MAY 2023

OFFSET-X

CLOSING THE DETERRENCE GAP AND BUILDING THE FUTURE JOINT FORCE

SPECIAL COMPETITIVE STUDIES PROJECT

MAY 2023

OFFSET-X

CLOSING THE DETERRENCE GAP AND BUILDING THE FUTURE JOINT FORCE

SPECIAL COMPETITIVE STUDIES PROJECT

The Special Competitive Studies Project is a bipartisan, non-profit project with a clear mission: to make recommendations to strengthen America's long-term competitiveness where artificial intelligence (AI) and other emerging technologies are reshaping our national security, economy, and society.

This second Defense Interim Panel Report (IPR) reflects the work that the Special Competitive Studies Project (SCSP) Defense Panel has conducted over the past year and a half. It builds off of the first Defense IPR, The Future of Conflict and the New Requirements of Defense, that was summarized in our Mid-Decade Challenges to National Competitiveness report.

SCSP Leadership

Authors

Justin Lynch
Senior Director

Jung-Ju Lee
Director

Luke Vannurden
Associate Director

Ylber Bajraktari
Senior Advisor

Greg Grant
Senior Advisor

Nicole Makar
Research Assistant

Thomas Riela
Research Assistant

Senior Advisors

This report benefited greatly from insights from more than one hundred experts, to whom we are deeply grateful. It aims to reflect many, though not all, of those insights. It was prepared by the SCSP staff and, as such, is not a consensus document of all the experts who assisted.
See Annex B for a complete list of contributors.

A Letter from the Chairman & Chief Executive Officer

As we enter a new era of warfare and international security, the stakes for the United States have never been higher. The convergence of emerging and advanced technologies with innovative operational concepts is creating new ways to employ force, as illustrated by the tragic war in Ukraine. Meanwhile, the People's Republic of China continues to amass the military capability to seize Taiwan by force, contest the U.S. military across domains, and reshape the international order beginning with the Indo-Pacific - the most consequential region of this century.

This report, the second one by our Defense team, argues that the time for action is now. In the near-term, the military services, combatant commands, and the civilian leadership that oversees them must proactively adopt capabilities that will allow them to deter or defeat any acts of aggression that directly threaten U.S. interests. To maintain military superiority in the medium-term and be favorably positioned for an enduring competition, the U.S. military needs a new force design.

Last year, SCSP proposed a technology-centered, competitive strategy – Offset-X – that would lay the groundwork for maintaining our military-technological superiority over all potential adversaries, including the People's Liberation Army. This report now takes the next logical step in the development of Offset-X strategy: proposing recommendations for the Joint Force that translate the ten elements of the institutional, competitive strategy into capabilities and force design requirements.

In the course of formulating this report, our team consulted with more than 150 leading experts in government, academia, and the private sector to create a comprehensive, effective, and actionable strategy. We encourage you to collaborate with us in this effort to ensure that America, and its many allies and partners, are strategically positioned and organized to excel in the techno-economic competition with China now and into the future.

Eric Schmidt
Chair, SCSP

Ylli Bajraktari
CEO, SCSP

Table of Contents

Executive Summary

We are in a decisive decade. China's growing military capabilities force the United States, for the first time in decades, to face the prospects of a conventional military defeat. China continues to amass a wide array of advanced capabilities designed specifically to counter the traditional American way of warfighting. It has identified dependencies in the Joint Force and is developing the concepts and capabilities to exploit them. A core component of which are its focused efforts to integrate by 2027 the mechanization, informatization, and intelligentization of its armed forces, putting itself in a position to reunify Taiwan by force, if necessary, and setting the stage to elevate the PRC to a position of strength, prosperity, and leadership on the world stage.[1]

If the United States does not rise to the challenge by moving with sufficient urgency to transform the Joint Force and develop and field next generation capabilities, the consequences could be dire. Most Americans alive today have only known a world in which the United States was the only true military superpower. That unchallenged military superiority has underwritten an international order that has fostered peace and prosperity on a scale that humanity has never before experienced. In contrast, the future we may be looking at – if we fail to act – could see a shift in the balance of power globally, and a direct threat to the peace and stability that the United States has underwritten for nearly 80 years in the Indo-Pacific – the most economically, technologically, and resource-critical region of this century. This is not about the anxiety of no longer being the dominant power in the world; it is about the risks of living in a world in which the Chinese Communist Party becomes the dominant power.

