust production efforts to develop additional sources of ventilators and PPE to meet the exploding number of COVID cases in late March.[59]

On March 13, the President announced that he was invoking the DPA's Title I distribution authority to enable HHS to speed the procurement of PPE and other items. The executive order gave HHS the authority to prioritize contracts and orders to meet national defense and emergency preparedness program requirements, specifically in the "areas of health and medical resources needed to respond to the spread of COVID-19, including personal

CHART 2

Federal Obligations Focused on COVID-19

SHARE OF TOTAL OBLIGATIONS AS OF JUNE 2, 2020, BY DEPARTMENT



NOTE: Department of Defense data are not fully represented due to standard 90–day lag in reporting.
SOURCE: Federal Procurement Data System–Next Generation, https://www.fpds.gov/fpdsng_cms/index.php/en/ (accessed July 10, 2020).

heritage.org

protective equipment and ventilators."[60] In short order, there were heated debates about whether the President should invoke the DPA Title I allocation authority to direct ventilator production—an action that he largely resisted.[61]

Debates about how various aspects of the DPA might be used in response to the public health crisis tended to dominate media reporting, but these masked the real work that was underway. Government agencies responded immediately to the pandemic by invoking emergency clauses in the Federal Acquisition Regulation (FAR) to delegate approval authority, increase the use of streamlined commercial contracting processes, and increase thresholds to help speed efforts.[62] Funding opportunities in such areas as 3D printing, biofabrication, and textiles[63] as well as collaborative projects between biomedical technology companies and the Army[64] also emerged rapidly. Companies across the spectrum responded to those opportunities to provide solutions during this time of crisis.

The results coming out of the industrial base were dramatic. In just the final week of March, federal obligations focused on COVID-19 rocketed from $636 million on March 24 to just shy of $2 billion by March 31.[65] Cumulative obligations reached over $7 billion as of April 21 and $14 billion by the start of June. Chart 2 breaks down these obligations by government agency.

The Coronavirus Aid, Relief, and Economic Security (CARES) Act further accelerated the immediate response and facilitated medium-term efforts to rebuild the domestic public health supply chain. For the longer-term resilience of that supply chain, the CARES Act added $1 billion to the DPA Fund and removed funding restrictions on individual Title III projects.[66] The tremendous infusion into the DPA Fund was its largest-ever appropriation, and some of these funds have already been used as the Administration has greatly accelerated Title III projects. Whereas, for example, it has taken 18 months to get rare earth Title III projects to the point of award, two COVID-19 pandemic-focused Title III projects, each over $120 million, have been started in less than a month utilizing those DPA funds.[67]

Most important, the impacts of these industrial base efforts were felt in the hospitals on the front lines of the fight against COVID-19. Despite frightening projections and spiking cases in early April, few hospitals suffered lasting shortages of PPE or ventilators, and numerous temporary field hospitals that were constructed were not even used for coronavirus patients.

Building Resilience: Lessons for the Future

COVID was an important testing ground in several aspects, but it was not as challenging to the defense industrial base as, for instance, the development of the B-29 or the atomic bomb were during World War II. Certainly, should the U.S. find itself in a longer-term conflict with an adversary such as China, the ability of our defense industrial base to respond to the destruction or disabling of our F-35 fighters or satellites would present a greater challenge. While DOD investment priorities and contracting approaches continue to prioritize capabilities and capacities focused on great-power competition, the essential question is whether we are building the real resilience that the nation requires to address today's—and tomorrow's—defense challenges.

Overall, our defense industrial base is well postured on at least two fronts.

- The basic authorities, regulations, structures, and tools available to government are solid. Despite some initial hiccups, this structure enabled an effective response to the multifaceted nature of the COVID-19 crisis. Many tools such as OTAs and DPA Title III that are supporting NDS priorities have similarly been deployed effectively during the current crisis.

- Companies across the spectrum are getting involved. Many commercial start-ups and nontraditional contractors engaged with DIU and AFWERX, and other DOD organizations immediately turned their efforts to support pandemic response efforts. One of those companies, for example, pursued and won a series of COVID-19 contracts that began in early April.[68]

There are still gaps and weaknesses that need to be addressed, however. The lack of robust capacity in areas of numerous industrial base sectors such as ground vehicles, shipbuilding, radars, and rocket motors, for instance, raises concerns for potential NDS contingencies. In these and other sectors, there is often one contractor with a preeminent market position and one or more other firms that struggle to keep up. Creating more opportunities for firms to compete for prototype contracts through middle-tier acquisition authority efforts or through OTAs, such as the Army is doing in its revamped timeline for the Optionally Manned Fighting Vehicle, is one way to build industrial capacity to meet NDS objectives.[69]

A recent analysis of the defense industrial base by a major defense trade association and fast-rising analytics firm gave the base a "C" grade based on "a business environment characterized by highly contrasting areas of concern and confidence."[70] Areas of concern included workforce, intermediate goods and services, and raw materials. While the middling overall grade is not terribly surprising, coming as it does from a trade association, it is very interesting to note that some of the highest scores in the report related to the industrial base's productive capacity and surge readiness.[71]

Turning back to the three components that are key for mobilizing the defense industrial base, there are several areas that are ripe for additional action in the coming months:

Capability

- Incentivizing new defense industrial base entrants will continue to be crucial. The trends in commercial technology are only accelerating, so DOD needs to continue to develop and scale business relationships with nontraditional suppliers.

- Eliminating industrial base dependence on China or another competitor nation

is imperative. Utilizing DPA Title III and other authorities or programs to address this dependence will be critical to enabling future crisis responses.

- Increasing the ability of companies and agencies to use rapid and flexible contracting mechanisms will be essential to successful responses to future crises. Carefully assessing the rugby scrum of contracting efforts used in the COVID-19 response, for instance, will help to determine which efforts are most successful at rapidly developing, producing, and delivering the needed capabilities at the needed time so that we are prepared for the future.

Capacity

- Developing DPA Title VII voluntary agreements could help to build the latent capacity of the defense industrial base to address future mobilization efforts.

- Prototyping efforts through OTAs as well as Section 804 middle-tier acquisition authority can help to create additional industrial base capacity akin to that of the numerous aircraft companies in World War II by increasing these prototyping efforts and linking them with production programs.

- Increasing visibility into defense supply chains through an independent third-party mechanism will help to identify capacity challenges in the defense industrial base as they develop and mitigate them before they have an operational impact.

- Stockpiling is a cost-effective way to build capacity in the defense industrial base. Building on the expansion of the Strategic National Stockpile in the CARES Act, DOD should explore ways to build additional capacity by stockpiling resources that are relevant for great-power competition.

Resilience

- Planning and organizing in advance will help to speed future mobilizations of the defense industrial base. Detailed plans and standing organizations are in no way solutions by themselves, but clearly outlining and aligning DPA and other authorities, policies, and responsibilities for future crises and taking an informed approach to planning will help to bring the best aspects of industrial policy to bear for the defense industrial base.

- Finally, the industrial base has clearly become an extended part of the battlefield in today's environment. A catastrophic cyberattack, an antisatellite attack destroying our Global Positioning System network, or a deadly second wave of COVID could cripple facilities or large parts of the defense industrial base with little or no warning. Thus, efforts such as CMMC will be crucial to building longer-term resilience in the defense industrial base.

Conclusion

This examination of past, recent, and ongoing national crises and changes in the national security environment has demonstrated the tremendous dynamism and resilience of our defense industrial base. When the chips are down, our private and public sectors clearly can deliver. From the global conflicts of the 20th century and the post-9/11 world to today's COVID-19 response and era of great-power competition, companies across the industrial base develop and produce systems and solutions to meet our national defense needs. Government agencies and Congress have similarly formed organizations and adjusted policies, created and aligned authorities, and otherwise worked toward the same goal.

Building resilience across our defense industrial base is a national security imperative. The dramatic federal spending on COVID-19 has led to speculation that future defense budget cuts are coming. Given the threats facing the nation and the inherent "stickiness" of

defense budgets, significant cuts (at least in the near term) are not likely.[72] Defense leaders need to use this time to build resilience in our industrial base for the future. Laws, regulations, plans, and policies can enable or inhibit how well the country can mobilize critical assets. There is no silver bullet, but the key is for government and industry to collaborate effectively and transparently to meet our evolving security needs.

Endnotes

1. C. Todd Lopez, "DoD Focuses on Sustaining Industrial Base Through Pandemic," U.S. Department of Defense, May 5, 2020, https://www.defense.gov/Explore/News/Article/Article/2177093/dod-focuses-on-sustaining-industrial-base-through-pandemic/ (accessed July 10, 2020).
2. See, for example, Elizabeth Behring, "Army's Organic Industrial Base Sustains the Greatest Fighting Force in the World," U.S. Army, March 14, 2018, https://www.army.mil/article/201827/armys_organic_industrial_base_sustains_the_greatest_fighting_force_in_the_world (accessed July 10, 2020).
3. U.S. Department of Defense, Office of the Under Secretary of Defense for Acquisition and Sustainment, Office of the Deputy Assistant Secretary of Defense for Industrial Policy, *Industrial Capabilities: Annual Report to Congress, Fiscal Year 2018*, May 2019, p. 80, https://www.businessdefense.gov/Portals/51/Documents/Resources/2018%20AIC%20RTC%2005-23-2019%20-%20Public%20Release.pdf?ver=2019-06-07-111121-457 (accessed July 10, 2020).
4. James Mattis, Secretary of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, U.S. Department of Defense, pp. 2–3, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (accessed July 10, 2020).
5. *National Security Strategy of the United States of America*, The White House, December 2017, p. 21, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (accessed July 10, 2020).
6. See Defense Innovation Unit, "About," https://diu.mil/about (accessed July 6, 2020).
7. See AFWERX, "Connecting Air Force Innovators and Accelerating Results," https://www.afwerx.af.mil (accessed July 10, 2020), and U.S. Army, "Army Futures Command," https://www.army.mil/futures (accessed July 10, 2020).
8. Eric Schmitt, "Iraq-Bound Troops Confront Rumsfeld over Lack of Armor," *The New York Times*, December 8, 2004, https://www.nytimes.com/2004/12/08/international/middleeast/iraqbound-troops-confront-rumsfeld-over-lack-of.html (accessed July 10, 2020).
9. Jacques S. Gansler, *Democracy's Arsenal: Creating a Twenty-First-Century Defense Industry* (Cambridge, MA: MIT Press, 2011), pp. 16–17.
10. Barbara W. Tuchman, *The Guns of August: The Outbreak of World War I* (New York: Macmillan, 1962).
11. Jim Garamone, "World War I: Building the American Military," U.S. Army, April 3, 2017, https://www.army.mil/article/185229/world_war_i_building_the_american_military (accessed July 10, 2020).
12. Mark R. Wilson, *Destructive Creation: American Business and the Winning of World War II* (Philadelphia: University of Pennsylvania Press, 2016), pp. 8–21. "Coercion" quote from p. 11.
13. Arthur Herman, *Freedom's Forge: How American Business Produced Victory in World War II* (New York: Random House, 2012), p. 13.
14. Wilson, *Destructive Creation*, p. 51.
15. Herman, *Freedom's Forge*, p. 10.
16. Wilson, *Destructive Creation*, p. 61.
17. Herman, *Freedom's Forge*, pp. 37–57 and 66–78.
18. Wilson, *Destructive Creation*, pp. 59–76.
19. Herman, *Freedom's Forge*, p. 248.
20. Gansler, *Democracy's Arsenal*, p. 12.
21. Wilson, *Destructive Creation*, pp. 74–78, and Herman, *Freedom's Forge*, pp. 86–88.
22. For detailed treatments of these issues, see Wilson, *Destructive Creation*, Chapters 4 and 5.
23. For the full story of the B-29 Superbomber, see Herman, *Freedom's Forge,* Chapters 16–18.
24. Wilson, *Destructive Creation*, p. 242.
25. *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952), https://supreme.justia.com/cases/federal/us/343/579/ (accessed July 10, 2020), and Joshua Waimberg, "Youngstown Steel: The Supreme Court Stands Up to the President," National Constitution Center, Constitution Daily Blog, November 16, 2015, https://constitutioncenter.org/blog/youngstown-steel-the-supreme-court-stands-up-to-the-president (accessed July 10, 2020).
26. U.S. Department of Commerce, Bureau of Industry and Security, "Defense Priorities and Allocations System Programs (DPAS)," https://www.bis.doc.gov/index.php/other-areas/strategic-industries-and-economic-security-sies/defense-priorities-a-allocations-system-program-dpas (accessed July 10, 2020).

27. Michael H. Cecire and Heidi M. Peters, "The Defense Production Act of 1950: History, Authorities, and Considerations for Congress," Congressional Research Service *Report for Members and Committees of Congress*, updated March 2, 2020, p. 9, https://fas.org/sgp/crs/natsec/R43767.pdf (accessed July 10, 2020).
28. 50 USC §4531(a)(1), https://uscode.house.gov/view.xhtml?path=/prelim@title50/chapter55&edition=prelim (accessed July 10, 2020).
29. See "Earmark Declaration," remarks by Representative Charles Dent of Pennsylvania, *Congressional Record*, Vol. 155, No. 116 (July 29, 2009), pp. E2057–E2058, https://www.govinfo.gov/content/pkg/CREC-2009-07-29/html/CREC-2009-07-29-pt1-PgE2057-3.htm (accessed July 10, 2020), and Air Force Research Laboratory, ManTech, "Defense Production Act Title III Project Establishes Domestic Source for Beryllium," Wright-Patterson Air Force Base, September 17, 2013, https://www.wpafb.af.mil/News/Article-Display/Article/819343/defense-production-act-title-iii-project-establishes-domestic-source-for-beryll/ (accessed July 10, 2020).
30. 50 USC §4558(c)(1), https://uscode.house.gov/view.xhtml?path=/prelim@title50/chapter55&edition=prelim (accessed July 30, 2020).
31. See James K. Jackson, "The Committee on Foreign Investment in the United States (CFIUS)," Congressional Research Service *Report for Members and Committees of Congress*, updated February 14, 2020, https://fas.org/sgp/crs/natsec/RL33388.pdf (accessed July 30, 2020).
32. Cecire and Peters, "The Defense Production Act of 1950: History, Authorities, and Considerations for Congress," pp. 14–19.
33. Wilson, *Destructive Creation*, p. 266.
34. Stockholm International Peace Research Institute, "SIPRI Military Expenditure Database," https://www.sipri.org/databases/milex (accessed July 10, 2020).
35. Gansler, *Democracy's Arsenal*, pp. 28 and 32–34.
36. Ibid., p. 11.
37. Ibid.
38. U.S. Government Accountability Office, *Defense Production Act: Agencies Lack Policies and Guidance for Use of Key Authorities*, GAO-08-854, June 2008, p. 6, https://www.gao.gov/assets/280/277418.pdf (accessed July 10, 2020).
39. James M. Hasik, *Securing the MRAP: Lessons Learned in Marketing and Military Procurement* (College Station: Texas A&M University Press, forthcoming January 2021); based on James M. Hasik, *MRAP: Marketing Military Innovation*, unpublished PhD dissertation, University of Texas at Austin, May 2016, https://www.slideshare.net/jhasik/hasikdissertation2016-70324459 (accessed July 10, 2020).
40. Reports for FY 2013 through FY 2019 are available at U.S. Department of Defense, Industrial Policy, "Congressional Interests and Reports," https://www.businessdefense.gov/resources/ (accessed July 10, 2020).
41. Addison Wiggin, "The Truth Behind China's Rare Earths Embargo," *Forbes*, October 20, 2010, https://www.forbes.com/sites/greatspeculations/2010/10/20/the-truth-behind-the-chinese-rare-earths-embargo/#21f1d76e7846 (accessed July 10, 2020).
42. Reports from December 2008 through calendar year 2018 are available at U.S. Department of the Treasury, "CFIUS Reports and Tables," https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-reports-and-tables (accessed July 10, 2020).
43. Title XVII, Review of Foreign Investment and Export Controls, in H.R. 5515, John S. McCain National Defense Authorization Act for Fiscal Year 2019, Public 115-232, 115th Cong., August 13, 2018, https://www.congress.gov/115/plaws/publ232/PLAW-115publ232.pdf (accessed July 26, 2020).
44. James K. Jackson, "The Committee on Investment in the United States (CFIUS)," Congressional Research Service *Report for Members and Committees of Congress*, updated February 14, 2020, pp. 1–2, https://fas.org/sgp/crs/natsec/RL33388.pdf (accessed July 10, 2020).
45. President Donald J. Trump, "Presidential Executive Order on Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States," The White House, July 21, 2017, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-assessing-strengthening-manufacturing-defense-industrial-base-supply-chain-resiliency-united-states/ (accessed July 10, 2020).
46. U.S. Department of Defense, Office of the Under Secretary of Defense for Acquisition and Sustainment, Office of the Deputy Assistant Secretary of Defense for Industrial Policy, *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States: Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806*, September 2018, passim, 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 (accessed July 10, 2020).

