

## I. Sustaining Conventional Military Deterrence

Maintaining a favorable balance of power will be essential to achieving America's long-term aims in the Indo-Pacific. Even as the military dimensions of the U.S.-China competition are likely to feature less prominently than in the U.S.-Soviet rivalry of the Cold War, the erosion of conventional deterrence in Asia would threaten to undermine the full range of U.S. economic and political interests in the region. While the United States still retains an overall military advantage over China, the gap has closed considerably over the last two decades and, absent urgent change, the regional balance may tip in China's favor by the late 2020s or early 2030s. In certain scenarios, the military balance may already disadvantage the United States.

China's military strategy has been predominantly asymmetric, seeking to disrupt, disable, or destroy the critical systems that enable U.S. military advantage. Responding to the asymmetric character of this competition poses an enormous challenge to the Defense Department (DoD) because it goes to the core of how the Joint Force fights wars, how the Pentagon and the defense industrial base develop technology, and how U.S. allies and partners build their armed forces. The National Defense Strategy and the Indo-Pacific Strategy Report pointed in the right direction to arrest and reverse these trends. Nevertheless, without requisite prioritization, forward-looking ideas, and consistent funding, subsequent shifts could end up being too little, too late.

In short, the United States needs a new American way of war. The underlying military problem is that U.S. warfighting concepts and forces remain vulnerable to Chinese "systems destruction warfare," which attacks critical nodes to create systemic effects.<sup>18</sup> The challenges that need to be addressed are numerous: U.S. air bases, aircraft carriers, and surface vessels are too vulnerable to Chinese air and missile attacks; current U.S. systems for command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) are brittle in the face of Chinese cyberattacks, electronic warfare, and long-range strikes; U.S. logistics systems, ports, and airfields are vulnerable to cyberdisruptions and physical attacks; and the Joint Force lacks sufficient precision-guided munitions. All of these shortcomings must be addressed with considerable focus and urgency.

To implement a new military strategy, the U.S. government will also have to change the way it does business. Reforming back-office processes cannot be pursued as an administrative sideshow, but rather as a foundation

to America's ability to compete more effectively. The Defense Department should revise its requirements, programming and budgeting, and acquisition processes to support and access the latest technological innovations. Bold and sustained leadership will be necessary at the Defense Department, at the White House, in the military services, and in the U.S. Congress to overcome powerful pockets of resistance that remain committed to legacy platforms and existing business models.

Finally, the United States should make a concerted push to reshape the regional balance of power by further networking the regional security environment and building the capacity of key partners. This should include developing closer military ties that could be leveraged in crisis or conflict, as well as supporting the ability of frontline states to better deter Chinese coercion and aggression. To do so, the United States should help regional militaries—prioritizing Taiwan, Japan, Vietnam, and the Philippines—develop the ability to challenge China's power-projection capabilities.

Different parts of the region will require different fixes. In some cases, the threat of sanctions against countries with security ties with Russia should be eased to facilitate balancing against China. Where more advanced military cooperation is neither technically nor politically feasible—as is the case throughout much of Southeast Asia—the United States should build a maritime common operating picture that can both kick-start security cooperation and deter lower levels of Chinese coercion. Finally, the United States should pay particular attention to supporting India's efforts to pose military dilemmas for China, thereby providing relatively low-cost means to complicate the ability of the People's Liberation Army (PLA) to concentrate attention and resources on U.S. strongholds in East Asia and the Western Pacific.

### Recommendations for U.S. Policy

#### DEVELOP A NEW AMERICAN WAY OF WAR

##### *Design a new military strategy and novel joint operational concepts for China contingencies*

Current U.S. military strategy and operational concepts for China incur significant risk of mission failure and unacceptable attrition, and trend lines suggest that this situation will worsen over time. This disadvantage will constrain U.S. policymakers across many potential contingencies, not just conflict scenarios. For instance, responses to gray-zone coercion are likely to be more muted if a strong response provokes

escalation with significant risk to U.S. forces. Absent an appropriate strategy and operational concepts, U.S. modernization and technology developments are likely to be unfocused and inefficient, and allies and partners will lack a clear understanding of their role in response to Chinese coercion or aggression.