To stay ahead of China and to close the near-term deterrence credibility gap, SCSP proposes a technology-centered, competitive defense strategy – Offset-X – that lays the groundwork for maintaining or re-gaining our military-technological superiority over all potential adversaries, including the People's Liberation Army.

Drawing on lessons learned from DoD's past three offset strategies and the United States' continued economic, societal, and technological strengths, SCSP outlined ten initiatives that cumulatively lay the technological-military foundations of a new competitive strategy.[2] Its objectives are to (1) reduce the potential military, economic, and political costs of war for the United States, its allies, and its partners while dramatically increasing such costs for China; (2)

[1] Military and Security Developments Involving the People's Republic of China, U.S. Department of Defense (2022).

[2] The Future of Conflict and the New Requirements of Defense, Special Competitive Studies Project at 32 (2022).

invalidate many of the PLA's concepts and capabilities aimed at countering U.S. advantages; (3) significantly increase the degree of unpredictability China must account for to be confident of military victory; (4) shift more risk from humans to machines, and from expensive and hard-to-replace systems to lower-cost, attritable systems; and (5) strengthen U.S. and allied ability to project power into heavily defended regions.

There is general agreement in the national security establishment on the broad strokes of the operational concepts required to counter potential Chinese aggression against Taiwan. These have been repeatedly highlighted in multiple wargames and analyses conducted both inside and outside of government. The U.S. military and our allies need to be able to fight in highly contested maritime, air, and space domains, including within reach of China's vast arsenal of ballistic, cruise, and air defense missile systems; the Joint Force must be able to defeat a potential PLA amphibious and air assault across the Taiwan Strait; and, the Joint Force must protect the United States homeland.

With the timelines that China appears to be operating with, DoD faces the challenge that, for the most part, it will be fighting with forces designed previously.[3] Regrettably, while the threat has been deliberately and urgently designing its forces against the U.S. military, the United States has not been designing, certainly not rapidly enough, against the threat. We contend that in order to close the deterrence credibility gap, the U.S. military needs a new force design, in addition to new capabilities. We stress the importance of undertaking a sweeping DoD-wide review of force presentation and force employment, similar to what the Marine Corps is undertaking with Force Design 2030, and we offer specific proposals here. In the interim, however, the military Services and combatant commands will have to take the capabilities and concepts we propose in this paper designed to defeat the PLA theory of victory, and adapt accordingly.

The following report is organized into five parts. **Part 1** discusses the changing character of warfare that is being driven by the convergence of emerging technologies on the battlefield and by operational lessons emerging from the war in Ukraine. It also discusses the PLA's theory of victory and the supporting concepts and capabilities.

Part 2 elaborates on the objectives the Joint Force should pursue to offset the PRC. It argues that fundamentally the United States military must have demonstrable ability to decrease the military, economic, and political cost of war for the United States, its allies, and its partners, and commensurate ability to increase such costs for the PRC in war.

Part 3 re-describes the sources of the Offset-X competitive strategy. It details persistent asymmetries the United States can leverage against the PRC, and recommends continually

[3] As described in CJCSI 3001.01A, Implementing Joint Force and Design, (2022) force design takes place from 5-15 years; force development from 2-7 years; and force employment from 0-3 years.

exploring new asymmetries to keep the PLA perpetually off-balance. These are asymmetries that stem from our democratic institutions, long-standing organizational biases, and hard-won operational experiences that are difficult, or even impossible for the PRC to replicate.

Part 4 outlines how to operationalize Offset-X in the near to medium-term. Organized by warfighting functions, it describes mission requirements, core capabilities, and technology-enabled solutions needed to fulfill them. We also provide illustrative examples in Annex A of existing and ready-to-field technological solutions that can bring some of these capabilities to bear today.

Finally, **Part 5** then spells out the characteristics of a Future Joint Force, derived from Offset-X, designed to employ the capabilities stemming from Offsets-X, and determined to meet the challenges of the future character of conflict. To guide the execution of this force design, each characteristic includes actions with near-term impact and actions with medium-term impact to equip the Future Joint Force with an enduring advantage.

Combined, this report then provides for three essential elements – a competitive institutional strategy, the operational capabilities required to underwrite this strategy, and joint forces needed to execute it. Cumulatively, we believe these three essential elements will not only close the window of vulnerability we may be facing in the near-term in the Indo-Pacific in 2025-2030 timeframe, but also position us well for a competition that is likely to be enduring, exhausting, and – likely – existential.