47. Ibid., p. 3.
48. U.S. Department of Defense, Industrial Policy, "Defense Production Act (DPA) Title III," https://www.businessdefense.gov/Programs/DPA-Title-III/ (accessed July 10, 2020), and U.S. Department of Defense, Industrial Policy, "IBAS Opportunities," https://www.businessdefense.gov/IBAS/Opportunities/ (accessed July 10, 2020).
49. See, respectively, notes 40 and 38, *supra*.
50. See Moshe Schwartz and Heidi M. Peters, "Department of Defense Use of Other Transaction Authority: Background, Analysis, and Issues for Congress," Congressional Research Service *Report for Members and Committees of Congress*, updated February 22, 2019, https://fas.org/sgp/crs/natsec/R45521.pdf (accessed July 10, 2020).
51. For a summary and links to DOD implementing instructions, see AcqNotes, "Acquisition Process: Middle-Tier Acquisition (Section 804)," updated December 31, 2019, http://acqnotes.com/acqnote/acquisitions/middle-tier-acquisitions (accessed July 10, 2020).
52. U.S. Department of Defense, "DoD Instruction 5000.02: Operation of the Adaptive Acquisition Framework," January 23, 2020, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002p.pdf?ver=2020-01-23-144114-093 (accessed July 10, 2020).
53. U.S. Department of Defense, Office of the Under Secretary of Defense for Acquisition and Sustainment, Office of the Deputy Assistant Secretary of Defense for Industrial Policy, *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States*, p. 49.
54. For details on CMMC, see U.S. Department of Defense, Office of the Under Secretary of Defense for Acquisition and Sustainment, Cybersecurity Maturity Model Certification, "CMMC Model," https://www.acq.osd.mil/cmmc/draft.html (accessed July 10, 2020).
55. Keith Bradsher and Liz Alderman, "The World Needs Masks. China Makes Them, but Has Been Hoarding Them," *The New York Times*, updated April 2, 2020, https://www.nytimes.com/2020/03/13/business/masks-china-coronavirus.html (accessed July 10, 2020).
56. Ana Swanson, "Coronavirus Spurs U.S. Efforts to End China's Chokehold on Drugs," *The New York Times*, March 11, 2020, https://www.nytimes.com/2020/03/11/business/economy/coronavirus-china-trump-drugs.html (accessed July 10, 2020).
57. Jerry McGinn, "How to Safeguard and Rebuild Our Public Health Supply Chain," *Business Insider*, April 14, 2020, https://www.businessinsider.com/dr-jerry-mcginn-safeguard-public-health-supply-chain-department-defense-cares-coronavirus (accessed July 10, 2020).
58. Jerry McGinn and Eric Lofgren, "COVID-19 Response—Executive Update," George Mason University, School of Business, Center for Government Contracting, April 8, 2020, https://business.gmu.edu/images/GovCon/Website/Center_for_Government_Contracting_COVID-19_Executive_Update.pdf (accessed July 10, 2020).
59. Gavin Gade and Megan Cassella, "Days After Ventilator DPA Order, White House Has Done Little to Push GM," *Politico*, April 2, 2020, https://www.politico.com/news/2020/04/02/white-house-general-motors-defense-production-act-161833 (accessed July 10, 2020).
60. President Donald J. Trump, "Executive Order on Prioritizing and Allocating Health and Medical Resources to Respond to the Spread of Covid-19," The White House, March 18, 2020, https://www.whitehouse.gov/presidential-actions/executive-order-prioritizing-allocating-health-medical-resources-respond-spread-covid-19/ (accessed July 10, 2020).
61. The President ended up suing the DPA allocation authority in a very limited way by directing specific companies such as GM to produce ventilators and other items when negotiations on voluntary efforts broke down. See, for example, W. J. Hennigan, "Trump Bets on Powers of Persuasion to Compel Big Business to Produce Urgent Medical Supplies," *Time*, March 24, 2020, https://time.com/5809264/trump-big-business-coronavirus/ (accessed July 10, 2020), and Gavin Gade, "'GM Was Wasting Time': Trump Invokes DPA to Force GM to Make Ventilators," *Politico*, March 27, 2020, https://www.politico.com/news/2020/03/27/trump-slams-gm-over-ventilator-production-delays-costs-151885 (accessed July 10, 2020).
62. Jerry McGinn, James Hasik, and Eric Lofgren, "COVID-19 Response—Contracting with Speed," George Mason University, School of Business, Center for Government Contracting, April 22, 2020, https://business.gmu.edu/images/GovCon/Website/GMU_COVID-19_Contracting_with_Speed.pdf (accessed July 10, 2020).
63. News release, "NIST Funding Manufacturing Institutes to Support Pandemic Response," U.S. Department of Commerce, National Institute of Standards and Technology, updated May 18, 2020, https://www.nist.gov/news-events/news/2020/03/nist-funding-manufacturing-institutes-support-pandemic-response (accessed July 10, 2020).
64. Medical Technology Enterprise Consortium, "Project Awards," https://www.mtec-sc.org/mtec-current-projects/ (accessed July 26, 2020).
65. McGinn and Lofgren, "COVID-19 Response—Executive Update."

66. H.R. 748, Coronavirus Aid, Relief, and Economic Security (CARES) Act, Public Law 116-136, 116th Cong., March 27, 2020, https://www.congress.gov/bill/116th-congress/house-bill/748/text?loclr=bloglaw%23toc-H0D9C019E301D4A9584058F8DA59D1CC8 (accessed July 11, 2020).
67. News release, "DOD Awards $138 Million Contract, Enabling Prefilled Syringes for Future COVID-19 Vaccine," U.S. Department of Defense, May 12, 2020, https://www.defense.gov/Newsroom/Releases/Release/Article/2184808/dod-awards-138-million-contract-enabling-prefilled-syringes-for-future-covid-19/ (accessed July 11, 2020), and news release, "DOD Awards $126 Million Contract to 3M, Increasing Production of N95 Masks," U.S. Department of Defense, May 6, 2020, https://www.defense.gov/Newsroom/Releases/Release/Article/2178152/dod-awards-126-million-contract-to-3m-increasing-production-of-n95-masks/ (accessed July 11, 2020).
68. Thomas Brewster, "Palantir, the Peter Thiel-Backed $20 Billion Big Data Cruncher, Scores $17 Million Coronavirus Emergency Relief Deal," *Forbes*, April 11, 2020, https://www.forbes.com/sites/thomasbrewster/2020/04/11/palantir-the-peter-thiel-backed-20-billion-big-data-cruncher-scores-17-million-coronavirus-emergency-relief-deal/#7444944a5ed1 (accessed July 10, 2020).
69. Sydney J. Freedberg Jr., "OMFV: Army Revamps Bradley Replacement for Russian Front," *Breaking Defense*, April 10, 2020, https://breakingdefense.com/2020/04/army-revamps-omfv-bradley-replacement-for-russian-front/ (accessed July 10, 2020).
70. National Defense Industrial Association, *Vital Signs 2020: The Health and Readiness of the Defense Industrial Base*, p. 5, https://www.ndia.org/-/media/vital-signs/vital-signs_screen_v2.ashx?la=en (accessed July 10, 2020).
71. Ibid, pp. 52–59.
72. Eric Lofgren, "Will Defense Budgets Remain 'Sticky' After the COVID-19 Pandemic?" *Defense News*, May 26, 2020, https://www.defensenews.com/opinion/commentary/2020/05/26/will-defense-budgets-remain-sticky-after-the-covid-19-pandemic/ (accessed July 10, 2020).

Strategic Mobility: The Essential Enabler of Military Operations in Great-Power Competition

John Fasching

"If everyone is thinking alike, then somebody isn't thinking."

—General George S. Patton

America's military instrument of national power has prevailed over those of our adversaries because of an unparalleled ability to project and sustain dominant force levels rapidly around the globe. In concert with the diplomatic, information, and economic instruments of national power, the military helps to implement America's national security and defense strategies,[1] but success in great-power competition and future conflict will require a reinfusion of innovation and resources.

Traditionally, the Department of Defense (DOD) has invested in a set of strategic mobility enablers that can move war-winning levels of combat forces, equipment, and supplies to sustain military operations at the time and place, and for the duration of, our choosing. DOD has developed and resourced the necessary strategic mobility–related doctrine, organizations, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) in order to meet the force-flow requirements of geographic combatant commanders in executing their operational war plans. This commitment is demonstrated by the four-star-level, joint United States Transportation Command (USTRANSCOM), which orchestrates American strategic mobility operations in concert with interagency, intergovernmental, multinational, nongovernmental, and commercial stakeholders.

Growing Critical Challenges

At the same time, however, America's competitors and adversaries have been making their own investments in an effort to offset American strategic mobility overmatch in future armed conflicts. Our recent military successes have been against nation-states that were not capable of global competition or nonstate actors with little to no ability to disrupt our strategic mobility capabilities. The nature of the competition through the conflict continuum vis-à-vis China, Russia, Iran, North Korea, and even the fight against terrorism, or likely combinations thereof, in an era of great-power competition and conflict demands strategic mobility–enabling processes and capabilities

Retired U.S. Army Lieutenant Colonel John Fasching has written and presented on strategic mobility issues for such organizations as the National Defense Transportation Association, the Association of the United States Army, and the National Academies of Sciences Transportation Research Board. The views expressed in this essay are those of the author alone and do not reflect the official policies or the positions of any DOD, joint, interagency, intergovernmental, multinational, nongovernmental, or commercial organization.

that are different from those we have now. Our current deployment process must be enhanced, particularly for "early" deployers in contested environments, because it is predictable and inadequate for ever-compressing, adequate military-response timelines and threat capabilities for disruption of our force flow.

Adversaries with advanced (and in some cases superior) weaponry, lethal global reach, and strategic mobility programs and capabilities of their own have combined to force us to acknowledge the contested nature of our military operating environments and adjust our concepts, strategies, plans, and capability development efforts. Concentrations of forces and supplies create target-rich environments, and our operations must become more and more distributed to increase our survivability and resilience as we move further away from benign operating environments.

Our most recent concerted, top-down directed strategic mobility investment occurred in the 1990s with nearly $50 billion directed by Congress and applied across DOTMLPF-P. It garnered strategic military air and sealift platforms and access to commercial lift capacities, globally prepositioned military equipment and supplies, deployment training exercises, railcars and equipment, deployment infrastructure, management systems, process improvements, and other deployment enablers. Over the 30 years since then, our deployment capability has declined relative to the anti-access/area denial (A2/AD) strategies and investments made by our adversaries to counteract our long-standing strategic mobility overmatch.

While operating in Iraq and Afghanistan, we deferred most investments in the modernization of strategic mobility enablers, and much of our current strategic mobility solution set now faces critical near-term age-out and obsolescence challenges. Our domination of the air, land, maritime, cyber, and space warfighting domains, which enabled unmatched force projection capabilities, has atrophied as we have had the operational luxury of largely uncontested, long-lead-time, rotational, and contractor-enabled deployments to Iraq and Afghanistan. While we accepted risk in deferring modernization, adversaries were developing their own global-reach capabilities that threaten to disrupt deployment operations both in America and en route to theaters of operation the next time we deploy a campaign-quality force in support of large-scale combat operations (LSCO). Our adversaries have invested heavily in A2/AD capabilities that directly threaten American strategic mobility.

There are cultural challenges that stand in the way of the necessary shift in our thinking about what our strategic mobility solution set should look like and how it should be prioritized to ensure the successful execution of our national security and defense strategies. Undoubtedly, fiscal pressure and competition for resources will limit significant investments in truly transformational programs of strategic mobility capability development, so we must refocus our attention on reconfiguring our existing strategic mobility solution set in affordable ways for little-to-no-notice, rapid, expeditionary, contested deployments against astute and dynamic great-power adversaries.

The $50 billion investment made 30 years ago has served us well, but it has run its course, and existing lift platforms and infrastructure should be reconfigured with the enabling of future, contested LSCO in mind. As the overall size of America's Joint Force has declined since the end of the Cold War, so too has the strategic mobility enterprise. Major portions of our strategic sealift and airlift platforms, rail deployment enablers, and deployment infrastructure have reached or are fast approaching the end of their serviceable lives, and spending for modernization has been either woefully inadequate or deferred entirely. These deferrals have created a gathering tsunami of strategic mobility–related funding requirements. In addition, our aging strategic mobility enabler set was designed for deployment operations and conditions that are vastly different from the operational challenges that we face today and will face in the near term. Combat vehicle

weights and dimensions have increased to improve fire power and crew survival rates; however, this trend affects a key performance parameter for new equipment development: the ability to transport and rapidly employ these vehicles.

This constant friction between weapon system lethality and survivability versus transportability and the cumulative impacts on strategic mobility is intensifying as military operating environments become more and more lethal. We are at an inflection point in the history of America's dominance in strategic mobility capability and overdue for another hard look at how to transform America's strategic mobility capability not only across America's joint military organizations, but also within the context of the interagency, intergovernmental, multinational, and commercial partners that are critical to our strategic mobility operations in any conflict.

The Strategic Mobility Triad

According to DOD's joint doctrine:

> Strategic mobility is the capability to deploy and sustain military forces worldwide in support of national strategy. Beyond the intrinsic capability of some US forces to self-deploy, the bulk of our nation's strategic mobility requirements are met through common-user sealift, common-user airlift, and pre-positioned stocks, known as the strategic mobility triad....[2]

Modernizing this triad requires planning, prioritization, coordination, and resourcing among joint, interagency, intergovernmental, multinational, and commercial (JIIM-C) partners.

Joint organizations that contribute to strategic mobility operations include the Navy, Air Force, Army, Marine Corps, geographic, and functional combatant commands. Since America's air and naval forces largely self-deploy, the strategic mobility triad predominantly supports the rapid movement of land-domain personnel, equipment, and sustainment from the Army and Marine Corps into conflict areas. Prepositioning some of their equipment, supplies, and ammunition allows some early deployers to fly in, draw equipment, and rapidly organize for combat, providing a deterrent effect through the rapid buildup of combat power in a theater of operations. Recent efforts to "combat configure" prepositioned stocks lessen the time it takes to issue the gear, thus "priming the pump" and accelerating the delivery of combat-ready forces to combatant commanders.

The four services plan, resource, coordinate, and synchronize their independent capability development efforts for strategic mobility, and the United States Transportation Command (USTRANSCOM) orchestrates the joint deployment process when forces are alerted to deploy.

- The Navy's Military Sealift Command (MSC), a component of USTRANSCOM, operates and maintains the 125 ships that sustain maritime domain operations and transport Army and Marine Corps forces. These MSC ships, which perform a wide variety of missions that provide all manner of logistics support to maritime assets, include hospital, cargo, underway fuel and dry cargo replenishment, and rescue and salvage ships.

- The Air Force operates aerial refueling and transport aircraft to support strategic mobility through its Air Mobility Command (AMC), also a USTRANSCOM component command.[3] The current air transport fleet includes 428 C-130 Hercules, 222 C-17 Globemaster, and 52 C-5 transport aircraft.[4]

- The Army's USTRANSCOM component command is the Military Surface Deployment and Distribution Command (SDDC). SDDC integrates and synchronizes surface deployment and distribution capabilities to project and sustain U.S. forces,

primarily through road, rail, and seaport operations and transportation engineering assessments, coordinating the movement of equipment from a unit's home station to its seaport of debarkation.

Interagency Partners and Strategic Mobility

Interagency partners play a critical role in strategic mobility's underpinning of U.S. national security by rapidly introducing military capabilities either domestically or abroad. The herculean effort involved in deploying campaign-quality forces and sustaining them for the duration of combat operations requires a vast network of non-military partners, starting with interagency organizations. In this context, the joint doctrinal definition of strategic mobility fails to account adequately for and describe enabling capabilities provided by the other "IIM-C" entities. Joint and service concepts under development must account for the fact that America's deployment process is only as reliable, fast, and effective as the JIIM-C stakeholders that enable it.

Using sealift as an example, the Army can be ready to deploy its equipment and initial sustainment stocks to seaports of embarkation in time to load aboard ships, but if the ships are not on par with their own readiness rates and abilities to meet force-flow synchronization timelines, the force will arrive late to the theater of operations, giving our adversaries more time to fortify defenses and further delay our deployment process while undermining the will of the American people to continue prosecuting military operations. Conversely, if Army units do not make it to the port on time, the sailing schedule will be delayed, causing delays all along the joint deployment process and negatively affecting the combatant commander's ability to execute his plan according to operational timelines.

The role of America's interagency partners in facilitating force deployments includes coordination by the Department of State in obtaining diplomatic clearances, basing rights, and overflight rights and building coalitions for military operations. Interagency support also includes heavy reliance on Department of Transportation (DOT) capabilities such as those provided by the United States Coast Guard to ensure maritime and port security. Another DOT interagency partner, the Maritime Administration (MARAD), provides multiple types of ships to deploy and sustain military operations through three programs that underpin the National Defense Reserve Fleet (NDRF): the Maritime Security Program (MSP); Voluntary Intermodal Sealift Agreement (VISA); and Voluntary Tanker Agreement (VTA). These three programs collectively give MARAD access to 185 ships. "At its height in 1950," however, "the NDRF consisted of 2,277 ships."[5]

In contrast to the decline in America's maritime capability, "China is seen as striving to overtake the U.S. as the dominant naval power in Asia and already boasts the world's largest navy in numbers of vessels."[6] Even with fewer U.S.-flagged ships, the need to find trained and qualified U.S. mariners, resources to recapitalize ships, and the necessary naval combatant ship escorts in the event of an LSCO puts our maritime-domain strategic readiness at unacceptable levels of operational risk. As aptly summarized by national security expert Loren Thompson:

> Washington…is not sending the right message to Moscow and Beijing if its goal is to deter aggression by demonstrating the means to respond quickly and forcefully. Lack of sealift could prevent the world's most capable ground force from getting to the fight in time to make a difference—or being able to sustain an effective defense over time without resorting to use of nuclear weapons. To put it bluntly, America could lose a Eurasian war for lack of timely sealift.[7]

On the Military Sealift Command side of the equation, our maritime readiness shortfalls were underscored during USTRANSCOM's most recent TURBO ACTIVATION (TA)

readiness exercise: "Of the 61 ships assigned to the Organic Surge Fleet at the start of TA 19+, a total of 63.9% (39 of 61 ships) were ready for tasking (RFT)."[8] Given that about 90 percent of the deploying equipment and sustainment stocks are moved to a contingency on sealift, the negative trends in U.S. sealift capability, capacity, resiliency, and readiness must be reversed.