The chairman of the Joint Chiefs of Staff should lead the effort to develop a new U.S. military strategy that explains how the United States alongside its allies and partners will use force to achieve the political objectives of defending U.S., allied, and partner interests from coercion while deterring or defeating Chinese aggression. In drafting the strategy, the Joint Staff should work closely with the Office of the Secretary of Defense, the relevant combatant commands, and the services.

The strategy should be grounded in preventing China from achieving its objectives—what strategists call “deterrence by denial”—rather than simply by punishing China, given that Beijing may be willing to tolerate substantial costs to achieve its objectives. This strategy must also account for political dimensions of military action, including China’s ability to escalate strategically through informational, diplomatic, economic, or military means, to include attacks on the U.S. homeland or nuclear escalation. It should exploit the advantages of coalition warfare and force China to be the aggressor or escalator at every step. Finally, the strategy should detail how the Defense Department and the commander of U.S. Indo-Pacific Command intend to coordinate military actions with allies, partners, and other instruments of national power to achieve effects that are greater than the sum of the parts.

Operational concepts for China should describe how the U.S., allied, and partner forces will conduct and coordinate military operations over time to achieve the military objectives of the strategy. The critical shift in these concepts must be the ability—whether through new technology or operational art—to strike at the PLA’s military centers of gravity without first gaining multidomain superiority, or without strategically unfavorable escalation. These concepts must be specific to conflict scenarios including Chinese coercion or aggression against Taiwan or Japan, coercion or conflict in the South China Sea, Chinese intervention into North Korea, and coercion or conflict in the Indian Ocean.

This strategy and these concepts should guide defense investments and reforms while explaining these choices to audiences inside and outside the Defense Department, including allies and partners. As such, they should contain sufficient unclassified information to communicate the main ideas and priorities, while classified versions contain greater detail.

***Build a more resilient architecture for command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR)***

Information has always been critical in warfare, but the concomitant development of information technology and precision-guided weapons has raised its importance to new heights. Given accurate information, precision-guided weapons can hit targets with reliable accuracy regardless of range. In this new regime, precision trumps mass, but it requires rapid, accurate information.

China’s systems destruction warfare would use multidomain attacks to deprive U.S. forces of the information and coordination that make precision-guided warfare so effective. This approach is particularly problematic because current U.S. C4ISR is relatively brittle, as it was designed and built in an era when competitors or adversaries could not attack U.S. assets in space or at long ranges. A new architecture must be able to operate effectively under long-range multidomain Chinese attacks. Given the inherent vulnerability of some of these systems and the attack surface they present, preclusive defense is impossible. Instead, U.S. C4ISR systems must degrade gracefully under attack and must function in different modalities to complicate China’s counter-C4ISR operations.

Improving the resilience of U.S. C4ISR architecture in the face of attack might be the single most effective step the United States can take to strengthen its conventional deterrent: China will be more readily deterred if Beijing doubts its ability to disrupt, degrade, or destroy U.S. C4ISR systems.

Specific components of this architecture should include:

- Space capabilities that are more resistant to kinetic and nonkinetic attacks;
- Alternatives to space for ISR, long-range communications, and position, navigation, and timing (PNT);
- Low probability of intercept and low probability of jamming data links;
- Cyberprotection that prioritizes sufficient trust in data over protecting network integrity;
- Sophisticated surveillance systems that can penetrate contested environments using speed or stealth to surveil critical targets;
- Alternative ISR systems that utilize large numbers of “good enough” sensors operating collaboratively in contested environments to target massed or imprecisely located targets;

- Doctrine and training to operate using alternative C4ISR concepts, particularly mission orders and peer-to-peer networks;
- Synthetic training environments that allow U.S. forces to exercise contested C4ISR operations;
- Research and development investments in artificial intelligence to improve target recognition, information processing, and the ability of sensors and networks to respond to jamming or cyberattacks; and
- Improvements in defensive countermeasures and offensive capabilities for electronic warfare (EW) that include:
  - » Developing a C4ISR architecture that can use multiple pathways to transmit data, including an ability to use networks of jam-resistant tactical data links to create larger “mesh” networks capable of supporting distributed, multidomain operations;
  - » Increasing the capacity of DoD and the services to conduct EW in multiple domains to disrupt enemy kill chains;
  - » Investing in stand-in jamming capabilities in the air, to include the use of unmanned or attritable aircraft in dense threat environments;
  - » Pursuing a layered EW posture for the Navy to defend against long-range anti-ship missiles, to include anti-satellite jamming, airborne EW platforms, and accelerated investments in terminal defenses;
  - » Investing in ground-based and unmanned EW platforms for the Marine Corps to provide an expeditionary EW capability as part of the Corps’ Expeditionary Advanced Basing Operations concept (EABO) that can disrupt enemy kill chains and enable maritime maneuver in previously contested environments;
  - » Investing in ground-based EW systems for the Army to help defend key forward locations against long-range air and missile attacks; and
  - » Investing in alternatives to GPS for all four services for position, navigation, and timing, and alternatives to millimeter-wave radars for terminal weapons guidance.