PART ONE

Challenges: The Changing Character of Warfare and the PLA's Theory of Victory

The Changing Character of Warfare. A modern great power war would be unlike anything Americans have ever experienced. Such a war would be fought at a greater scale, wider geographic distribution, and much higher intensity than the U.S. military experienced over the past two decades. It would likely include an unprecedented mobilization of resources, large-scale cyber attacks, missile strikes against both military and critical civilian infrastructure even on American soil,[4] and the disablement or destruction of space-based assets that underpin critical functions of our economy, society, and military. Such a war could inevitably devolve into a prolonged contest that places a high premium on the strength of the nation's industrial base, innovation ecosystem, and political will. Knockout blows, decapitation strikes, and short, decisive battles, often aspired to, would likely fail to materialize.

We are already in a persistent conflict below the level of armed clashes with China and Russia. Their authoritarian governments have blurred the line between war and peace through frequent cyber attacks, unrelenting disinformation operations, aggressive theft of intellectual property, and sabotage.[5] The individualization of war is creating new ways to use coercion or force to achieve political ends. In addition to targeting militaries, infrastructure, or populations, states can now use microtargeting at scale to wage denigration campaigns, impose psychological pressure, and under certain circumstances, target key individuals with biological warfare, traditional targeted killings, or even global strike platforms.

We have already seen many changes on the battlefield in Ukraine, to include the integration of leading-edge technologies with traditional ways of fighting. The proliferation of sensors, AI-enabled analytical tools, smart and loitering munitions, and widely-available space-based imaging and communications are altering the hider-finder contest in ways that are leading to an increasingly transparent battlespace, but also potential opportunities for deception. The

[4] Critical infrastructure refers to those sectors that are considered so vital to the United States that their incapacitation, virtual or physical, would have a debilitating effect on security, national economic security, national public health or safety. See Critical Infrastructures Protection Act of 2001, 42 U.S.C. §5195c (2001).

[5] Gray Zone Project, Center for Strategic and International Studies (last accessed 2022); China Cyber Threat Overview and Advisories, Cybersecurity & Infrastructure Security Agency (last accessed 2022); David Bandurski, China and Russia are Joining Forces to Spread Disinformation, Brookings TechStream (2022).

Ukrainian battlefield is a patchwork of deep trenches and bunkers as troops from both sides have been forced to go underground or huddle in cellars to survive. It is proving exceedingly difficult to mass or move large formations and remain undetected on land, in the air, in or underwater, or in space.

This reality challenges military operations that rely on surprise or tactics that include applying concentrated force on the adversary's weakest points. In a transparent battlespace, advantages will accrue to the side that trusts, empowers, disaggregates, and equips its tactical units. It will reward those forces that have the shortest response time from detection to destruction. Militaries also increasingly create operational opportunities by using long-range, precision fires to disrupt or outright block enemy logistics, destroy higher echelon headquarters, and disrupt operations rather than relying primarily on concentration of forces and tempo.

Drones are changing fire and maneuver in Ukraine, especially when compared to the use of drones over the past two decades in the wars in Afghanistan and Iraq. Both Russian and Ukrainian forces have effectively used many types of drones as expendable intelligence, surveillance, and reconnaissance (ISR) systems, or munitions, or to correct long-range artillery fires with pin-point accuracy. Cheap, attritable drones have also played an important role in degrading costly, advanced air defense systems by forcing them to expend limited missile stocks, while exposing themselves to follow-on attacks by more sophisticated drones and higher-end missiles.[6] They have also been used for counter-value attacks, targeting civilian infrastructure to break popular will to fight. At the same time, drones have proven vulnerable to air defenses and electronic warfare, which reinforces the need to treat many drones as attritable assets.[7]

The tempo of war is also accelerating. Militaries that dynamically change their processes and establish effective, integrated systems to take advantage of large datasets and emerging technologies can dominate the observe, orient, decide, act (OODA) loops by reaching speeds and scales that are impossible to match with analog processes.[8] The growing transparency of the battlefield, the acceleration of the targeting process,[9] and the ability to use drones to eliminate the distance between sensors and shooters all indicate that new technologies are accelerating, and in some cases compressing the decision-making processes and making survival on future battlefields even more challenging. The war in Ukraine itself has become a crucible for military innovation, driving the development and adoption of new concepts and technologies.