Intergovernmental (civilian) and multinational (military) cooperation and agreements provide basing and prepositioning sites, overflight rights, customs and transportation clearances, and access to other required infrastructure for coordinated global deployments. U.S. forces flow through host-nation commercial seaports and airports and clear them using distribution infrastructure alongside commercial cargoes. Commercial cargo operations must be balanced with military force flows to avoid both negative effects on host-nation economies and the undermining of public support for U.S. deployments abroad.

Public and geopolitical pressure can deny U.S. forces the use of planned deployment infrastructure, as when Turkey denied access to U.S. forces during Operation Iraqi Freedom.[9] Turkey's decision precluded a large-scale maneuver operation into Iraq from the north and caused a sealift logjam. It also delayed the commencement of U.S. offensive ground operations. Fortunately, Iraq lacked the long-range, precision strike capability to threaten Kuwaiti ports and could not turn the operational delay into a significant military advantage.

Today's adversaries have studied recent U.S. deployments and will precisely target the relatively few world-class seaports and airports on which U.S. forces largely depend for rapid, efficient, and effective deployment operations, thus adding to force-flow planning and execution challenges as potential host nations weigh the risks involved in granting access.

Commercial Assets and Civilian Contractors

Commercial-partner airlift and sealift capacity is made available for military deployments through the Voluntary Intermodal Sealift Agreement and Civil Reserve Air Fleet (CRAF) programs that leverage U.S.-flagged commercial strategic lift platforms to deploy and sustain military forces in times of war. The armed services have largely relied on outsourcing to commercial industry to fill capability gaps in deploying and sustaining forces during recent operations. Operations Iraqi Freedom and Enduring Freedom saw unprecedented levels of contractors on the battlefield, and those trends are extremely hard to reverse, particularly once the services have divested themselves of force structure by leveraging the support of contractors.

Given the lethality and risks inherent in the changing character of war in contested environments the likes of which we have not seen since World War II, we must reassess the tactics, techniques, and procedures associated with fully leveraging commercial assets and civilian contractors for strategic mobility capability in anticipated contested environments. We can ill afford losses on the scale of the 1,614 ships and 9,521 mariners lost by the Merchant Marine during World War II.[10] Nor can we absorb the significant losses of commercial aircraft in strategic mobility roles that, given the proliferation of advanced anti-aircraft weapons systems, are likely in fights with great-power adversaries and their proxy forces.

DOD is but one part of an extensive, complex JIIM-C team, providing strategic mobility in response to almost every type of operation, from disaster response and consequence mitigation to large-scale combat operations. The COVID-19 pandemic response highlighted how defense support to civil authorities can augment a whole-of-nation—or even a whole-world—response. It also exposed national vulnerabilities and areas where we may be accepting unreasonable risk, particularly where supply chains originate in or run through competitor or adversary nations, thus threatening our strategic mobility capabilities.

Great-power competitors and adversaries are developing and leveraging multi-domain, global reach, and strategic mobility capabilities

of their own to counter our phenomenal but aging and predictable joint deployment process and its enablers. Maintaining robust strategic mobility capabilities significantly deters rational bad actors and is part of our calculus for military courses of action when adversaries threaten U.S. national security interests.

Moreover, maintaining overmatch requires a concerted strategy and the resourcing of operational capability across JIIM-C stakeholders and enabling organizations. When the information system screens go black and information and data stop flowing because of disruptions in the space and cyber domains, our ability to operate depends on institutional memory and training in the use of pre-digitized battlefield tools, tactics, techniques, and procedures. For example, if an adversary were to deny the use of GPS, U.S. forces would have to rely on celestial, terrain-associative, or other navigational and target location techniques.

Weaknesses in the Joint Deployment Process

America's adversaries understand that America's recipe for success is its joint deployment process, and they understand the importance of contesting our strategic mobility overmatch in any future conflict. Our adversaries are fully leveraging opportunities during competition across their own instruments of national power to offset our traditional overmatch in strategic mobility.

For example, China invests heavily to gain a controlling interest in global seaports of strategic value; owns about 90 percent of the International Organization for Standardization (ISO) shipping container manufacturing market; and has constructed and is improving facilities on islands it has built as A2/AD defensive outposts in the South China Sea. China's published "Made in China 2025" strategy clearly indicates that Beijing seeks to dominate certain manufacturing industries—many of which are critical to U.S. national security and force-projection capability. According to China's English-language website:

> Nine tasks have been identified as priorities: improving manufacturing innovation, integrating technology and industry, strengthening the industrial base, fostering Chinese brands, enforcing green manufacturing, promoting breakthroughs in ten key sectors, advancing restructuring of the manufacturing sector, promoting service-oriented manufacturing and manufacturing-related service industries, and internationalizing manufacturing.
>
> The above ten key sectors are:
> 1. New information technology
> 2. High-end numerically controlled machine tools and robots
> 3. Aerospace equipment
> 4. Ocean engineering equipment and high-end vessels
> 5. High-end rail transportation equipment
> 6. Energy-saving cars and new energy cars
> 7. Electrical equipment
> 8. Farming machines
> 9. New materials, such as polymers
> 10. Biomedicine and high-end medical equipment.[11]

This list has implications for where we acquire war materiel and enablers, particularly within the maritime domain. According to Loren Thompson:

> In its bicentennial year of 1976, the United States was the biggest builder of commercial oceangoing vessels in the world. Dozens of ships were under construction at domestic shipyards. The Reagan Administration wiped out the industry (and 40,000 jobs) by eliminating construction subsidies without seeking reciprocal action from other shipbuilding nations.
>
> That was a self-inflicted wound. But then in 2006, Beijing designated commercial shipbuilding as a strategic industry and began channeling massive state

subsidies to the sector. End result: China has become by far the biggest producer of commercial ships in the world, while fewer than 200 ships in the global fleet of 44,000 oceangoing vessels are American.

The U.S. today barely manages to rank among the top 20 commercial shipbuilding nations (it's number 19), and all of the oceangoing ships built recently in America were for use on protected domestic routes. Industry experts say without that protection, the commercial shipbuilding sector and the U.S. merchant marine would literally cease to exist.[12]

In the candid words of former USTRANSCOM Deputy Commander and DOT Administrator Lieutenant General Ken Wykle (Ret.):

The ability to rapidly deploy our forces suffers from two primary deficiencies. The first is a lack of Merchant Marine ships, and the second is a lack of qualified merchant mariners.

First, the ships. This is a matter of sheer numbers. In 1951, the U.S. Merchant Marine had 1,288 ships operating in international trade. Today, there are 81 ships. This means the U.S. Merchant Marine does not have the shipping capacity our country needs to deploy and supply the most capable military in the world....

The human capital shortage may be worse than the shortage in ships. A report by the Maritime Administration to Congress highlighted the problem. The report "estimates that 11,768 qualified mariners... are available to crew the Ready Reserve Force...the estimated demand for mariners [in an emergency] is 13,607."[13]

As strategic risk to missions and forces during future crisis response operations and attrition continue to manifest, these pressures will change how we deploy and redeploy forces. We are going to have to fight our way to the fights. Combat configuration–related reviews of the entire joint deployment process, from origin to destination, should be undertaken. JIIM-C operations against adversaries with global reach and advanced weaponry in all domains require whole-of-nation and multinational approaches, investments, and planning.

It is crucial that previous assumptions about capital and combat losses be called into question. The next version of the nation's strategic mobility solution set must reflect the harsh realities of JIIM-C operating environments and how our soldiers, sailors, airmen, Marines, Coast Guardsmen, Merchant Mariners, Medical Service Corps personnel, and populations are trained and prepared to respond to periodic windows of ubiquitous battlespace and global combat operations.

The October 1, 2016, missile attack on the former MSC Expeditionary Fast Transport Ship HSV-2 Swift[14] indicates the complexities of operating in a JIIM-C-enabled, contested environment in which the lines between competition and conflict are all but indistinguishable. It also highlights how non-governmental organization actors or their proxies can complicate deployment and sustainment operations. The attack was carried out by Houthi rebels off the coast of Yemen, and the vessel was leased to the United Arab Emirates for a humanitarian aid mission—a potpourri of JIIM-C operations on both sides.

Dynamic Force Deployment

Another example of how we must change our execution of global force projection involves the joint reception, staging, onward movement, and integration phase of the joint deployment process, which concentrates critical infrastructure, equipment, and personnel into a target-rich environment. All-domain effects on civilian populations and infrastructure that enable America to mobilize and deploy its forces can demoralize and undercut the popular will to support military operations. Therefore, as part of "dynamic force employment,"

DOD is exploring how to conduct more geographically dispersed, mobile, and distributed operations to offset increased risk to mission and forces. LSCO will test the nation's character, and senior leaders must candidly address the implications of this operational shift to contested environments in their strategic messaging and testimony before Congress.

Corey New, a retired Army colonel and former commander of the Defense Logistics Agency's Susquehanna Depot, has said that "building combat power begins at origin, not in a theater of operations." Extrapolating his point, in globally contested operations, America's military may be employing combat power at origin and en route, not just in theaters of operations. How well we transition to this new paradigm correlates directly with any deterrent effect on our adversaries. Acknowledging the reality of increasingly lethal global operating environments, our national military strategy seeks to deter adversaries and win during the competition phase *before* large-scale armed conflict. If deterrence fails, our ability to fight and win decisively hinges on a robust and resilient strategic mobility set of enablers and rapid, near-term offset strategy solutions. Our challenge is to respond operationally to—and navigate "gray area" warlike acts by—competitors and adversaries as they affect all warfighting domains, as well as all instruments of United States national power (diplomatic, information, military, and economic).

The National Defense Strategy (NDS) cites "[r]esilient and agile logistics" as a key area of capability modernization and states that DOD "will prioritize prepositioned forward stocks and munitions, strategic mobility assets, partner and allied support, as well as non-commercially dependent distributed logistics and maintenance to ensure logistics sustainment while under persistent multi-domain attack."[15] Two challenges cascade from that guidance for joint operating environments and adversary capabilities:

- The lines between JIIM-C deployment and sustainment operations blur in realistic (defense) planning scenarios and defense support to civil authorities (DSCA) potential missions, particularly when the homeland is no longer a sanctuary, and

- The American strategic mobility capability set and the joint deployment process used to execute it are JIIM-C partner–enabled, but the full complement of stakeholders have not performed all-domain, contested operations at scale and echelon since World War II.

Studying Mobility Capability Requirements

The cyclical, congressionally mandated Mobility Capability Requirements Study (MCRS) is currently underway and should ascertain strategic mobility gaps and shortfalls associated with the execution of deployment operations in support of combatant commanders' operational plans in the context of likely scenarios and adversary capabilities. In a June 2018 *Airman Magazine* interview, General Darren McDew stated:

> [I]f I had a crystal ball and talked about this new Mobility Capability Requirements Study…it will be different than all the ones we've had previous[ly] for a couple of different reasons.
>
> The biggest of which is we're acknowledging a contested environment from day one. That's huge.
>
> We're also acknowledging something that we've got to come to grips with—attrition. We've never in our history, accounted for the attrition of logistics and mobility in our war plans. For now, we've got numbers we've subscribed to for a number of years that say these are the numbers of assets we need to accomplish the mission. But, that assumes everything makes it. On time. Every time.

> We don't believe that's realistic in today's environment. The character of war has changed to a place not just with bombs and bullets, but also ones and zeros. It's a reality that attrition will exist in the next war.[16]

Those involved in MCRS are underappreciated American heroes with a wicked problem to solve: informing strategic mobility decisions during persistent conflict and great-power competition with compressing response timelines and ever more complex and lethal operating environments. Contested operating environments require increased resilience across JIIM-C partner organizations. We must bolster our ability to defend key terrain and operations globally and "harden" our strategic mobility platforms, systems, and processes for better survivability and resilience. Our assessments and analysis must leverage the full power of JIIM-C enablers to deploy, redeploy, and sustain LSCO across potential conflicts involving China, Russia, North Korea, Iran, and counterterrorism efforts.

Leveraging the Navy/Marine Corps distributed lethality concept and reimagining the Army "cargo" aboard MSC and MARAD ships as taskable-en route, Army-provided, cross-domain effects–capable warfighting platforms can help to offset capability gaps and shortfalls in naval escorts by leveraging Army-assisted maritime defense and offense as a near-term approach to alleviating the risks that confront missions and forces. Reimagining the usable stowage areas on the weather decks of MSC and MARAD sealift ships as Army maneuver space in and from the maritime domain provides for the operational realities of contested logistics required to meet NDS guidance. If adversaries continue to shrink our advantages or if fiscal environments deteriorate to austerity-measure levels for DOD, the next iteration of air and sealift recapitalization will need to innovate quickly and cheaply to maintain strategic mobility overmatch and enhance joint combined arms maneuver capabilities over strategic distances.

DOD and others with a deployment mission could investigate the use of mobile, small-reactor power generators in plans for war, natural disasters, or attacks on power grids in the homeland or theaters of operations. For example, reactor generators infused with sealift recapitalization could power sealift ship enhancements to enable self-defense; conduct joint all-domain maneuver through contested maritime operations; and power directed energy, railgun, and other new weapons systems and platforms secured on sealift ships' weather decks, providing a new level of protection and offensive capability en route. Joint experimentation, training, and readiness exercises should include realistic scenarios requiring Army weapons systems live fire for cross-domain, joint combined arms maneuver, providing general-support/reinforcing fires in and/or from the maritime domain and for ship defense.

Other bolted-on or tied-down offset capabilities should be considered in the near term.[17] Mobile reactor generators could be ship-based or unit-based and power modular, ISO-container-configured life support to give combat-configured Army weapons crews a plug-and-play, scalable capability for contested JIIM-C operations. Increasingly, adversaries with strategic reach will force us to innovate and rethink how we will fight our way to the fights. Mobile reactor generators would also pay dividends if we should ever need to establish or repower portions of electrical power grids or reestablish digital connectivity and a base for stability operations after an electromagnetic pulse attack on the homeland, en route, or in theater during LSCO.

Rethinking strategic mobility would revive U.S. shipbuilding and encourage both innovative, militarily useful modifications, starting with commercial ships that DOD is considering purchasing, and focused efforts to recapitalize America's sealift fleet, industry, workforce, and supply chains. This includes U.S.-based manufacturing industries supplying materiel for strategic mobility. Similar thinking and actions must reverberate among the airlift and prepositioning communities as well.

The Secretary of Defense, Chairman of the Joint Chiefs, Commanding General USTRANSCOM, and service secretaries and chiefs have their work cut out for them. They must influence the prioritizing of precious resources by the JIIM-C enterprise as well as by each other and the National Security Council. The strategic mobility enabling team must be cohesive, self-synchronizing, and motivating with second-order, third-order, and fourth-order stakeholders understanding how to execute a complex joint deployment process effectively in a slim-margin, volatile, and hypercompetitive commercial marketplace. Commercial partners and civilians enable strategic mobility and are a part of the capital and combat loss equation.

As summarized by former Army Lieutenant General Sean MacFarland:

> Acting and reacting at the speed of multidomain warfare, executing cross domain fires and maneuver, will demand an unprecedented degree of integration between the services at multiple echelons, and therein lies the problem.
>
> A coherent force must be integrated across all elements of DOTMLPF-P (doctrine, organization, training, materiel, leadership and education, personnel, facilities and policy). However, since August 2011, when the Joint Forces Command folded its flag, no organization has had sufficient authority and resources to coordinate efforts across the services to develop joint warfighting concepts and support their implementation....[18]

The Joint Staff is continually updating and creating concepts to deal with the anticipated operating environments, but ownership and improvement of the joint deployment process, from concepts to fielded capabilities, has become a shared responsibility extending beyond the Joint Staff's authorities and responsibilities. USTRANSCOM integrates efforts of the "as is" strategic mobility capability set during operations; however, because there is no single conductor of planning, programming, budgeting, and oversight, the services (and other JIIM-C partners) invest individually as they see fit. As a result, the U.S. strategic mobility overmatch is atrophying relative to advances in competitor and adversary capability. Services and interagency and commercial partners and allies prioritize capabilities based on their perspectives, authorities, and perceived return on investment, further adding to the difficulty of capability management.

The point of convergence for action and synchronization for JIIM-C capability development is at the National Security Council level, which implies that consideration should be given to establishing this integrating oversight function at this level of authority as well. Unfortunately (and again), legislation may be the only remedy for the strategic mobility conundrum short of failing militarily against one or more great-power adversaries as ugly scenarios unfold.

Western military strategists and planners seek paths of least resistance and courses of action that minimize capital losses (such as ships, planes, and ports) and combat losses (such as soldiers, sailors, mariners, airmen, government civilians, and contractors) in obtaining military objectives. The military's capital is blood and treasure, and our nation's military conflicts will reap a return on investment commensurate with yesterday's and today's strategic mobility resourcing priorities. Barriers that prevent the rapid provision of combat-ready forces to combatant commanders can increase risks for missions and forces exponentially by allowing adversaries more time to prepare their cross-domain defenses and/or execute offensive strike operations against the U.S. and its partners. A combat multiplier for America's military is working in concert with other strategic planners within other instruments of national power, as well as with multinational partners, and planning for disruptions all along the joint deployment process.