### ***Build a combat-credible posture in the Indo-Pacific***

If attacking U.S. C4ISR systems is atop China’s targeting list, attacking U.S. forward bases, and particularly air bases, is a close second. China has made significant investments in long-range ISR and strike assets to attack fixed air bases and mobile aircraft carriers. China hopes the threat of these attacks will deter U.S. intervention by negating a substantial portion of U.S. airpower early in a conflict, thereby creating time and space for a fait accompli, and by causing potentially irreparable attrition to forward-deployed aircraft squadrons. A combat-credible posture would undermine China’s deterrence logic and weaken its military strategy by demonstrating that attacks on forward bases would not neutralize U.S. striking power in the region, and that attrition to U.S. forces would be within acceptable limits such that America and its allies could continue fighting.

A combat-credible posture in the Indo-Pacific should include:

- Adopting, exercising, and demonstrating an ability to execute a more dispersed basing posture in which dozens of airfields can support air operations in a crisis;
- Acquiring equipment and maintainer personnel to support rapid movement between bases;
- Making major air bases more resilient to attack by:
  - » Hardening, burying, or making redundant critical facilities such as fuel storage and pumps;
  - » Expanding runways or improving ramp and apron space to serve as expedient runways;
  - » Improving and exercising rapid runway repairs;
  - » Increasing passive defenses against area-effects weapons;
  - » Increasing active defenses against cruise missiles at major air bases;
  - » Increasing use of camouflage, concealment, deception, and electronic warfare to degrade Chinese ISR and battle-damage assessment; and
  - » Exercising air base operations under worst-case attack conditions.
- Renewing and fully supporting the Compact of Free Association with the Federated States of Micronesia, the Marshall Islands, and Palau, which provide irreplaceable access to critical geography;
- Developing support infrastructure and greater access at existing airfields, and improving runways and

infrastructure at key locations in the Compact of Free Association states like Palau and Yap; and

- Increasing deployments of ground-based precision fires for land and anti-ship attacks.

### ***Increase investments in critical munitions and munitions development***

Precision-guided warfare against China would require huge numbers of precision-guided weapons. Additionally, these weapons must be capable of striking both high-value and massed targets in highly contested environments with degraded information. Current U.S. munitions inventories are inadequate to support sustained combat against China, and especially in weapons that can penetrate China's anti-access/area denial networks.

To address this, the Defense Department should:

- Increase stockpiles of critical munitions, such as long-range anti-ship missiles;
- Develop and deploy mobile and relocatable land-based launchers for long-range cruise, ballistic, and hypersonic weapons in the Indo-Pacific;
- Develop and deploy affordable munitions that can operate collaboratively in contested environments to strike massed or imprecisely located targets;
- Develop area-effects weapons that comply with current U.S. policies regarding cluster munitions, or seek waivers from these policies;
- Accelerate development of longer-range air-to-air weapons;
- Develop modular weapons with updatable seekers, control units, motors, and software to protect stockpiles from obsolescence; and
- Work with Congress and the defense industry to increase munitions production capacity.

### ***Develop concepts and capabilities for contested logistics***

Attacks on U.S. air bases are one part of a broader Chinese strategy to impede the ability of U.S. forces to operate and sustain operations in East Asia. U.S. forces in Asia are at the end of a long logistical tether that was not designed to operate under precision long-range attacks. U.S. surge forces moving into the theater likewise rely on

transportation equipment and infrastructure that were designed assuming sanctuary from attack. China's ability to hold these systems at risk using long-range fires and cyberattacks threatens the ability of the United States to project and sustain combat power in the Indo-Pacific.