---

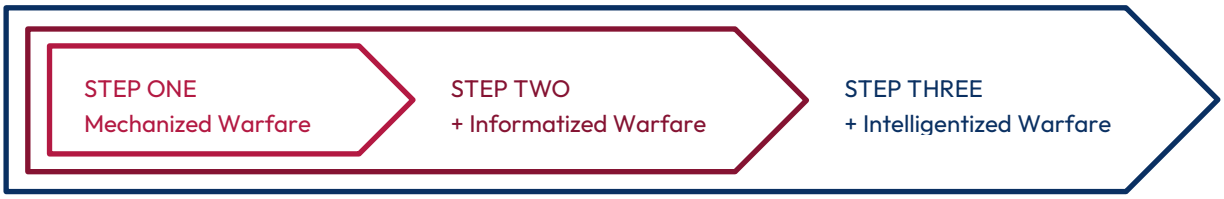
[6] Private engagement with experts on January 26, 2023.

[7] Roughly 90 percent of all drones used in combat in Ukraine are lost, primarily to electronic countermeasures. See Mykhaylo Zabrodskyi, et al., Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February – July 2022, Royal United Services Institute for Defence and Security Studies at 2 (2022). Quadcopters have an average life expectancy of three flights, while fixed-wing drones have an average life expectancy of six flights. See Mykhaylo Zabrodskyi, et al., Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February – July 2022, Royal United Services Institute for Defence and Security Studies at 37 (2022).

[8] Frans Osinga, Science, Strategy, and War: The Strategic Theory of John Boyd, Eburon Academic Publishers at 270 (2005).

[9] Charlie Parker, Uber-Style Technology Helped Ukraine to Destroy Russian Battalion, The Times (2022).

China's Theory of Victory. China is undoubtedly closely observing the emerging lessons from the war in Ukraine. However, for some time now, the People's Liberation Army (PLA) has been harnessing emerging technologies and adapting to the changing character of warfare, principally to deter or defeat the U.S. military, as well as to pursue regional and global ambitions. For over three decades, and the PLA has closely studied the "American way of war." It correctly determined that the U.S. military relies on precision munitions-battle network warfare, which the PLA calls "informatized warfare."[10] It has identified the U.S. military's command, control, communications, and targeting networks as the U.S. operational center of gravity and developed a theory of victory centered around system destruction warfare. This system destruction warfare concept aims to disrupt the flow of internal information, the time sequencing of control-attack-evaluation systems, and essential components of an adversary's operational system through kinetic and non-kinetic means to deconstruct and defeat a military.[11]



In addition to organizing and investing to win informatized wars, the PLA seeks to leapfrog U.S. military capabilities. It intends to capitalize on the growing capabilities of AI, big data, advanced computing and networks, and supporting technologies to conduct what it calls "intelligentized warfare," which involves system-of-systems confrontation relying on information moving through digital systems and networks.[12] Intelligentized warfare has four key features: (1) increased information processing, (2) accelerated decision-making, (3) swarm attacks, and (4) cognitive warfare.[13] The PLA theory of victory ultimately entails shifting from informatized warfare to a hybrid of mechanized, informatized, and intelligentized warfare. It intends to do so by 2027.[14]

Moving beyond theory, the PLA has already organized and equipped itself to counter the U.S. military's way of operating under the conditions of informatized warfare. It has established the People's Liberation Army Rocket Force and amassed a formidable and still expanding arsenal of

[10] Rush Doshi, The Long Game: China's Grand Strategy to Displace American Order, Oxford University Press at 76 (2021).

[11] Jeffrey Engstrom, System Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare, RAND Corporation at 15-17 (2018). System destruction warfare includes but is not limited to the destruction of bases and carriers used for power projection – a move that was earlier associated with anti-access area-denial thinking.

[12] Michael Dahm, Chinese Debates on the Military Utility of Artificial Intelligence, War on the Rocks (2020).

[13] Koichiro Takagi, The Future of China's Cognitive Warfare: Lessons from the War in Ukraine, War on the Rocks (2022).