When Congress perceives that the resourcing being provided to project U.S. military

forces to our best advantage is inadequate, it acts—usually cyclically, as it did in the early 1990s given the risks to mission and forces during the Operation Desert Shield force buildup. Another large capital infusion from Congress, however, although critically needed, is unlikely, as are any changes in service authorities under Title 10 of the United States Code. We will therefore have to think our way through reusing, recycling, and repurposing what we have and how we use and maintain it.

In chaotic operating environments, particularly during large-scale deployments in defense of American citizens on American soil, the deployment of military forces in support of America's national security interests can rapidly become complex. Adversary efforts to offset our strategic mobility overmatch could soon manifest themselves in artificial intelligence–infused, machine-blended, bioengineered, quantum-computed, and hypersonically executed operations with effects in all domains. COVID-19 catalyzed our strategic mobility response to a biowarfare scenario in which JIIM-C capabilities were rapidly deployed and sustained in the U.S. and its territories. Deferred investments in our globally focused strategic mobility solution set invite failure in the absence of bold and audacious steps from the Pentagon, which should provide specified guidance with targeted support from the White House and Congress.

From a national power perspective, ensuring strategic mobility is the best way to ensure success in great-power competition, as speed and mobility matter more than ever. Winning rapidly in synchronization within all domains is precisely the issue on which military concept developers and future plans strategists are focusing their time and mental energy. No matter what the executives, think tanks, and concepts and futures elements of joint and military service staffs decide with respect to U.S. strategic mobility, Pentagon programmers and budgeteers must win the prioritization battles with senior leaders to fund myriad, loosely connected, military components of capability woven together with those of other crucial JIIM-C partners. American strategic mobility has always been the differentiator for our military wins and losses, and our investments in its evolution will continue to play an essential role in determining where America stands geopolitically.

Some of the nation's best and brightest minds are applying excellent foresight to America's strategic mobility challenges through the congressionally mandated MCRS. Their work produces our best realm-of-the-possible recommendations with respect to what the nation's strategic mobility solution set needs to get the military to the fight based on combatant commanders' required force-flow timelines and likely scenarios. However, the MCRS must account for U.S. forces fighting their way to the fights and how that changes the required platforms and force structures.

The MCRS could recommend joint war-gaming and experimentation to include underway, Army live-fire, sealift emergency deployment readiness exercises (SEDREs). It could also recommend that DOD expand its demonstrations of concept technology and inclusion of interagency partners such as MARAD and the USCG in bolt-on/tied-down, Army-provided, cross-domain maritime operations. Given the divestment of tanks from the Marine Corps, the Army may want to experiment with a waterborne capability analogous to its current airborne and air assault capabilities. Recent training by Army tactical units through artillery live-fire operations from the well-deck of a small Army watercraft vessel is indicative of the problem sets and solutions in the Pacific that drive fully leveraged maritime-domain approaches to complex problems.

Shifting the armed services' approaches to how they meet their mission sets requires whole-of-government capability development to maximize return on taxpayer investments ahead of audits and accountability office inquiries. Services focus on modernizing "strike" capability within their specific domains of operation, but investments in "lift" or (more important) "movement and maneuver" capability must also keep pace.

The MCRS offers near-term context for a useful USTRANSCOM product that looks into mid-term and long-term prospects: the Future Deployment and Distribution Assessment (FDDA).[19] Senior DOD leaders and their staffs dedicate time and talent to making informed, bold, and audacious decisions to stay ahead of geopolitical waves and the operational implications of near-term, mid-term, and long-term strategic mobility. USTRANSCOM can help to lead thinking about how to improve, but stakeholders invest according to their individual risk-reward calculations and trade-offs based on their funding.

Importance of Assumptions

Assumptions are of fundamental importance to the planning of military operations and can skew the selection of the best course of action to pursue. The concepts, plans, studies, and assessments being deliberated will drive U.S. strategic mobility. In addition, the need to replace obsolescing inventory carries with it the opportunity not only to modernize equipment, but also to reimagine how our strategic mobility capabilities might better support the projection and sustainment of military power in a changed world.

Some assumptions that inform the MCRS, ongoing concept development, war-gaming and experimentation work, and future assessments must also consider the possibility of significant DOD budget austerity. Russia is proof that ingenuity is the product of austerity: Its new icebreaker ship, for example, also furnishes capability as a movement and maneuver (kinetic effect–capable) maritime-based missile launcher. More dual-purpose, covert, and nefarious coopting of traditionally benign transportation and enabling platforms for military utility, including strike capability, are forthcoming, and U.S. strategic mobility conceptualizers and planners should take note.

For Army early deployers like airborne and special operations forces, planning for contested deployments from home station to initial objectives has always been the norm, but that mindset and capability, depending on threats, risks, and windows of opportunity, expand in the force as strategic maneuver becomes scalable. As Major General Steve Farmen has said repeatedly, we will fight by, with, and through our ports. We find ourselves in this new operational reality because our adversaries are positioning themselves for success during competition so that they can prevail if competition evolves into armed conflict. Army planners would be wise to adopt a "home station = line of departure" mindset. In the past, the line of departure in potentially clashing with enemy forces was always drawn on a linear battlefield in a distant theater of operations beyond the unit's tactical assembly area. We no longer have that luxury.

From a survivability-move perspective, agility matters; maritime lift platform recapitalization, development, and fielding must focus on strategic maneuver and multi-domain operations; and mobility will increase the odds of survival in tomorrow's highly lethal environment. Agility matters especially for a maritime nation whose adversaries are astute and dynamic at weaponizing things to affect its economy, a linchpin of which is maritime commerce. More and more, adversaries will garner global reach with hypersonic-enabled warhead delivery, or electromagnetic gun delivery, or high-powered energy delivery, or cyber-delivery, or effects creation in any of the other domains within which we operate.

An example of the coopting of a ubiquitous, global transportation platform for covert missile launches is the innovative Russian Club-K containerized missile system that can be hidden in plain sight, most likely undetected, until it is employed.[20] Imagine the scenarios that could play out with just a few globally prepositioned or mobile Club-K systems leveraging trucks, trains, and maritime platforms.

Increasing Interdependence of Processes

Any evaluation of U.S. strategic mobility and Army deployment and redeployment must account for the effects of increasingly interdependent processes among JIIM-C stakeholder operations that must be planned, coordinated, and synchronized at echelon and scale to meet

contested and ever-compressing combatant commander force-flow requirements. Adversaries use disinformation operations against vulnerable components of military operations, such as the initial phases of deployments, coopting useful conduits on social media to foment social unrest, division, and obstructionism within the U.S. and its partners. They leverage proxy and organic military forces to produce both kinetic and "soft power" effects to interrupt force flows and have positioned themselves to pressure nations economically to hinder U.S. strategic mobility operations, applying all instruments of their national power against our ability to deploy and sustain combat forces rapidly and effectively.

We must rethink strategic mobility, our development of plausible scenarios, and our assumptions with an eye to developing concepts for joint, all-domain command and control. These concepts must anticipate JIIM-C and instantaneously formed and dissolved Combined Joint Task Forces, and they must be considered with a view to the execution of broad ranges of missions, from delivering humanitarian aid, consequence-mitigation rations, and rapidly developed and manufactured vaccines or other life-sustaining supplies and equipment in Air Mobility Command or Civil Reserve Air Fleet aircraft to rapidly forming and executing task forces in support of local law enforcement or LSCO.

Our current operating environment amplifies the importance of national stockpiles, strategic reserves, and prepositioned equipment and supplies as critical enablers of strategic mobility to garner tactical effects expeditiously at global points of need. Our developers of military concepts, particularly those developing the family of joint and service concepts such as the one that will address contested logistics, must account for great-power conflict, military workload for DSCA missions, and attrition in the organic industrial base.

Many American military leaders view strategic mobility as predominantly in the sustainment or logistics portfolio. This is a philosophical error that has negatively affected the focus, readiness, and degree of investment necessary to maintain dominance in strategic mobility on pace with adversary capabilities. Tomorrow's military operating environments will dictate a proper reconceptualization of deployment as a component of movement and maneuver—and therefore as a combat multiplier.

The first component of strategic mobility is deployment, which remains the principal task that underpins the movement-and-maneuver warfighting function, enabling a nation's forces to gain a positional advantage over those of an adversary. The strategic repositioning of the U.S. military's footprint from Europe to the United States after the end of the Cold War has made defending Eastern Europe from Russian military aggression exponentially more difficult.

With the clarity and focus of the National Security Strategy and National Defense Strategy, and given the stark realities that adversaries seek to disrupt deployment and sustainment operations across all domains, strategic mobility must be categorized within the Joint Staff as a movement-and-maneuver and force-application issue with prioritized requirements and investments commensurate with the criticality of the task. This necessary philosophical shift is resonating in the Pentagon as the realities of joint all-domain operations in great-power competition take root, and it has the potential to shape the next iterations of joint concept development.

The Joint Staff must renew its efforts to codify strategic mobility and deployment conceptually within the J/G-3 (plans and operations) staff sections rather than under the J/G-4 (logistics) staff section. Logisticians play a key, supporting role, but ownership and alignment of the "deploy" task, as a commander's first mission-essential task, must reside in the maneuver plans and operations staff sections of organizations.

Conclusion

I believe that we are training the next greatest generation of Americans not to storm distant beaches (though some levels

of amphibious assaults might be necessary), but rather to be experts in understanding and mastering the complex, interwoven "battlespace" of tomorrow's conflicts (and the condition-setting that is occurring during competition). Military planning for the next battles must take into account all of the tools and domains available to the U.S., as well as all of the ways by which they might be countered by the most sophisticated opponents.

American preeminence in the ability to deploy, employ, and sustain our military globally in concert with synchronized actions by other instruments of our national power underpins our position as a global superpower. Clausewitz tells us that "[w]ar is not merely a political act, but also a real political instrument, a continuation of political commerce, a carrying out of the same by other means."[21] Enhancement of our strategic mobility offers us a unifying, pressing, and foundational issue upon which JIIM-C stakeholders, both in America and in other like-minded nations, can move forward. It also will have widespread benefits across all aspects of American military power and extend into and across a broad range of industrial sectors—a win-win in anyone's book and a reasonable first step to ensure America's success in great-power competition.

Endnotes

1. *National Security Strategy of the United States of America*, The White House, December 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (accessed July 11, 2020), and James Mattis, Secretary of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, U.S. Department of Defense, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (accessed July 11, 2020).
2. U.S. Department of Defense, Joint Chiefs of Staff, Joint Publication 3-35, *Joint Deployment and Redeployment Operations*, January 10, 2018, p. I-7, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_35.pdf (accessed July 11, 2020).
3. U.S. Air Force, Air Mobility Command, "About Us," https://www.amc.af.mil/About-Us/ (accessed July 11, 2020).
4. Fact sheet, "C-130 Hercules," U.S. Air Force, Air Mobility Command, June 14, 2017, https://www.amc.af.mil/About-Us/Fact-Sheets/Display/Article/977514/c-130-hercules/ (accessed July 11, 2020); fact sheet, "C-17 Globemaster III," U.S. Air Force, Air Mobility Command, May 14, 2018, https://www.amc.af.mil/About-Us/Fact-Sheets/Display/Article/977489/c-17-globemaster-iii/ (accessed July 11, 2020); and fact sheet, "C-5 A/B/C Galaxy and C-5M Super Galaxy," U.S. Air Force, Air Mobility Command, December 18, 2017, https://www.amc.af.mil/About-Us/Fact-Sheets/Display/Article/977534/c-5-abc-galaxy-and-c-5m-super-galaxy/ (accessed July 11, 2020).
5. U.S. Department of Transportation, Maritime Administration, "Vessels of the Maritime Administration," last updated March 22, 2019, https://www.maritime.dot.gov/history/vessels-maritime-administration/vessels-maritime-administration (accessed July 11, 2020).
6. Associated Press, "China Home-Built Aircraft Carrier Tests Weapons at Sea," *Defense News*, June 1, 2020, https://www.defensenews.com/training-sim/2020/06/01/china-home-built-aircraft-carrier-tests-weapons-at-sea/#:~:text=BEIJING%20%E2%80%94%20China's%20Defense%20Ministry%20said,enhance%20training%20of%20the%20crew (accessed July 11, 2020).
7. Loren Thompson, "How the U.S. Navy's Aging Sealift Fleet Could Lose America's Next War in Eurasia," *Forbes*, January 21, 2020, https://www.forbes.com/sites/lorenthompson/2020/01/21/how-the-us-navys-aging-sealift-fleet-could-lose-americas-next-war-in-eurasia/#66a22f8027f6 (accessed July 11, 2020).
8. USTRANSCOM J37, *United States Transportation Command Comprehensive Report for TURBO ACTIVATION 19-PLUS*, December 16, 2019, Executive Summary, https://www.globalsecurity.org/military/library/report/2019/ustranscom_turbo-activation19-plus_aar_20191216.pdf (accessed July 11, 2020).
9. Richard Boudreaux and Amberin Zaman, "Turkey Rejects U.S. Troop Deployment," *Los Angeles Times*, March 2, 2003, https://www.latimes.com/archives/la-xpm-2003-mar-02-fg-iraq2-story.html (accessed July 11, 2020).
10. "American Merchant Marine at War: U.S. Merchant Marine Casualties During World War II," http://www.usmm.org/casualty.html (accessed July 11, 2020).
11. News release, "'Made in China 2025' Plan Issued," People's Republic of China, State Council, updated May 19, 2015, http://english.www.gov.cn/policies/latest_releases/2015/05/19/content_281475110703534.htm (accessed July 11, 2020).
12. Loren Thompson, "Coronavirus Highlights U.S. Strategic Vulnerabilities Spawned by Over-Reliance on China," *Forbes*, March 30, 2020, https://www.forbes.com/sites/lorenthompson/2020/03/30/coronavirus-highlights-us-strategic-vulnerabilities-spawned-by-over-reliance-on-china/?utm_source=Sailthru&utm_medium=email&utm_campaign=EBB%2003.31.20&utm_term=Editorial%20-%20Early%20Bird%20Brief#324ff1f69a1c (accessed July 11, 2020).
13. Kenneth Wykle, "The US Armed Forces Have a Mobility Problem," *Defense News*, August 14, 2018, https://www.defensenews.com/opinion/commentary/2018/08/14/the-us-armed-forces-have-a-mobility-problem/ (accessed July 11, 2020).
14. Kirk Moore, "Former U.S. Navy HSV-2 Swift Wrecked in Yemen Missile Attack," WorkBoat, October 7, 2016, https://www.workboat.com/news/bluewater/hsv-2-swift-wrecked-yemen-missile-attack/ (accessed August 21, 2020).
15. Mattis, *Summary of the 2018 National Defense Strategy of the United States of America*, p. 7.
16. "Power Conductor," interview with General Darren W. McDew, *Airman Magazine*, June 25, 2018, https://airman.dodlive.mil/2018/06/25/power-conductor/ (accessed July 11, 2020).
17. An example is the use of Marine Corps weapons platforms embarked aboard U.S. Navy amphibious ships to provide ship defense as in the case of the USS *Boxer* (LHD-4) during a recent deployment to the Persian Gulf. Ryan Pickrell, "Marines Sailed Through the Strait of Hormuz with an Armored Vehicle on the Boxer's Flight Deck," *Marine Times*, August 15, 2019, https://www.marinecorpstimes.com/news/your-military/2019/08/15/marines-sailed-through-the-strait-of-hormuz-with-an-armored-vehicle-on-the-boxers-flight-deck/ (accessed July 11, 2020).
18. Sean MacFarland, "Joint Operations Need a Guiding Hand," Association of the United States Army, February 25, 2020, https://www.ausa.org/articles/joint-operations-need-guiding-hand (accessed July 11, 2020).

19. Patrick McLeod, "Future Deployment and Distribution Assessment," Military Operations Research Society, MORS Symposium, January 26, 2011, https://apps.dtic.mil/dtic/tr/fulltext/u2/a540695.pdf (accessed August 20, 2020). See also "Far-Term Technology Focus: Future Deployment and Distribution Assessment (FDDA)," in U.S. Transportation Command, "Research, Development, Test, & Evaluation (RDT&E)," *USTRANSCOM Handbook* No. 60-2, July 22, 2016, p. 26, https://www.ustranscom.mil/cmd/associated/rdte/references/HB60-2.pdf (accessed August 20, 2020).
20. Michael Stott, "Deadly New Russian Weapon Hides in Shipping Container," Reuters, April 26, 2010, https://www.reuters.com/article/us-russia-weapon/deadly-new-russian-weapon-hides-in-shipping-container-idUSTRE63P2XB20100426 (accessed July 11, 2020).
21. Carl von Clausewitz, *On War*, trans. Col. J. J. Graham (London: Kegan Paul, Trench, Trubner & Co., 1918), Vol. 1, Ch. I, https://oll.libertyfund.org/pages/clausewitz-war-as-politics-by-other-means (accessed July 11, 2020).

The Intelligence Posture America Needs in an Age of Great-Power Competition

David R. Shedd

The United States faces an expanded national security landscape of threats that are interconnected by the rise of great-power competition from China, Russia, and their allies. The wide array of these threats to America's security will require our national defense and intelligence posture to adapt to a world that for nearly 20 years has been fixated on defeating international terrorists. For decades following the end of World War II and the onset of the Cold War, America's attention was focused almost entirely on the Soviet threat. Now our intelligence capabilities must be refocused to counter the global challenges to American national security interests from a rising China and an emboldened Russia in order to give decision-makers options for addressing the nefarious activities of these two great powers.

In the decades preceding the collapse of the Soviet Union, America's spies were almost singularly focused on collecting secrets on the USSR and its Communist allies. For the past two decades, however, U.S. intelligence agencies have been dedicated to thwarting international terrorism and supporting two long unconventional wars in Afghanistan and Iraq.