To address this, the Defense Department should:

- Integrate logistics and sustainment considerations into military strategy and operational concept development for China from the outset;
- Pursue the air base resiliency initiatives outlined above and apply similar measures to key ports, naval facilities, and other critical infrastructure in the region;
- Conduct a review of the Navy's Combat Logistics Fleet (CLF) force structure, employment strategy, and shipbuilding industry to design a new CLF fleet architecture that can deliver contested maritime logistics support;
- Accelerate development of methods to rearm U.S. Navy vertical launch system cells at sea; and
- Develop concepts and capabilities to support distributed operations with a more responsive logistics system.

## **EMPOWER THE DEFENSE DEPARTMENT TO HARNESS AMERICA'S NATIONAL SECURITY INNOVATION BASE**

### ***Reform Defense Department organizations and processes, including requirements, programming and budgeting, and acquisition***

The Defense Department originally designed the core decisionmaking processes that determine the size and shape of the future Joint Force (requirements, programming and budgeting, and acquisition) for the industrial age and the Cold War threat environment. These processes, although still sound, have a range of flaws and assumptions that make them inadequate to the task of building the future force. They should be updated to accommodate new and rapidly changing technologies and the current complex and evolving threat environment.<sup>19</sup> Specifically, the requirements process, which was designed to develop new capabilities from scratch within the defense ecosystem, must adjust to the new innovation environment, developing ways to more quickly and efficiently adapt existing technologies developed outside of DoD or the traditional defense industrial base to emerging warfighting problems. The programming

and budgeting process also need additional flexibility to allow the department to rapidly acquire emerging technologies as they develop, rather than waiting for the next full cycle of the process to culminate 18 to 24 months down the road. To this end, the Office of the Secretary of Defense should consider withholding significant funding when delivering fiscal guidance to the services, using this funding during its review of service spending plans to inject new proposals into the budget throughout the process, as opposed to only at the beginning. Further, Congress should consider realigning appropriations titles according to the type of life cycle a system has (for example, durable goods, such as aircraft carriers; evolvable systems, such as software; or expendable systems, such as munitions) as opposed to the part of the life cycle a system is in (research and development, procurement, or maintenance). This realignment would allow the department to move programs from development into production more quickly, while also making the total life cycle cost of the system more transparent.

***Ensure the Defense Department can develop, access, and leverage the latest technologies***

The global innovation environment has changed substantially since the Cold War, when big advances in military technology generally came out of DoD labs before eventually migrating to the commercial sector. Now, private companies are at the leading edge of developing new technologies with significant military applications, including artificial intelligence (AI) and machine learning. This presents a major challenge for the Defense Department in identifying these technologies and bringing them into the defense enterprise, when many companies are unwilling or unable to work with the Defense Department as a customer, and DoD is slow to absorb their potential and need for iteration. The defense market is small relative to the size of commercial technology markets, and some companies view cooperation with DoD as damaging to their brand. In addition, barriers to entry into the defense sector are high due to the complex regulatory regime governing defense contracts. DoD cannot easily invest in promising technologies outside of certain contractual frameworks.

To begin to address these challenges, DoD and traditional defense industry primes have developed new means of reaching out to the technology sector, including most notably through government entities, such as the Defense Innovation Unit, and private entities, such as venture capital funds run by defense primes.<sup>20</sup> However, these means of bringing new and disruptive technologies

into the defense enterprise remain inadequate given the sheer scale of innovation with military applications happening outside of the Defense Department's remit, and DoD's limitations as a customer.<sup>21</sup> These dynamics will have to change. DoD should invest more in capturing these technologies and helping new technology start-ups grow, while also continuing to invest in DoD labs and the traditional defense industrial base, which remain critical to sustaining U.S. military technological superiority. DoD should also take steps to make itself a more attractive customer or partner for new technology companies by developing ways to demonstrate a start-up's viability, such as with its own venture capital capability.