In the 1990s, intelligence capabilities were hollowed out by President Bill Clinton under the false premise of a "peace dividend" from a defeated Soviet Union. That assumption of a safer world proved false in the wake of the September 11, 2001, terrorist attacks. Almost immediately, America's slimmed-down Intelligence Community (IC) shifted its focus from nation-state threats posed by a rising China or a defeated Soviet Union to a new type of adversary. The events of 9/11 demonstrated that nontraditional enemies could do enormous damage to our way of life while expending few resources—either people or funds—in the process. After 9/11, the IC rallied to shift a shrunken resource base—people, secret collection, and analytic capabilities—and spent the next five years rebuilding itself to address the new threat of Islamic radicals.

Following those attacks, President George W. Bush called for a significant increase in resources for the IC, which had been starved by budget and personnel cuts during the 1990s. There was an immediate redirection of intelligence capabilities to confront a new and growing threat from international terrorism and a war in Afghanistan aimed at denying the terrorists a safe haven. The IC acted expeditiously and effectively to undertake the necessary shifts by becoming much more focused on finding terrorists and denying them the ability to plan and execute their attacks. The intelligence officer also moved to serve side-by-side with the warfighter, first in Afghanistan and then in Iraq after the U.S. invasion in 2003.

Obtaining intelligence to warn of, prevent, and respond to the actions of an adversary remains the core business of the IC. Yet America's intelligence agencies remain ill-postured to address the threats posed by China and a

reemergent Russia. These gaps must be closed while the IC continues to address the disruptive capabilities of non-state terrorist groups such as al-Qaida, ISIS, and Hezbollah.

Complicating the landscape, globalization is producing its own national security challenges. Propaganda campaigns to shape people's hearts and minds are but one example of the global nature of these challenges. The disinformation campaigns mounted by state and non-state players promoting unanticipated objectives leverage commercial mass-media outlets, further complicating the process of warning, preventing, and responding. The IC's shortfall in providing anticipatory warning about complex emerging threats is the result of insufficient resources. Even though the IC simply does not have sufficient capability and capacity to deal equally with every threat that America faces, it must adapt to this changing reality.

The 2017 National Security Strategy and the Intelligence Community

President Trump's 2017 National Security Strategy states that our national security requires that the U.S. be able to determine whether and where geostrategic and regional shifts are taking place that will threaten our interests. To that end, the strategy calls on the IC to collect, analyze, and develop options for the decision-maker to address the panorama of threats. Policymakers expect the IC to engage in aggressive collection of strategic-level intelligence that enables the anticipation of geostrategic shifts such as we see currently with China and Russia. At the same time, American intelligence also needs to obtain secret information essential to generating reliable tactical intelligence so that decision-makers can respond effectively to the actions and provocations of our adversaries.

The President recognizes that modernization of U.S. military forces to overmatch America's adversaries requires intelligence support. To have an improved capability, one has to have some idea of the opponent's capability. Moreover, the strategy underscores that "[i]ntelligence is needed to understand and anticipate foreign doctrine and the intent of foreign leaders, prevent tactical and operational surprise, and ensure that U.S. capabilities are not compromised before they are fielded."[1]

Adversaries like China and Russia are now mastering technology to build up their own capabilities, which in turn are used to undermine U.S. interests at home and abroad. These same adversaries are making significant investments in artificial intelligence (AI) and machine learning (ML) initiatives for processing and analyzing large quantities of data. Knowing specifically what our adversaries are doing requires that the U.S. IC be able to understand their languages in addition to having the expertise to understand the scientific and technical capabilities that they are pursuing. As they did during the Cold War, U.S. spy agencies need to attract and retain deep country and regional subject matter experts with ample foreign language capabilities and professional spies with technical proficiency in order to gain a significantly increased understanding of the intentions of China, Russia, and their allies.

Spy tradecraft—the art of collecting secrets—needs to be adapted to match today's threats. We know, for example, that China is investing vast sums of money in cutting-edge dual-use technologies that will enable the government to track its own citizens. These same technologies are being used to uncover the plans and intentions of China's adversaries including the U.S. A plan backed by Chinese President Xi Jinping illustrates just how critical technology development is to the Chinese government (and the Chinese Communist Party):

> China will invest an estimated $1.4 trillion over six years to 2025, calling on urban governments and private tech giants like Huawei Technologies Co. to lay fifth generation [5G] wireless networks, install cameras and sensors, and develop AI software that will underpin autonomous driving to automated factories and mass surveillance.[2]

Intelligence: What Is It and What Role Does It Play?

In the Intelligence Community, "intelligence" refers to a dynamic set of actions that relies on collection requirements established by the customers of intelligence, sharing the information within the IC so that various types of analysis can be performed, and then disseminating the results of insights to its customers. Former longtime intelligence professional Mark Lowenthal provides a classic definition of intelligence: "[I]ntelligence is the process by which specific types of information important to national security is requested, collected, analyzed, and provided to policymakers."[3] This essay focuses primarily on information as intelligence: that is, the macro-world of ideas, propaganda, and perception and how our adversaries are working to shape public perspectives on the larger strategic competition with the U.S.

From the standpoint of national security or military operations, intelligence needs to provide decision advantage: "Successful intelligence provides advantages to decision-makers they would not otherwise have, so an analyst must know the frame of mind of the decision-maker and the strategy to help the policymaker to succeed."[4] In other words, one obtains a better understanding of the competitor and is able to hide that advantage so that the competitor is unaware that his efforts have been compromised and his secrets discovered.

In his 2019 worldwide threats briefing to the U.S. Congress, then-Director of National Intelligence Daniel Coats described the nature of the emerging new threats:

> The post-World War II international system is coming under increasing strain amid continuing cyber and WMD proliferation threats, competition in space, and regional conflicts. Among the disturbing trends are hostile states and actors' intensifying online efforts to influence and interfere with elections here and abroad and their use of chemical weapons. Terrorism too will continue to be a top threat to US and partner interests worldwide, particularly in Sub-Saharan Africa, the Middle East, South Asia, and Southeast Asia. The development and application of new technologies will introduce both risks and opportunities, and the US economy will be challenged by slower global economic growth and growing threats to US economic competitiveness.[5]

The role of intelligence, whether it is providing information or identifying options for the policymaker or the military commander in the field, is to protect American interests at home and abroad. This is not new. What has changed is that intelligence must now be refocused to cover a more diverse and complex set of national security threats. U.S. intelligence faces expanded threats emerging from cyber warfare, adversarial use of AI and ML, space-based capabilities, and very sophisticated counterintelligence from competitor nations that are able to invest in the most advanced technologies.

The National Intelligence Strategy and the Intelligence Community

The IC published its *National Intelligence Strategy* (NIS) in 2019 to provide its workforce with strategic direction for the next four years. While the NIS does not outline specific priorities (these are kept classified), the strategy asserts that "all IC activities must be responsive to national security priorities." It further specifies that:

> All our activities will be conducted consistent with our guiding principles: We advance our national security, economic strength, and technological superiority by delivering distinctive, timely insights with clarity, objectivity, and independence; we achieve unparalleled access to protected information and exquisite understanding of our adversaries' intentions and capabilities; we maintain global awareness for strategic warning; and we leverage what others do well, adding unique value for the Nation.[6]

These four principles for the intelligence enterprise give the IC's rank and file a clear framework to adjust and identify needed resources to hone in collecting and analyzing the intentions and capabilities of near-peer adversaries.

To fully understand the challenges facing the Intelligence Community as it adapts to new circumstances, it is important to know its composition and how it is resourced. The IC is composed of 17 elements, including the Office of the Director of National Intelligence (ODNI).[7] Of these, eight reside within the Department of Defense (DOD),[8] a fact that underscores the importance of intelligence to America's defense posture and to the warfighter in particular. These elements operate in a federated fashion with each one receiving its own appropriated budget within the National Intelligence Program (NIP). Supplementing the NIP funds is the Military Intelligence Program applicable to some of the DOD-based intelligence elements.

The Director of National Intelligence (DNI), a position established by the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004,[9] is called upon to "lead a unified, coordinated, and effective intelligence effort. In addition, the Director shall…take into account the views of the heads of departments containing an element of the Intelligence Community and the Director of the Central Intelligence Agency" in guiding America's disbursed intelligence personnel and capabilities.[10]

A Tale of Intelligence Transformation: 2001 to the Present

America's spy agencies have evolved since their establishment over an extended period following World War II and during the Cold War with the USSR and its allies. A certain Sovietology discipline matured over the decades. The IC benefited from deep investments in language skills; deep development of expertise on Soviet political, military, and economic developments; and unique spy tradecraft driven by the need to develop, recruit, and handle Soviet and Soviet-bloc spies and ferret out spies working against the U.S. and its allies.

After the USSR collapsed, the U.S. no longer had a clearly defined adversary. This so-called peace dividend, combined with disinvestment in human talent and technical capacity, led in the 1990s to a significant reduction in the nation's intelligence capabilities. Then, when al-Qaeda attacked the homeland in 2001, the Bush Administration directed the IC to shift its focus to countering Islamic terrorism. Soon after the terrorist attacks, President George W. Bush assigned the Director of Central Intelligence, George Tenet, the de facto responsibility to become America's combatant commander for countering international terrorism while also serving as America's top intelligence officer. This informal designation for the DCI underscored the role that intelligence would play for years to come in the war on international terrorism.

The events of 9/11 provided an opportunity both to revitalize our nation's intelligence capabilities and to redirect resources to counter a very different type of adversary compared to the USSR during the Cold War. Acquiring new capabilities was given top priority. These capabilities included recruiting Arab, Farsi, Urdu, and other language proficient personnel, adapting technical collection to pursue geolocational discovery, augmenting tactical collection to identify small terrorist cells, and identifying clandestine Internet communications by Islamic extremists.

To address the redirection and rebuilding of intelligence capabilities in the aftermath of the attacks in 2001 and the ensuing wars in Afghanistan and Iraq:

> [T]otal intelligence spending grew by about 110% from 2001 to 2012. National defense excluding intelligence grew by 55% over that time period…. [W]hen measured from 1980, total intelligence spending by 2012 had grown 274%, while national defense spending without intelligence had grown 82% over that time period.[11]

Even with significant growth in the intelligence budgets, however, a side effect of the rise of counterterrorism as the top priority for America's intelligence agencies was to downgrade collection and analysis with respect to more traditional geopolitical issues around the globe. In effect, countering terrorist organizations became vastly more important than countering competitor countries.

The demand for battlefield-level intelligence increased significantly as American and coalition warfighters went into Afghanistan after late 2001 and after the 2003 invasion of Iraq. Geolocational data to detect the enemy's whereabouts was of paramount importance. Our already limited resources shifted further away from clandestine collection on China and Russia to focus on electronically intercepting terrorist messages, honing imagery collection at the battlefield level, and performing clandestine human intelligence at a more tactical level. The warfighter demanded that strategic-level intelligence collection be fused with field-level tactical collection and analysis to find and destroy the enemy on the ground.

American Intelligence in a Rapidly Changing World

As U.S. intelligence collection and analytical priorities shifted to address Islamic terrorism, those same enemies adapted their operational planning and activities. U.S. cyber-focused operations had to adapt to finding an enemy that was modifying its use of web-based presence to communicate, recruit terrorists, and launch propaganda operations. America's spies were essential to disrupting Islamic terrorists' communications and operational planning.

The buildup of counterterrorist (CT) capabilities is now useful in meeting the intelligence demands associated with today's world. For example, data analytics that was used in CT operations to identify and counter "fake news" now has widespread application in confronting the national security challenges we face from nation-state competitors.

Former National Counterterrorism Center Acting Director Russell Travers has noted that we "will never have enough analysts to process the available information so Artificial Intelligence and Machine Learning are not 'nice to have' they are an imperative." Travers quotes from the interim report of the National Security Commission on Artificial Intelligence:

> With respect to data, the government is well positioned to collect useful information from its worldwide network of sensors. But much of that data is unlabeled, hidden in various silos across disparate networks, or inaccessible to the government… Even more data is simply expelled as "exhaust" because it is not deemed to be immediately relevant.[12]

Travers adds that "[w]e have a long way to go to realize the benefits of Artificial intelligence and machine learning."[13] Data analytic processing that results in usable information for IC analysts will help to expand the range of available sources and in turn facilitate the dissemination of better "indications and warning"[14] to the customer.

Our adversaries, both state and non-state, are resilient and adaptable. They continue to invest in their own capabilities, ranging from cyber-focused operations to advanced weaponry, in order to upend our way of life and that of our allies. Our intelligence agencies must therefore continue their own journey of change—and in some instances transformation—to meet today's more complex national security threats and stay ahead of our adversaries. This includes a reexamination of how intelligence should be managed in a post-9/11 world:

> The U.S. Government must fundamentally reexamine the manner in which the Intelligence Community manages intelligence information. In many instances, the intelligence failures that preceded the terrorist attacks of September 11, 2001 were marked by an insistence—whether historically or legally grounded—that intelligence information must be tightly

controlled by the intelligence collector. Often, this position was based on a mistaken predicate, namely that an agency "owned" information that it had collected.[15]

The reforms in America's intelligence enterprise spurred by 9/11 focused on removing barriers to the sharing of two types of information by U.S. agencies: information collected outside the U.S. and information lawfully obtained inside the U.S. Before September 11, 2001, U.S. law (as it still does) prevented the Intelligence Community from conducting surveillance of U.S. citizens. Once granted legal authority pursuant to an investigation, U.S. law enforcement agencies could surveil citizens, but they could not share that information with the Intelligence Community.

The terrorist attacks of 9/11 showed that there was a gap between these two worlds where dangers inside and outside of the U.S. overlapped to create opportunities for enemies—opportunities about which the federal government was ignorant because of the prohibition on sharing information. The Intelligence Reform and Terrorism Prevention Act of 2004[16] led to improvements that made critical CT information more readily available to those charged with disrupting terrorist plots against the homeland, but better information sharing is still needed.

Designing and directing the nation's intelligence capabilities requires a resilient and committed IC leadership operating with a sense of urgency. America's adversaries are constantly and rapidly adapting their capabilities in cyber operations, social media, and other means of technology. American intelligence must remain focused on improving its own intelligence tool kit and staying ahead of the enemy, but that is not enough. America's intelligence agencies also need to pursue improvements in their business processes so that they not only can deliver better products to the decision-maker in a timelier manner, but also will be able to operate more efficiently and effectively if significant resource constraints reappear.[17]

Despite the IC reforms enacted post-9/11, additional action is needed. Collaboration among the spy agencies needs to improve. There is still a propensity among bureaucracies to avoid sharing information. The reasons for not sharing may include concerns by the agency that collected the information that the sensitive intelligence will be mishandled by other agencies and perhaps even leaked to the media or sourced in such a way that sensitive collection methods are exposed. Notwithstanding significant changes in how the spy agencies work today, the evolving threats to the nation require that the IC and its 17 elements continue to adapt.

One area of adaptation is technology itself. In order to be more effective in driving the integration of innovative technology within American intelligence, the IC must shift its culture mindset that expects any needed new technology to be developed within the community. The IC needs to welcome commercial technology solutions, modifying them as necessary to meet the mission requirements of the intelligence professionals.

The IC leadership should consider how best to shift resources and capabilities as they pertain to the adoption of technical capabilities (AI, ML, etc.) that can be applied to the rise of great-power competition. Oracle Cloud's Adaptable Business research project led to the interesting finding that business efficiency increases by 64 percent when the right technology is implemented alongside seven key cultural factors within an organization—all of which are factors that can be linked to characteristics in today's intelligence enterprise:

1. Flexibility and embracing change,
2. Learning culture,
3. Data-driven decision-making,
4. Open communication and collaboration,
5. Shared digital vision and participative leadership,

6. Entrepreneurial culture, and

7. Critical thinking and open questioning.[18]

According to the research, many organizations have invested in the right technologies but lack the culture, skills, or behaviors necessary to fully reap their benefits. The study found that business efficiency increases by only 27 percent when technology is implemented without the identified seven factors.[19]

America's intelligence professionals, in shifting their attention to the rising security threats posed by China, Russia, and their allies, are well postured to do so in only two out of the seven areas: critical thinking/open questioning and a learning culture. The IC as a whole is reluctant either to embrace open communication and collaboration across its 17 elements or to demonstrate flexibility and embrace change. The intelligence elements also fall short of applying data-driven decision-making at every level, having a shared digital vision, or promoting an entrepreneurial culture. If the Intelligence Community is to meet the challenges of the 21st century, its leaders need to address these shortfalls with a sense of urgency. If implemented, their strong and unwavering direction can offer opportunities to enhance the effectiveness of the IC's workforce.

The pivot of 2001 toward combating Islamic extremism as the top intelligence priority and away from a focused attention on the rise of China and the geopolitical aspirations of Russia has shaped the mindset of today's collectors. For example, for two decades, an entire generation of intelligence operators has not been schooled in how to conduct traditional operations against state actors, much less against our near-peer competitors. As a former CIA human intelligence operator observed in 2017:

> Over the past 15 years, this "global war on terror" mindset has become the default at the CIA. After accusations that it was stuck in the Cold War, the agency began to trade concealment devices and human sources for military hardware. Under a directive from President George W. Bush, it expanded its ranks to fight terror. It bulked up its abilities to track and target a dispersed enemy fighting an asymmetrical war. Gone were the days, it seemed, of risky brush passes in a heart-pounding, adrenaline-filled four-second period when an officer was "black"—meaning free, just for a moment, from hostile surveillance and able to pass a message to an asset. The Cold War was over; we had a new enemy to defeat.[20]

To address the security threats posed by China, Russia, and their allies effectively, our experienced operators and analysts must be reprioritized to meet customers' demands for accurate, relevant, and timely intelligence related to capable adversaries. These adversaries are not only capable of mounting complex operations against the U.S., but also able to detect sophisticated operational activities against them. Reflecting on the challenges posed by a rising power, Secretary of State Mike Pompeo has pointedly characterized the nature of the threats presented by a rising China:

> Under [Premier] Xi Jinping, the [Chinese Communist Party] has prioritized something called "military-civil fusion."... It's a technical term but a very simple idea. Under Chinese law, Chinese companies and researchers must—I repeat, must—under penalty of law, share technology with the Chinese military.
>
> The goal is to ensure that the People's Liberation Army has military dominance. And the PLA's core mission is to sustain the Chinese Communist Party's grip on power—that same Chinese Communist Party that has led China in an increasingly authoritarian direction and one that is increasingly repressive as well....[21]

Time to Accelerate Intelligence Transformation

Technology. The IC agencies are keenly aware that they are operating in a complex world of information technology that is changing rapidly. How America's spies respond to these changes is vital. The advent of fifth generation (5G) technology is on the verge of establishing China as a near-peer competitor in telecommunications. Although there are barriers to entry that limit Huawei's access to the U.S. market, the Chinese 5G footprint is expanding at a rapid clip around the world including among U.S. allies. The intelligence threat posed by Huawei is of a significance that should not be underestimated:

> As an adversarial power, China cannot be allowed to use its government-controlled companies to gain a significant foothold in the United States' burgeoning 5G wireless networks. Such a presence would be a clear national security threat that could decisively compromise American telecommunications and data infrastructure—including the communications integrity of the US military and intelligence community...
>
> The U.S. must not be complacent. Beijing's "civil-military fusion" practices must not be allowed to threaten U.S. national security. Further, the U.S. must penalize Beijing's blatant attempts to threaten America's critical infrastructure and to use its technology industry as an extension of state espionage.[22]

Technology is generally multipurposed and often integrated into multiple strands of hardware and software. For example, AI combined with ML can be incorporated into the daily use of intelligence capabilities to support analysis, counter cyber threats, and also address insider threats. Machine learning holds promise for cyber defense.

The single biggest challenge for network defenders is detection: finding the adversary's presence in one's own network. Detection times vary based on the sophistication of the attacker and defender, but the average lingers at well over a year. While defenders have improved, in many cases, intruders can operate for months within the target network, unnoticed and unconstrained.[23] As cybersecurity expert Ben Buchanan has noted:

> Virtually every major cyber attack—such as Stuxnet, the two blackouts in Ukraine, and NotPetya—has been preceded by months, if not years, of reconnaissance and preparation. This window offers an opportunity. If machine learning can improve detection, interdiction, and attribution, it can dramatically reduce the potential dangers of cyber operations. That said, machine learning has been applied to cyber defense for several years already and challenges persist; it is thus vital to ground the evaluation of machine learning-aided cyber defense not just in theory but in practical—and ideally measurable—results.[24]

Our intelligence professionals must have the very best technology at their disposal. Today, technological innovation rests predominantly in the private sector. To bridge this gap, IC leaders need to promote the development of deeper public–private partnerships to facilitate rapid adoption of this technology. Unfortunately, because of mutual distrust, these partnerships are not easy to forge. Nonetheless, commercial companies can help to find innovative ways both to exploit the vast and increasing body of open-source information available to the intelligence analyst and to counter the sophisticated counterintelligence methods employed by China, Russia, and others to protect their secrets.

As Russell Travers noted in 2019, at least one vehicle for such collaboration already exists:

> Over the past two years, there has been a marked increase in Industries' willingness to work with one another, the

> US government and foreign partners to counter terrorism through the Global Internet Forum to Counter Terrorism (GIFCT). Originally created by Facebook, Microsoft, Twitter and YouTube, GIFCT has provided a vehicle for discussions and potential information sharing....
>
> The recent move to establish GIFCT as an independent organization, or NGO, offers a formalized opportunity to better leverage the respective strengths of the private sector and the U.S. government against this dynamic problem. The new construct looks to sustain and deepen industry collaboration and capacity, while incorporating the advice of key civil society and government stakeholders.[25]

The IC leadership needs to adapt commercially available "off the shelf" technology, even if modifications may be required to meet a specific intelligence need. Simultaneously, the IC leadership should cut off funding for technology development within its agencies if it lags far behind what is available in the private sector. This also requires a change in the cultural mindset to make the IC more receptive to adopting commercially based technology. Former Intelligence Community Chief Information Officer John Sherman has underscored that:

> Our adversaries are moving out quickly in many areas such as cyber, artificial intelligence and machine learning, information and asymmetric warfare, not to mention other capabilities such as conventional weapons and space. We must respond with equal urgency. We can and must win in an arena increasingly defined by technology, data, and cybersecurity. This requires even greater innovation and partnerships between the government, industry, allies, and academia.[26]

The IC requires commercial support in developing computer infrastructure that allows collectors and analysts to tackle rough problems such as breaking sophisticated encryption related to leadership communications or advanced weapon systems and identifying denial and deception tactics by adversaries. These capabilities must be secure yet interoperable across intelligence and defense platforms.

Information Integration. Managing information sharing effectively in a classified world remains enormously challenging because of the need to protect our secrets. Nonetheless, the balance between "the need to share" and "the need to protect" is askew under the current paradigm among our intelligence professionals. It is imperative to have in place a data management system in which every person that touches a piece of classified information is monitored to ensure not only that mission needs are met, but also that secrets are protected.

IC analysts are inundated by information, but the most important information needed to "connect the dots" can remain undiscovered or unavailable because the right information is not always identified for the right user. Barriers to information sharing persist among analysts, operators, and military personnel even within the same agency and certainly between the IC's various elements. This shortfall must be addressed to improve the quality of analytic work. As Damien van Puyvelde, Stephen Coulthart, and M. Shahriar Hossain have argued:

> Interest in data analytics has been growing due to the demand for more reliable intelligence products following the controversies caused by the 9/11 attacks and the absence of weapons of mass destruction in Iraq. Prior to 9/11 the US intelligence community lacked and missed specific pieces of information pointing to the terrorist plot. In 2002, a national intelligence estimate made a series of erroneous assessments regarding Iraq's WMD programme, which were later used to justify the US decision to go to war in Iraq. These events cast doubt on the intelligence collection and analysis

> capabilities of America's spy agencies, especially in the domain of human intelligence (HUMINT). Big data capabilities, it was hoped, would compensate for the limitations, and sometimes the absence, of HUMINT. Consequently, US intelligence agencies began to embrace more systematic and sophisticated data collection and analysis techniques.[27]

Enacting user-based access controls across IC data repositories offers a way to take the human intervention out of the information-sharing conundrum when accompanied with data user rights. What good does it do for an analyst to learn after judgments have been made that information was available but could not be accessed because of artificial barriers? Information needs to be controlled, but in a world where threats are often interconnected, the barriers to accessing mission-relevant information need to be removed so that the IC can provide the most accurate assessments possible to policy customers.

Integrated intelligence assessments are equally important for all customers. This is underscored by the case of the U.S. military, which needs reliable intelligence to maintain situational awareness and be prepared to prevent war but, if necessary, to fight and decisively win the next one. With reference to the Army (although it is equally true for all of America's uniformed services):

> Army HUMINT must be prepared to operate within multiple domains and employ materiel modernization to leverage artificial intelligence/fusion capabilities to reduce cognitive burdens on analysts. The Army G-2X enterprise must adapt to meet the readiness demands of great power competition by ensuring our CI, HUMINT, and security personnel are prepared to deploy, fight, and win across the spectrum of conflict. Through modernization, the Army G-2X enterprise must be able to build an agile CI, HUMINT, and security force that fully embraces the Information Age, including leveraging technology to reduce cognitive burdens on the force and deliver intelligence at the speed of mission.[28]

The complexities associated with understanding, preparing, and as necessary responding to more sophisticated adversaries calls for the best possible integrated intelligence for our warfighters and planners.

Talent. Removing barriers to hiring and retaining America's top talent is essential to addressing complex national security challenges. The backbone of the IC's performance, effectiveness, and efficiency is the quality and retention of its people. The good news is that the IC has no problem attracting prospective personnel with extraordinary skills and backgrounds. The bad news is that the IC lacks the ability to hire them quickly enough, and significant expertise is lost because the hiring process can takes as much as a year. Also, once in the IC, talented officers leave because they become disaffected by bureaucracy that discourages analytic dissent or by elements that discourage joint-duty career-enhancing assignments among the IC's 17 components.

As it relates to attracting and retaining the best and brightest personnel for the IC, two significant barriers need to be addressed.

First, the granting of a security clearance for an intelligence professional and/or supporting government contractor with the requisite skills remains inefficient despite some gradual improvements. In figures released in late November 2019, the Defense Counterintelligence and Security Agency "noted a dramatic drop in security clearance processing times as of FY 2019 Q4—295 days for Top Secret clearances (down from a high that reached over 500 days), and 181 days for Secret security clearances, down from over 300 days." These "DoD/Industry only numbers…represent the fastest 90% of all clearances."[29] However, the most talented professionals are not likely to wait a year or longer to start their jobs.

Second, when the time it still takes to get a security clearance is combined with the time

needed for a hiring decision—often more than a year—it is not hard to see why the new graduate in one of the highly sought-after technology fields may well not wait to be hired by an intelligence agency. It often takes much longer for first-generation American applicants with highly desirable native foreign language skills to be cleared. It is difficult to quantify the loss of talent and capability this represents, but we can assume that the Intelligence Community does lose badly needed talent.

A case study of graduates from the North Carolina State University Master's Program in Advanced Analytics provides some insights. If a graduate of this 10-month program were interested in a career in national security, it would be next to impossible for that individual to be interviewed, offered a job, and cleared through the process in less than 10 months. Even assuming a somewhat faster hiring process, 40 percent of those hired will leave their employment within two years because of perceived opportunities for job growth elsewhere—obviously a huge loss for any intelligence agency. Many leave for the private sector.[30]

Suitability Barriers to IC Talent Management. Different suitability norms ("suitability" refers to judgments about a person's character traits and conduct) among the IC elements act as a significant constraint on the movement of talent within the IC to meet the highest intelligence priorities. This obstacle also undermines IC team building. The receiving element often raises subjective objections under the guise of finding the prospective person "unsuitable" for the rotational assignment even though the criteria for security clearance are the same for all IC personnel. The resultant delays, often measured in months, undermine the use of the best talent despite IC mission requirements.

This obstacle must be removed if the IC is going to be able to place its talent where it is most needed to meet the requirements of the nation's political or military leadership and prioritize resource allocations to match the greatest threats that appear on the horizon. Removing the suitability barriers to transfers of IC personnel would also remove an important reason for the IC's talent drain. The ODNI should establish policies that significantly reduce what are often many months of delay in having personnel move from one IC element to another.

The Changing Persona of Clandestine Collection. The advent of biometrics and other threats to secure operation make obtaining core secrets from clandestine human sources extraordinarily challenging. Many of the technologies used by intelligence professionals are readily available to our adversaries, state and non-state alike. Facial recognition and biometrics more generally make the use of alias operational tradecraft nearly impossible. Human intelligence collection must therefore continue to evolve both to address the counterintelligence threats to securely running foreign human spies and to protect its own operational capabilities from the watchful eye of our adversaries.

A major shift in how human intelligence operations are conducted is required. While not easy, and while tradecraft must be applied, online (or cyber-based) human intelligence operations must be increased to spot, assess, develop, recruit, and handle human sources. At the same time, human-to-human interaction in a clandestine manner faces significant hurdles. "U.S. spies are no longer being tailed by foreign governments in about 30 different countries," according to one report, "because advances in facial recognition, biometrics and artificial intelligence have made it almost impossible for the agents to [maintain a false identity]."[31] One former CIA senior officer noted insightfully in 2015 that:

> As we continue to advance technologically, in essence making our world smaller, the potential threats posed by these advancements will make both protecting and exploiting real secrets exponentially more difficult. In addition, as these challenges continue to grow, those tasked with addressing them will need to adjust at a much more rapid rate. This applies

> both to field operatives as well as to their managers...
>
> The next generation of operatives and their managers will need to be more familiar with, if not adept at, technological augmentation. Augmentation, not replacement. While the tendency to rely increasingly on technology to make HUMINT collection more efficient is commendable, adherence to the core principals [*sic*] will ensure that human operations remain as secure as possible.[32]

Cyber Integration. The DNI has the authority to assign responsibilities within the IC, but the absence of clear policy direction on cyber issues leaves intelligence professionals without the guidance they need with respect to the parameters of their cyber activities. In addition, because of the absence of a policy framework, the IC elements, alongside other elements of the executive branch, have been left to chart their own courses as individual departments or agencies in executing offensive and defensive cyber activities as an element of U.S. national security.[33]

Adversarial threats in the cyber domain change quickly and are increasingly complex. As for the appropriate governance to meet cyber threats, Executive Order 12333, as amended by President George W. Bush in July 2008,[34] did not specifically address cyber as an intelligence discipline. Nonetheless, in just the few years since the IC's principal presidential directive was amended, it has become apparent that specific cyber "lanes in the road" need to be identified within the IC and throughout government.

Cyber intelligence informs a significant number of sub-disciplines such as cyber security, cyber defense, cyber offence, and cyber support to traditional military operations, as well as the establishment of international norms on cyber behavior during peacetime. These missions call for intelligence professionals who are competent to address the multi-strand demands associated with cyber operations, but there is a critical shortage of cyber talent in the public sector as it competes with private industry because demand for the unique skills and knowledge needed to combat the growing threats in the cyber domain has outpaced the supply of that talent for years. The public sector struggles to attract the required numbers of cyber-trained and experienced personnel because of its slow hiring process and lower compensation compared to the private sector.[35] For example, February 2015, the Pentagon had reached only the midway point in staffing Cyber Command and was backing away from the long-held goal of deploying a full force of 6,000 cyber personnel by 2016.[36] As a top priority, the IC must spend whatever is necessary to train existing IC officers with transferable skills and high potential to be cyber intelligence officers. Training is available in the private sector.[37]

Executive Order 12333 as amended gives the DNI the authority to define roles and responsibilities for elements of the Intelligence Community.[38] What is needed now to achieve enhanced integration among the key cyber collection agencies—the National Security Agency, Central Intelligence Agency, and Federal Bureau of Investigation—are clearly articulated policies for defining their respective missions and how information will be shared among them in a transparent manner. The IC leadership needs to remain focused on achieving "unity of cyber mission," which must be the top priority for anticipating and providing warning to the decision-makers about future threats. Under well-defined rules, the Cyber Threat Intelligence Integration Center (CTIIC) may eventually be in a position to contribute a strong analytic product on cyber threats.

Some progress has been made, but it is not enough. Cyber legislation was stalled for years, but with passage of the cyber bill in 2015, a framework for addressing cyber-related activities has begun to take form.[39] The CTIIC, established at the instigation of the White House ostensibly to conduct analysis of cyber threats, appears to have an ill-defined mission. It also has neither the resources nor the standing among the big departments and agencies to assess cyber threats.[40]

Counterintelligence. Catching spies and protecting our secrets is the traditional framework for counterintelligence. In order to counter highly sophisticated adversaries, however, the scope of counterintelligence needs to be expanded. This broader definition needs to include what our adversaries are doing through disinformation and other forms of information warfare to undermine both the U.S. and its friends and allies. IC talent needs to be placed against this broader definition of counterintelligence.

While the Chinese, Russians, and other adversaries have long wanted to steal our secrets by any means possible, these nations now leverage big data to promote their interests, using all forms of media to foster a false narrative of events in and outside the U.S. Counterintelligence requires identifying and then protecting our national security information on a much broader level. CI must still include its traditional focus on protecting our own secrets from foreign spies, but our security also depends on identifying and countering disinformation and insider threats, as well as responding to adversaries' efforts to disrupt U.S. intelligence. As Christopher Costa and Joshua Gelzter have written:

> If the U.S. government is to fight off disinformation—which can now be created on an industrial scale and spread globally not just by states but also by terrorists and criminals—it must reinvigorate and broaden the practice of counterintelligence.
>
> For too long, the focus of U.S. counterintelligence has been safeguarding government secrets and corporate intellectual property, particularly by thwarting foreign efforts to recruit potential thieves. We must remember that counterintelligence also means warding off efforts to divide and weaken us. We can draw on our Cold War experience and update our responses to reflect modern technologies.[41]

Today, "Moscow and other governments are learning key disinformation tactics from non-state actors" that are using more sophisticated cyber-generated influence operations. All adversaries are now in the cyber domain.

> These developments suggest a future in which both non-state and state actors will contest the United States through online disinformation campaigns, even while more traditional global power competition tied to geography continues to play out. Moreover, it seems inevitable that the Chinese, Iranians, and others will escalate their malign social media efforts much as the Russians have done. FBI Director Christopher Wray recently acknowledged that other countries have been exploring such influence efforts.[42]

The opportunities for the IC to identify and then counter the broad range of counterintelligence threats are coupled with the challenges and opportunities related to technology, information integration, people talent, and clandestine collection. All of these pieces must fit together to maximize the ability of our spy agencies to respond to a much higher national security threat environment for years to come. An effective response to these threats does not require additional funding or personnel resources for the IC, but rather reprioritization of existing capabilities.