***Sustain and enhance a traditional and nontraditional defense industrial base that is robust, flexible, and resilient***

Large diversified conglomerates mostly comprised the industrial base that produced war materiel for World War II and throughout much of the Cold War. After a wave of divestment of defense business units and the subsequent consolidation of remaining businesses driven by the post-Cold War peace dividend, the U.S. industrial base became dominated by a relatively small number of specialized defense and aerospace companies. These circumstances have left the traditional U.S. defense industrial base exposed to certain vulnerabilities, which were thoroughly catalogued in a 2018 DoD report—including lack of competition, fragile supply chains, and difficulty attracting and retaining skilled labor and engineering talent.<sup>22</sup>

At the same time, a new critical component of the defense industrial base has emerged in the form of companies developing advanced commercial technologies with significant military applications, as discussed above. A healthy industrial base, broadly defined, is a vital ingredient to U.S. defense competitiveness; DoD should not be passive about its future. In both cases, DoD must review its own regulatory regimes and contracting practices to foster a healthy defense innovation and industrial base, and Congress must support the department with legislative changes where necessary. DoD should start by fully implementing the new acquisition authorities included in the 2016 and 2017 National Defense Authorization Act, including further streamlining its regulatory frameworks. DoD should also develop a way to evaluate the benefits of a regulation against the cost of enforcing it. Finally, DoD and Congress should both use this metric to evaluate if, when, and under what circumstances different regulations should be enforced. Reducing



regulatory burden could lower barriers to entry into the defense sector, allowing more nontraditional companies to enter the market, as either primes or subcontractors.

#### **STRENGTHEN AND NETWORK U.S. ALLIES AND PARTNERS**

##### ***Develop ally and partner anti-access/area denial capabilities***

America's allies and partners must be capable of defending themselves alongside U.S. forces. Unfortunately, many U.S. allies and partners in the Indo-Pacific face the same challenges as the United States because their armed forces are similarly vulnerable to attacks on air bases, surface vessels, C4ISR systems, and critical infrastructure. They also lack sufficient quantities of the right kinds of munitions to sustain operations against China.

To address this, DoD must work together with the State Department, Congress, and foreign governments to utilize Foreign Military Financing and Maritime Security Initiative (MSI) funding to help regional states develop concepts and capabilities that would challenge Chinese power-projection operations with some of the same kinds of anti-access/area denial systems that China developed to undermine U.S. military advantages. Prioritizing Taiwan, Japan, Vietnam, and the Philippines, specific initiatives should include:

- Conducting wargaming, analysis, exercises, and concept development for high-end warfare with key allies and partners to develop a shared understanding of the challenge and an appreciation of how they can contribute in a crisis or conflict;
- Developing and exercising C4ISR capabilities for cooperative targeting in contested environments;
- Shifting allied and partner operational concepts away from traditional maneuver and territorial defense toward greater use of area denial, long-range fires, cyberattacks, electronic warfare, and mobile defenses in depth;
- Supporting specific investments in mines, coastal defense cruise missiles, jammers and dazzlers for terrestrial and space-based systems, anti-radiation munitions, mobile air and missile defenses, short-range guided munitions such as anti-tank weapons, and cyberattacks;
- Working with more capable allies and partners to add long-range precision fires, air-independent propulsion diesel-electric attack submarines, unmanned surface and undersea vessels, unmanned aerial vehicles for ISR

and offensive strikes, and air and missile defenses for key fixed sites; and

- Encouraging U.S. allies and partners in the region, particularly Taiwan, to stockpile fuel, food, medicines, and munitions to prepare for potential Chinese blockades.

##### ***Promote security networks among U.S. allies and partners***

The past decade has seen the emergence of new security networks involving various constellations of American allies and partners in the Indo-Pacific. These networks complement U.S. bilateral alliances and strategic partnerships, and Washington should continue to encourage their formation and growth. The United States should support the deepening of security ties between Japan and Australia, including by urging its two allies to finalize a reciprocal access agreement. Trilaterally, Washington should work with Tokyo and Canberra to enhance intelligence sharing, focusing on maritime domain awareness within the first island chain. Through its dialogue with Japan and India, the United States should explore new opportunities for trilateral military exercises and joint defense research and development. Washington should also make a priority of getting trilateral cooperation with South Korea and Japan back on track. Finally, American efforts to advance security networking in the Indo-Pacific should enlist European powers where practical. Specifically, the United States should work with France and India to stand up a new trilateral consortium to share information regarding the movement of Chinese military vessels in the Western Indian Ocean.<sup>23</sup>

##### ***Build a common operating picture in Southeast Asia***

Many U.S. allies and partners are concerned about China's actions toward their maritime territories and resources. Leveraging a shared interest in maritime domain awareness could be advantageous to competition below armed conflict, while building coalition cohesion in the event of a crisis. Toward this end, Congress should expand Foreign Military Financing for Indo-Pacific countries and continue funding the Maritime Security Initiative (Section 1263 of the FY16 National Defense Authorization Act), which is due to expire at the end of FY2020. Without additional resources, Congress should also guard against expanding MSI authorities to other countries for fear of diluting the original intent of building partner capacity among Southeast Asian partners.