Building a More Effective Intelligence Enterprise

As demonstrated after the terrorist attacks of 2001, the U.S. Intelligence Community has demonstrated that it can redirect its resources to meet a different type of threat. It did so immediately in the aftermath of the attacks in 2001 in order to pursue aggressive collection and analysis of Islamic terrorist groups. The goals for intelligence are immutable. Intelligence resources must be postured to give the policymaker and warfighter alike the upper hand against the adversary. That upper hand requires collecting threat warnings that can be

prevented from becoming a reality or be countered by reliable intelligence.

The ability of America's spy agencies to address the wide array of complex threats emerging from the need to deter great-power rivals requires IC leadership committed to applying the resources to address the highest threat vectors. It requires a strong sense of urgency with a top goal of harnessing the power of emerging and disruptive technologies as applied to data analytics, artificial intelligence, machine learning, 5G, and quantum computing while enabling the integration of autonomous systems. Currently, America's intelligence professionals must be prepared to ensure unambiguous advantage in the event of conflict escalation, but the IC needs to be able to act preemptively and provide advance warnings of threats to our national security from both state and non-state actors.

With this in mind, there are several actions that can and should be taken. Specifically:

- **The Director of National Intelligence should require all IC members to provide a plan with specific goals to increase their partnerships with the private sector to acquire cutting-edge technology and infrastructure support.** Each plan should be accompanied by a road map and timetable for adoption of that technology. In an era of significant growth in data and data processing requirements, America's intelligence professionals require the best technology that the private sector has to offer. They should therefore promote agile public–private partnerships to assure their access to the technological innovation that is constantly emerging from America's vibrant commercial sector.

- **The DNI needs to establish a needs-based information-sharing model with appropriate auditing functions to enable enhanced data access by all intelligence professionals with a need to know.** Notwithstanding advances over the past two decades, mission-essential information sharing remains too restricted within the IC due to the propagation of data stovepipes and absence of user-based permissions. Fear continues to drive the risk calculus by the so called owners of data (the agencies that obtain the classified information). The result could be failure to provide adequate warning because mission users are unable to access siloed information.

- **For the Top Secret/Sensitive Compartmented Information clearance, the DNI should mandate and then rigorously enforce time constraints on the security clearance process.** The IC must depend on state-of-the art CI monitoring for its first ring of protection. Therefore, bureaucratic barriers that prevent the timely entry of much-needed talent must be eliminated, and every effort must be made to retain vital personnel and to facilitate ingress to and egress from the IC for that talent. Special allowances are needed for compensation related to highly desirable science, technology, engineering, and mathematics (STEM) talent. Interchangeability of intelligence personnel talent must be promoted aggressively among the 17 elements of the IC to meet the highest intelligence requirements. Suitability barriers to accepting transfers of personnel need to be removed.

- **Clandestine human intelligence collection needs to reevaluate how it can identify, assess, develop, and recruit foreign spies by using different tactics.** Human intelligence operations can no longer rely solely on traditional tradecraft for in-person meetings using alias personas that are subject to discovery because of microchip information and biometrics. A comprehensive revamping of clandestine human intelligence collection is needed. Today's threats to traditional spying will require far more reliance on

online cyber personas and far less reliance on foreign-based collection efforts by American operators.

- **The Acting DNI took an important step in mid-May with the announcement that intelligence-focused cyber efforts would be consolidated under an IC Cyber Executive.** However, this does not go far enough to meet the challenges of cyber-centric requirements. The IC's capabilities against determined adversaries now need to be rigorously assessed with a view to ensuring the IC's ability to defend and respond as necessary to an adversary's capabilities in cyberspace.

- **The DNI needs to lead in expanding the scope and depth of America's counterintelligence focus to address our adversaries' ability to use aggressive cyber online operations to influence the hearts and minds of Americans.** This expanded application of CI can meet the continued need to address more complex challenges pertaining to insider threats in a cyber-centric world and the need to protect national security secrets.

Conclusion

The foundation of U.S. intelligence is sound, but America's intelligence agencies face a range of new national security challenges from emerging great-power competitors. To meet these challenges, the IC needs to attract and retain deep subject matter expertise, including foreign languages, and to focus on China and Russia (and their allies), enhanced operational tradecraft, and a significant increase in the use of technology and STEM-trained personnel to apply artificial intelligence, machine learning, and data analytics in an effective manner. Cyber-centric operational capabilities for U.S. intelligence personnel must become the norm for achieving success against determined and relentless adversaries.

The Intelligence Community, with the benefit of clearly articulated requirements from the policymaker and the warfighter, is capable of delivering invaluable intelligence. This requires bold leadership that is prepared to invest in its people, technology, and security. The leadership needs to incentivize the increase of IC integration and strengthen public–private partnerships to maximize access to innovative technologies.

The challenges facing our intelligence professionals are not for the faint of heart. Dealing with these challenges will require creativity and meaningful steps to break down the bureaucratic walls among the IC's 17 elements. America's national security deserves nothing less than a federated Intelligence Community that operates with unity of effort and interdependence, confronting the capabilities of our adversaries with an eye to providing high-confidence decision advantage for every customer of the world's finest intelligence organizations.

Endnotes

1. *National Security Strategy of the United States of America*, The White House, December 2017, p. 32, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (accessed June 17, 2020).
2. Bloomberg News, "China's Got a New Plan to Overtake the U.S. in Tech," updated May 21, 2020, https://www.bloomberg.com/news/articles/2020-05-20/china-has-a-new-1-4-trillion-plan-to-overtake-the-u-s-in-tech (accessed June 17, 2020).
3. Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 2nd ed. (Washington: Congressional Quarterly Press, 2003), p. 8.
4. Jennifer E. Sims, "Decision Advantage and the Nature of Intelligence Analysis," Chapter 24 in *The Oxford Handbook of National Security Intelligence*, ed. Loch K. Johnson (New York: Oxford University Press, 2010), Abstract, https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780195375886.001.0001/oxfordhb-9780195375886-e-0024?result=4&rskey=0ztes9 (accessed July 26, 2020).
5. Daniel R. Coats, Director of National Intelligence, "Worldwide Threat Assessment of the US Intelligence Community," statement before the Select Committee on Intelligence, U.S. Senate, January 29, 2019, p. 4, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf (accessed June 17, 2020).
6. Office of the Director of National Intelligence, *National Intelligence Strategy of the United States of America*, 2019, p. [1], https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf (accessed June 17, 2020).
7. The Office of the Director of National Intelligence; the Central Intelligence Agency (other than the ODNI, the only element of the IC that is outside of a department); the National Security Agency; the Defense Intelligence Agency; the National Geospatial Agency; the National Reconnaissance Office; the four intelligence elements of the Army, Navy, Air Force, and Marine Corps; the Federal Bureau of Investigation's National Security Branch; the Department of State's Bureau of Intelligence and Research; the Department of the Treasury's Office of Intelligence and Analysis; the Drug Enforcement Administration's Intelligence Program; the Department of Homeland Security's Office of Intelligence and Analysis; the Department of Energy's Office of Intelligence and Counterintelligence; and U.S. Coast Guard Intelligence.
8. The National Security Agency, the Defense Intelligence Agency, the National Geospatial Agency, the National Reconnaissance Office, and the four intelligence elements of the Army, Navy, Air Force, and Marine Corps.
9. S. 2845, Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458, 108th Cong., December 17, 2002, https://www.congress.gov/search?q=%7B%22search%22%3A%22cite%3APL108-458%22%7D (accessed July 17, 2020).
10. Executive Order 13470, "Further Amendments to Executive Order 12333, United States Intelligence Activities," July 30, 2008, in *Federal Register*, Vol. 73, No. 150 (August 4, 2008), p. 45326, https://fas.org/irp/offdocs/eo/eo-13470.pdf (accessed July 17, 2020).
11. Marshall C. Erwin and Amy Belasco, "Intelligence Spending and Appropriations: Issues for Congress," Congressional Research Service *Report for Members and Committees of Congress*, September 18, 2013, p. 6, https://fas.org/sgp/crs/intel/R42061.pdf (accessed June 17, 2020).
12. Russell E. Travers, Acting Director, National Counterterrorism Center, "Counterterrorism in an Era of Competing Priorities," remarks delivered at Washington Institute for Near East Policy, November 8, 2019, p. 8, https://www.dni.gov/files/NCTC/documents/news_documents/Travers_Washington_Institute_Remarks_as_Prepared.pdf (accessed July 17, 2020). Punctuation as in original.
13. Ibid.
14. "Indications" are signs or evidence that reveal an entity's intent to perform some act, and "warning" connotes an immediacy of action that poses a danger. The unexpected recall of soldiers from leave or movement of supply trucks to an area indicate that an opponent is up to something of importance per an IC analytic customer's stated interests. Similarly, the movement of fueling vehicles to a missile launch pad is a sign or warning that the launch of a missile is imminent.
15. Senate Report 108-258, *To Authorize Appropriations for Fiscal Year 2005 for Intelligence and Intelligence-Related Activities of the United States Government, the Intelligence Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for Other Purposes*, 108th Cong., 2nd Sess., May 5, 2004, p. 7, https://www.congress.gov/congressional-report/108th-congress/senate-report/258/1?s=1&r=42 (accessed July 17, 2020).
16. See note 9, *supra*.
17. David R. Shedd, "Intelligence and National Defense," in *2016 Index of U.S. Military Strength*, ed. Dakota L. Wood (Washington: The Heritage Foundation, 2015), pp. 45–59, https://s3.amazonaws.com/ims-2016/PDF/2016_Index_of_US_Military_Strength_FULL.pdf (accessed July 17, 2020).
18. Oracle Cloud, "Adaptable Businesses and the Productivity Paradox," in *The Adaptable Business: Future Skills and Cultural Forces*, 2019, pp. 3 and 11, https://www.oracle.com/a/ocom/docs/dc/the-adaptable- business.pdf?elqTrackId=28c5abc9c44d4a5d872b2e6cd1a92c68&elqaid=79966&elqat=2 (accessed July 17, 2020).

19. Ibid., p. 3.
20. Alex Finley, "How the CIA Forgot the Art of Spying," *Politico Magazine*, March/April 2018, https://www.politico.com/magazine/story/2017/03/cia-art-spying-espionage-spies-military-terrorism-214875 (accessed July 17, 2020).
21. Secretary of State Michael R. Pompeo, "Technology and the China Security Challenge," remarks delivered at the Commonwealth Club, San Francisco, California, January 13, 2020, https://www.state.gov/silicon-valley-and-national-security/ (accessed July 17, 2020).
22. Klon Kitchen, "The U.S. Must Treat China as a National Security Threat to 5G Networks," Heritage Foundation *Issue Brief* No. 4952, April 16, 2019, p. 1, https://www.heritage.org/technology/report/the-us-must-treat-china-national-security-threat-5g-networks.
23. FireEye, *M-Trends 2020*, FireEye Mandiant Services *Special Report*, p. 11, https://content.fireeye.com/m-trends/rpt-m-trends-2020 (accessed June 16, 2020).
24. Ben Buchanan, "A National Security Research Agenda for Cybersecurity and Artificial Intelligence," Center for Security and Emerging Technology *Issue Brief*, May 2020, p. 7, https://cset.georgetown.edu/wp-content/uploads/CSET-A-National-Security-Research-Agenda-for-Cybersecurity-and-Artificial-Intelligence.pdf (accessed July 17, 2020). See also Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations* (New York: Oxford University Press, 2017), Chapter 2.
25. Travers, "Counterterrorism in an Era of Competing Priorities," p. 12.
26. John B. Sherman, Assistant Director of National Intelligence and Intelligence Community Chief Information Officer, "From the IC CIO," in Office of the Director of National Intelligence, "Strategic Plan to Advance Cloud Computing in the Intelligence Community," June 26, 2019, p. 1, https://www.dni.gov/files/documents/CIO/Cloud_Computing_Strategy.pdf (accessed July 17, 2020).
27. Damien van Puyvelde, Stephen Coulthart, and M. Shahriar Hossain, "Beyond the Buzzword: Big Data and National Security Decision-Making," *International Affairs*, Vol. 93, No. 6 (November 2017), p. 1398, https://www.chathamhouse.org/sites/default/files/images/ia/INTA93_6_06_VanPuyvelde%20et%20al.pdf (accessed July 17, 2020).
28. Lieutenant Colonel Marcus O'Neal, "Army G2X Support to Army Readiness and Modernization Priorities," *Military Intelligence Professional Bulletin*, Vol. 46, No. 1 (January–March 2020), p. 23, https://fas.org/irp/agency/army/mipb/2020_01.pdf (accessed July 17, 2020).
29. Lindy Kyzer, "How Long Does It Take to Process a Security Clearance? (Q4 2019)," ClearanceJobs, November 20, 2019, https://news.clearancejobs.com/2019/11/20/how-long-does-it-take-to-process-a-security-clearance-q4-2019/ (accessed July 17, 2020).
30. Institute for Advanced Analytics, "Master of Science in Analytics: 2019 Alumni Report," reported as of January 4, 2020, http://analytics.ncsu.edu/reports/alumni/MSA2019.pdf (accessed July 17, 2020).
31. Emily Crane, "Will the Digital Age Kill Off Spying? CIA in Crisis as Facial Recognition, Biometrics and AI Make It Increasingly Difficult for Agents to Maintain Their Cover Abroad," *The Daily Mail*, December 30, 2019, https://www.dailymail.co.uk/news/article-7837767/CIA-faces-crisis-intelligence-gathering-digital-footprints.html (accessed July 17, 2020).
32. John Sano, "The Changing Shape of HUMINT," *The Intelligencer: Journal of U.S. Intelligence Studies*, Vol. 21, No. 3 (Fall/Winter 2015), pp. 79–80, https://www.afio.com/publications/SANO%20John%20on%20The%20Changing%20Shape%20of%20HUMINT%20Pages%20from%20INTEL_FALLWINTER2015_Vol21_No3_FINAL.pdf (accessed July 17, 2020).
33. See U.S. Government Accountability Office, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, GAO-13-187, February 2013, https://www.gao.gov/assets/660/652170.pdf (accessed July 17, 2020).
34. See note 10, *supra.*
35. Amber Corrin, "Is There a Cybersecurity Workforce Crisis?" *Federal Computer Week*, October 15, 2013, https://fcw.com/articles/2013/10/15/cybersecurity-workforce-crisis.aspx (accessed July 17, 2020).
36. Aliya Sternstein, "Need a Job? Cyber Command Is Halfway Full," Nextgov, February 6, 2015, http://www.nextgov.com/cybersecurity/2015/02/need-job-cyber-command-halfway-full/104817/ (accessed July 17, 2020).
37. See, for example, SANS Institute web site, www.sans.org (accessed July 17, 2020).
38. *Federal Register*, Vol. 73, No. 150 (August 4, 2008), pp. 45326–45327.
39. Rob Lever, "Congress Passes Long-Stalled Cybersecurity Bill," *Space War*, December 18, 2015, http://www.spacewar.com/reports/Congress_passes_long-stalled_cybersecurity_bill_999.html (accessed July 17, 2020).
40. "Fact Sheet: Cyber Threat Intelligence Integration Center," The White House, February 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center (accessed July 17, 2020).

41. Christopher P. Costa and Joshua A. Geltzer, "To Fight Disinformation, Rethink Counterintelligence," *Defense One*, October 14, 2019, https://www.defenseone.com/ideas/2019/10/fight-disinformation-rethink-counterintelligence/160582/ (accessed July 17, 2020).
42. Ibid.

U.S. Alliances: Crucial Enablers in Great-Power Competition

Andrew A. Michta, PhD

The United States today is at a geostrategic disadvantage that is significantly greater than the "correlation of forces" (as Soviet generals put it) that the U.S. confronted during the Cold War. Unlike in the era of great-power competition with the Soviet Union when the U.S. faced a single geopolitical foe, today America is confronted by two great powers—one revisionist, the other transformational—aligned in the common goal of displacing the United States from its dominant position as the hub of the liberal world order.

Three decades of unequivocal and misguided commitment to globalization and the internationalization of our manufacturing have left America's power significantly depleted. The post–Cold War era has seen persistent budget and trade deficits, deindustrialization and the attendant radical centralization of supply chains in China, and an overall decline in the competitiveness of the American labor force, with U.S. STEM (science, technology, engineering, and mathematics) programs at premier universities increasingly catering to foreign students, fewer of whom are choosing to remain and work in the United States after graduating. At the same time, two decades of low-intensity wars-cum-"state building" projects in Afghanistan and the Middle East have depleted the capabilities of the U.S. military, and the demands of these theaters have driven a large portion of defense systems acquisition programs and contracting.[1]

The Grand Strategic Challenge

Meanwhile, the Russian Federation has undergone two cycles of military modernization. The scope of this effort may pale in comparison to expenditures by the United States, but two decades of *de facto* disarmament by our European allies have allowed Moscow to change the balance of power along NATO's eastern flank.

More important, China's investment in its military—especially qualitative improvements facilitated by massive technology transfers from the United States and increasingly from Europe, as well as the rapid expansion of its navy—has begun to tilt the balance of power in the Indo-Pacific region against the United States, with the People's Liberation Army Navy (PLAN) staking an exclusive claim to the South China Sea. While the PLAN is already challenging the sovereignty of Taiwan and putting Japan on notice that its security can no longer be taken for granted, it is also increasingly operating in the Mediterranean, entering the Baltic Sea, and—with its tenders to buy 33,000-ton

Andrew A. Michta, PhD, is the Dean of the College of International and Security Studies at the George C. Marshall European Center for Security Studies. The views presented are those of the author and do not necessarily reflect those of the George C. Marshall European Center for Security Studies, the Department of Defense, or the United States Government.

nuclear-powered icebreakers—preparing to punch through the Arctic Ocean.