Future legislation should more explicitly direct this effort to focus on creating a common operational picture

in Southeast Asia.<sup>24</sup> A common operational picture would provide shared situational awareness of activity in the air and maritime domains to all participating allies and partners. It would allow regional states to track activity, both in their sovereign airspace and maritime territory, as well as destabilizing behavior in international airspace and waters. In peacetime, this shared system would keep states apprised of illicit trafficking and violations of fisheries or mineral rights. In crises or conflicts, it would provide situational awareness about the disposition of enemy military forces. The shared nature of this system would provide it with a measure of strategic resilience, as China would be reluctant to attack a shared, multinational system during crises or limited conflicts, for fear of unfavorably escalating a crisis or limited conflict into a broader regional war. Protecting sensitive intelligence, surveillance, and reconnaissance collection capabilities would be an obstacle to developing such a system. To help allay these concerns, the system could be tiered, with the lowest tier sharing basic civilian airspace and maritime awareness data along with commercially available satellite information. The second tier could build on this and incorporate less-sensitive military ISR data, such as electro-optical/infrared (EO/IR) sensor feeds from publicly acknowledged ISR platforms. The third tier could offer fused, multi-intelligence information to the most trusted members.

#### ***Allow exemptions to the Countering America's Adversaries Through Sanctions Act (CAATSA) for countries seeking to balance against China***

The United States should seek to reduce Russian revenue from overseas arms sales; however, this goal should be pursued more flexibly with greater attention to how it affects the military balance in Asia. Certain Indo-Pacific states, particularly India, Indonesia, and Vietnam, have long been customers of Russian military equipment. It is ultimately counterproductive to sanction these countries, or threaten to sanction them, for buying Russian equipment that would improve their ability to counter Chinese coercion or deter Chinese aggression. Moreover, further isolating Russia in Asia and preventing its arms sales to a variety of states could push Moscow into a closer and more co-dependent relationship with Beijing. Congress should therefore allow CAATSA exemptions for Indo-Pacific states that wish to procure Russian weapons, provided these weapons would be used to balance against China. Over the long term, the U.S. government and defense industry should explore policies, incentive structures, and offerings that would give regional partners affordable options to buy American military equipment and services instead.

#### ***Support Indian military choices that create dilemmas for China in peacetime, crisis, and conflict***

India has the potential to contribute as a military counterweight to China. Unfortunately, structural impediments and resource constraints have hobbled India's ability to keep pace with China's military modernization over the last 20 years. However, even without fundamental reform, the Indian military can still pose dilemmas for China and support a more competitive posture alongside the United States. Toward that end, the United States should actively support India to take the following actions, in addition to removing U.S. roadblocks when appropriate, such as those associated with CAATSA described above:

- Increasing investments in super- and hypersonic anti-ship missiles, along with investments in maritime domain awareness and long-range ISR to target these weapons;
- Acquiring more submarines—and particularly air-independent diesel-electric attack submarines—relative to surface vessels;
- Improving military transportation infrastructure, particularly from the Indo-Pakistan border to the northeastern border with China, and from the internal lowlands to the mountainous border region;
- Consolidating aircraft procurement around one or two fighters to create greater economies of scale and efficiencies in operation;
- Making major investments in electronic warfare, cyber offense, and counterspace systems;
- Leveraging commercial space systems and partnering with other spacefaring nations such as the United States to share access to certain space-based systems;
- Shifting the “make in India” program away from large systems integration and toward developing centers of excellence and innovation in key areas of technology, modeled on the Israeli defense start-up sector; and
- Shifting the Indian army away from massed territorial defense toward multidomain operations comprising long-range fires, electronic warfare, cyberwarfare, anti-maritime, anti-air, engineering, and information operations.