Last but not least, China's Belt and Road Initiative (BRI), with some 50 "special economic zones," and its "17+1" initiative are critical steps toward tying the economies of Europe, Russia, and Africa to China as part of China's larger effort to form a single Eurasian supply-chain network. Once in place, centered on the yuan as the new reserve currency and defended by Chinese military power, the BRI will be poised to effect a "grand inversion" in which the maritime supremacy over the land domain that for half a millennium has favored the West would effectively be reversed. In such a scenario, the European Rimland would cease to be the transatlantic gateway to Eurasia, becoming instead the terminal endpoint of a China-dominated Eurasian empire.

In short, the grand strategic challenge that this round of great-power competition poses for American security and for the democratic West (as well as democracies in Asia) cannot be overstated. Consequently, the role of alliances as a fundamental enabler of American power will be critical in the next decade and beyond.

The Trump Administration's realignment of U.S. national security and defense priorities toward great-power competition is encapsulated in the 2017 *National Security Strategy*[2] and the 2018 *National Defense Strategy*.[3] Both documents (the latter's unclassified 12-page summary having been released by then-Secretary of Defense James Mattis) were long overdue, as changes in the balance of power worldwide have only accelerated following the 2008 "great recession" that exposed deep structural imbalances in the United States economy. Although the United States government managed to stabilize the situation by flooding the markets with liquidity in the aftermath of that crisis, the structural deficiencies of the U.S. economy—especially our excessive reliance on foreign supply networks for ever-greater portions of the economy, including military contracting—were not addressed.

This weakness was exposed during the devastating aftershocks of the Wuhan coronavirus pandemic, with the United States learning the hard way how vulnerable it had become to its principal adversary, China, on account of Beijing's radical centralization of supply chains for products critical to dealing with the crisis. The pandemic has made it imperative that the United States relearn the lesson of the importance of allies who can provide diffuse and redundant supply chains in critical areas while also serving as key enablers for the United States when it comes to its foreign and security policy.

NATO

No alliance proved more essential to the United States' victory in the Cold War than the North Atlantic Treaty Organization, and no other alliance is in greater need of repair today. In the first few decades following the Cold War, NATO devolved into an essentially political structure used to integrate post-Communist states into the transatlantic system and, although membership in the European Union was never expressly conditioned on NATO membership, to help lay the groundwork for the EU's *acquis communautaire*.[4] In the first decade of the 21st century, the alliance became, on the one hand, a growing source of friction between the United States and the largest European allies while, on the other hand, old allies such as the United Kingdom and new ones, including Poland, enabled the United States' global war on terrorism after 9/11.

The process of deconstructing NATO into a collective security organization of sorts continued unabated through the 2014 Russian seizure of Crimea and the invasion of eastern Ukraine. By then, NATO's military capabilities, including the residual forces deployed by the United States to Europe, had become a pale shadow of its once-formidable armies. Furthermore, logistical infrastructure across NATO had become degraded to the point that even moderate-scale joint exercises were problematic. Recent efforts to reverse the trend—the DEFENDER-Europe 20 exercise, for example, was to be the largest such exercise along the eastern flank of NATO since the

end of the Cold War, combining some 20,000 U.S. forces and 18,000 European forces—were effectively stopped by the "shelter-in-place" orders triggered by the COVID-19 pandemic, with only a portion of the troops exercised across the theater.

In addition to the fact that NATO's forces are inadequate to the task at hand, an even greater challenge may be that the alliance's political consensus concerning the overarching strategic threat is fractured. I call the latter problem the "regionalization of security optics," whereby the nature and degree of threat perception morphs as one moves from east to west. Countries along the front line such as Norway, the Baltic States, Poland, and Romania see Russia as a clear and present danger, while countries in the middle of the continent such as Germany have an attenuated view of the risk. France sees the principal pressure points as being in the Mediterranean and North Africa, and the Russian threat registers only remotely in Spain or Portugal.

This fractured threat perception—rather than the oft-discussed resentment against the alleged "transactionalism" of the Trump Administration—is the key reason why the majority of the European NATO allies have consistently failed to meet their agreed-upon 2 percent of GDP defense spending targets, which have been in place since the Warsaw summit of 2016.[5] The much-touted argument that NATO is not just about shared interests but also about shared values (President Trump's critics point to his alleged de-emphasis of the latter) is a false binary because NATO, as the most effective military alliance of like-minded democracies in history, has always been about both.

What has fueled the current turmoil in the alliance is the inability of key governments to see eye-to-eye with the United States on the nature of the threat to the West that is posed by Russia, which wants to revise the post–Cold War political settlement, and by the People's Republic of China (PRC), which wants to replace it. The absence of a policy consensus on Russia in particular is likely to remain the foundational obstacle to properly resourcing NATO and may in fact cause continued spikes in disagreement within NATO like the one triggered by reports that the Trump Administration planned to remove 9,500 U.S. troops from Germany.[6]

The United States will continue to draw great benefit from its leadership role in the NATO alliance, which serves both as an effective force multiplier and as a source of political influence in Europe and Eurasia more broadly. NATO's contribution to American security in an era of resurgent great-power competition rests on its ability to offset Russian and, increasingly, Chinese pressure on and in Europe, especially the two powers' ongoing efforts to reduce U.S. influence on the continent and *ad extremis* to separate European defense from America's. The critical importance of the NATO alliance as a force multiplier and pathway to lowering the overall price tag for American defense worldwide cannot be overstated.

The question, however, that continues to polarize the U.S. security community is the practical scope of what NATO should be contributing to the common defense and how such contributions address the challenges facing the United Sates not only in the European theater, but also in the Indo-Pacific region. Some analysts have gone so far as to suggest that NATO has an important role to play in Asia and that it should plan accordingly.[7] Such a strategy would be yet another permutation of the "burden sharing" that has been much debated throughout NATO's history, except that this time, the burden would be extended to a theater that historically has not been part of NATO's strategic domain, making such a strategy likely to fail.

What NATO needs is not more "burden sharing" but "burden transferring," a term I use to indicate that the greatest contribution NATO can make to the defense of the transatlantic community is for its European allies to resource their defense properly. This is necessary if the Europeans (with U.S. enablers in place and a modernized core strategic nuclear deterrent) are to be able to deter and, if need be,

defend Europe against a revisionist Russia in the event that the United States is pulled into an emergency in the Indo-Pacific region.

The imperative of "burden transferring" to Europe reflects the twin dilemmas facing the United States when it comes to collective defense: The geostrategic challenge we confront is orders of magnitude greater than in the Cold War, but the size of the United States military is simply too small to meet the requirements in both theaters, deter aggression, and win decisively. The United States should maintain a significant component in Europe. U.S. Army Europe, as currently structured, serves a critical role as both an enabler and a fighting force, with exercises on allied territory along NATO's eastern flank essential to developing the warfighting capability of U.S. troops and ensuring that they are fully interoperable with our allies. The same goes for continued exercises that serve to demonstrate the ability of the United States to reinforce the European theater in a crisis.

However, these will never fully replace the manpower and resources that the Europeans must bring to bear if deterrence in Europe is to hold. This is especially the case should a crisis arise elsewhere, as the United States military is no longer structured as it once was to fight two major theater conflicts plus one smaller engagement in a secondary theater; rather, we are—and are likely to remain—able to engage in only one major theater and one smaller operation if we want to prevail.

The key variable in a workable "burden transferring" approach as NATO's strategy in the unfolding era of great-power competition is an urgently needed political consensus within the alliance. In this context, the ongoing efforts, driven principally by France, to establish "strategic autonomy" for Europe in NATO—exemplified by programs such as Permanent Structured Cooperation (PESCO), Coordinated Annual Review on Defense (CARD), and the European Defense Fund as currently conceived—are counterproductive and likely to fail because the divergent security optics mentioned earlier will block any such consensus on defense-spending formulas that does not include the United States. The current tenor of the European defense and security debate—punctuated by occasional injudicious outbursts by European leaders that the NATO alliance is "brain dead"—only further undermines the ability of the alliance to come together around a common strategy.

Alliances in the Asia–Pacific Region

Asia is fast becoming the principal area of concern for U.S. defense strategy. The exponential growth of Chinese economic power over the past decade in particular has given rise to military capabilities that increasingly challenge the United States Navy's ability to dominate the theater. China has one-fifth of the world's population, and its military budget is second in size only to that of the United States.[8] Moreover, financial reserves accumulated over decades of predatory trade practices will allow it to continue buying companies, technologies, and expertise unless the United States and its allies impose severe restrictions on China's access. As many as 200 million Chinese citizens travel the world as tourists and work, study, and live abroad, and this number could increase significantly when the current pandemic restrictions are lifted.

The Indo-Pacific theater is also dramatically different from Europe: It rests on a series of bilateral alliances between the United States and its key partners, not on one bureaucratized structure like NATO's. The region is increasingly being transformed by China's abandonment of its former reticence and its growing geostrategic assertiveness, and the leadership of the People's Republic of China under Xi Jinping sees the PRC as having effectively caught up with the United States.

China is a Communist neo-Confucian state marked by repression and rigidity at home, and its foreign and military policy is marked by political and military mobilization and the putting forth of ever-bolder claims, its claim to "exclusivity" in the South China Sea being perhaps the most visible example. The leadership in Beijing seems certain that its path to global

economic dominance will soon be accompanied by expanding military influence that, as the PLAN's power projection capabilities grow, will allow it to dominate militarily.

With this in mind, Beijing has been building its hard power arsenal at a rapid pace, with the expansion of the nuclear, conventional, space, cyber, and information components at an unprecedented pace, posing a truly multi-domain challenge to the United States military. Aided by four decades of unprecedented freedom of access to America's technology, research, and knowledge economy, Beijing is poised to compete for supremacy in the Pacific within the next decade.

When it comes to China, Europe is unlikely to become a close ally of the United States any time soon. Although the devastation wrought by the Wuhan coronavirus on EU economies and Beijing's aggressive information campaigns targeting Europe could change elite attitudes to some extent, Germany, France, and especially Italy (but also a number of other countries, including some in Central Europe) see China principally in economic terms, with opportunities still outweighing risks, especially for smaller, capital-starved European economies outside the European Union and hence not eligible for recovery assistance funds.

The pivotal allies for the United States in Asia are Japan, South Korea, and Australia—the Asian "troika"—whose continued alliance with the United States stands in direct contradiction to Xi Jinping's "China Dream" of a globally dominant PRC to be established through a purposeful strategy of expansion across Eurasia and into the Pacific. The United States also has formal alliances with the Philippines, Thailand, and New Zealand, but their overall strength is derivative when it comes to our core alliances with the troika. The future of the troika depends on the future of each of its members: If China should succeed in isolating one of them, the risk to the security of the others would grow exponentially.

Chinese expansion is already well underway, though Beijing continues to face considerable obstacles to displacing the United States from the center of the global system. The immediate targets of this expansion drive are Hong Kong, where the process of dismantling its autonomy is already near completion, and Taiwan, which will face increased pressure once Beijing has bent Hong Kong to its will. This pattern of expansion targeting the three key U.S. allies in Asia can be seen in the proliferation of Chinese port investments; the development of PRC naval capabilities (including tenders for several nuclear-powered aircraft carrier battle groups); and the exponential investments in anti-access/area denial (A2/AD) capabilities by the People's Liberation Army (PLA) and PLAN.

China's overarching strategy is to break out of a territorially based defense strategy, harden its defenses of transcontinental and overseas transportation routes, and leverage its decades-long access to America's research and development (R&D) base and—even more important—its manufacturing and materials technologies to bring about a qualitative leap in PLA and PLAN capabilities vis-à-vis the United States. This is especially the case when it comes to command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR); strategic support forces; cyber and information; and unmanned systems in space.

Interlocking Alliances

The United States continues to derive great benefit from its leadership position in the NATO alliance and its close bilateral alliances with the troika in the Western Pacific. Our naval, air, and ground troop basing in Europe as well as in Japan, South Korea, and Australia continues to give us flexibility and supportability in power projection across both the Atlantic and the Pacific with the ability to rely on the military resources of our allies as a force multiplier.

In Europe, the effectiveness of NATO demands a strategy of "burden transferring" with continued U.S. nuclear strategic guarantees and continued coordination with our enablers. This must be combined with a small but effective, trained, and integrated Joint

Force component that both provides strategic linkage for the United States and Europe and reinforces the credibility of the larger transatlantic defense strategy.

Arguably, the greatest challenge facing the United States and its European allies, more than the interminable debates about the percentage of GDP to be allocated as a sign of commitment to the alliance, will be the imperative need to rebuild Europe's real usable military capabilities. This strategy of "burden transferring," whereby the Europeans take core responsibility for the continent's defense across multiple domains—not as an exercise in "strategic autonomy" but as a clearly defined and agreed-upon task *within* NATO—will be key to preserving European security and ensuring that the transatlantic bargain holds as we enter arguably the most dangerous period of great-power competition.

In Asia, the Western Pacific is also critical to the security of the Eurasian landmass, with continued close U.S. alliances with the troika presenting a direct challenge to Beijing's military planners. Coupled with U.S. bases on its territory, in Guam, and in Hawaii, the United States has the ability to develop a successful strategy to contain, deter, and if need be defeat China in a future conflict in the Pacific, provided it retains the flexibility to move its forces in the region in a crisis. We must therefore ensure that the troika can withstand direct pressure from China and that its members do not become vassalized over time. Continued close alliance with the United States will allow the three countries to exercise effective counterpressure against the advancing militarization of great-power competition in Asia and respond with effective force if deterrence fails.

There can be little doubt today that the PRC's primary goal is to reestablish itself as a dominant power in eastern Eurasia and the Western Pacific, absorbing Taiwan, isolating and ultimately vassalizing Japan, and pushing the United States back to the margins of the Asia–Pacific region. The second element of Beijing's strategy, which entails its close cooperation with Moscow, is to accomplish the decoupling of the United States from Europe, with long-term economic and population trends favoring China in its *de facto* alliance with the Russian Federation against the United States.

These two trends inextricably connect America's alliances in Europe and in the Asia–Pacific region: They mutually reinforce one another if successfully consolidated and conversely contain within themselves the seeds of each other's destruction. Preserving and strengthening the two as part of a coherent global defense strategy should be a key U.S. policy priority.

Conclusion

Grand, bureaucratized alliances do not simply unravel. They become hollowed out over time as threat assessments change and political will atrophies. This is the risk if NATO continues along its current path of "burden sharing" amid ongoing allegations of American "transactionalism." The preservation of NATO is vital to both Americans and Europeans because the alliance continues to serve both as a deterrent to Russia and as a values-based framework with which the West can confront China. NATO offers the best existing format for common defense and effectively ensures that the North Atlantic remains the internal waterway for Western democracies.

The preservation of America's alliances in Asia is essential to our ability to contain and deter China, for without them we cannot ensure that our rethinking of the U.S.–China relationship will take place on American terms. If NATO were to unravel or the troika to fall out of its close alliance with the United States, or if both were to occur, the entire Pacific Ocean west of Hawaii would become a contested space with the United States directly exposed to the risk of being pushed into its own hemisphere.

Endnotes

1. Thomas P. Ehrhard, "Treating the Pathologies of Victory: Hardening the Nation for Strategic Competition," in *2020 Index of U.S. Military Strength*, ed. Dakota L. Wood (Washington: The Heritage Foundation, 2020), pp. 24–26, https://www.heritage.org/sites/default/files/2019-10/2020_IndexOfUSMilitaryStrength_ESSAYS_EHRHARD_0.pdf.
2. *National Security Strategy of the United States of America*, The White House, December 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (accessed June 17, 2020).
3. James Mattis, Secretary of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, U.S. Department of Defense, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (accessed June 17, 2020).
4. "The *Acquis Communautaire* is the accumulated body of European Union (EU) law and obligations from 1958 to the present day. It comprises all the EU's treaties and laws (directives, regulations, decisions), declarations and resolutions, international agreements and the judgments of the Court of Justice. It also includes action that EU governments take together in the Area of Freedom, Security and Justice and under the Common Foreign and Security Policy. ¶ New EU Member States must accept all the existing *acquis*—some elements of it during a transitional period—and put in place mechanisms to adopt future elements of the *acquis*. ¶ The Court of Justice has ruled that the EU *acquis* takes precedence over national law if there is a conflict, and that the *acquis* may have direct effect in the Member States." Vaughne Miller, "The EU's *Acquis Communautaire*," British House of Commons Library *Research Briefing*, Standard Note SN/IA/5944, last updated April 26, 2011, p. 1, https://researchbriefings.files.parliament.uk/documents/SN05944/SN05944.pdf (accessed July 25, 2020).
5. Press release, "Warsaw Summit Communiqué Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw 8–9 July 2016," North Atlantic Treaty Organization, last updated March 29, 2017, https://www.nato.int/cps/en/natohq/official_texts_133169.htm (accessed July 28, 2020). See esp. para. 34.
6. Hans Binnendijk, "The Folly of a NATO Troop Withdrawal Decision," *Defense News*, June 10, 2020, https://www.defensenews.com/opinion/commentary/2020/06/09/the-folly-of-a-nato-troop-withdrawal-decision/ (accessed June 10, 2020).
7. See, for example, Ian Brzezinski, "NATO's Role in a Transatlantic Strategy on China," Atlantic Council, New Atlanticist Blog, June 1, 2020, https://www.atlanticcouncil.org/blogs/new-atlanticist/natos-role-in-a-transatlantic-strategy-on-china/ (accessed June 17, 2020).
8. Lucie Béraud-Sudreau, "Global Defence Spending: The United States Widens the Gap," International Institute for Strategic Studies Military Balance Blog, February 14, 2020, https://www.iiss.org/blogs/military-balance/2020/02/global-defence-spending (accessed July 28, 2020).