[14] Military and Security Developments Involving the People's Republic of China, U.S. Department of Defense (2022).

medium- and long-range precision missiles capable of striking U.S. land and sea bases and the connections between them throughout the region, and delaying or even preventing the United States from rapidly intervening in a crisis.[15] They have also made massive investments in Air Force and Naval aircraft, increasing their capacity to attack U.S. forces.[16] As part of these robust anti-access/area denial (A2/AD) efforts, it has also built a dense web of integrated air defense systems to prevent the U.S. military from gaining command of the air domain and to target U.S. reinforcements attempting to enter the theater of operations.[17]

To operationalize system destruction warfare, in 2015 the PRC also created the PLA Strategic Support Force (SSF) to merge information operations, including cyber, psychological operations, electronic warfare, and space operations. The SSF has already established a network for strategic information support that funnels intelligence throughout theater commands and enables joint operations. It also conducts strategic information operations intended to paralyze adversary command and control (C2) systems.[18]

In sum, the PLA has focused on pursuing capabilities across all domains that challenge the U.S. military's ability to project power into the Indo-Pacific, and once there, to enjoy freedom of movement and action.[19] This is a marked departure from previous U.S. military experiences, specifically during the First Gulf War, the wars in the Balkans, and the Global War on Terror, when U.S. forces were able to rely on their ability to (1) build up military power in a region within safe zones before initiating offensive operations and (2) operate from secure bases in order to achieve air superiority followed by sequenced attacks on a degraded enemy. Additionally, China would be able to generate enormous combat power in the Taiwan Strait due simply to proximity.

These realities, combined with the PRC's anti-access/area-denial capabilities and concepts, will deny us the build-up time and benign environment in a Taiwan contingency. U.S. forces will instead have to re-posture instantaneously, and bring decisive combat power to bear within days, to blunt or deny invading PRC forces. While doing so, the U.S. military will have to develop the ability to engage the PLA's operational centers of gravity before the U.S. Air Force can even establish air superiority.

---

[15] Christopher Mihal, Understanding the People's Liberation Army Rocket Force: Strategy, Armament, and Disposition, Military Review (2021).

[16] Xiaobing Li, The Dragon's Wing: The People's Liberation Army Air Force's Strategy, Journal of Indo-Pacific Affairs (2022); Eric Heginbotham, et al., An Interactive Look at he U.S.-China Military Scorecard, Rand Corporation (2015).

[17] Derek Solen, PLA Army Air Defense Units Improve Effectiveness, Resiliency, and Jointness, China Aerospace Studies Institute (2021).

[18] John Costello & Joe McReynolds, China's Strategic Support Force: A Force for a New Era, National Defense University at 2 (2018).

[19] Mike Yeo, China's Missile and Space Tech is Creating a Defensive Bubble Difficult to Penetrate, Defense News (2020).

PART TWO

Objectives for the Joint Force

Confronted with the changing character of warfare and the PLA's theory of victory, the United States military needs a Joint Force with the concepts, capabilities, and characteristics needed to deter PRC military aggression, and if necessary, defeat the PLA. Doing so would close the immediate window of vulnerability we may be facing in the Indo-Pacific and potentially usher in a new character of competition between the U.S. and China. To strengthen deterrence, the Joint Force needs to pursue the following mutually supporting sub-objectives:

- **Decrease the military, economic, and political costs of war for the United States, its allies, and its partners and significantly increase such costs for the PRC.** Shifting the equation to favor the United States more than it does today would strengthen deterrence by increasing the probability that the PLA would be so attrited in a high-end war that it would be denied its military objectives and be left significantly deflated. It would also increase the probability that the political and economic cost of war would be too high to achieve a strategic victory, even if the PLA is able to accomplish its immediate military objectives. Increasing the probability of either outcome would likely alter the PRC leadership's decision-making calculus, and assure U.S. allies and partners.[20]

- **Invalidate PLA investments, concepts, and capabilities.** The PRC has spent decades and trillions of dollars developing the means to defeat the U.S. military, and is poised to spend even more time and money on its efforts to create, scale, and field the capabilities to support its theory of victory. If the U.S. military can reduce the effectiveness of the PLA's concepts and capabilities, it would invalidate massive PRC investments and undermine the PRC's confidence in military success.

  The U.S. military can reduce the effectiveness of the PLA's concepts and capabilities by becoming more resilient in two ways. First, by prioritizing systems that are more robust against the electromagnetic spectrum, cyber, and precision kinetic strikes described in system destruction warfare. This also includes dispersing capabilities and hardening nodes against kinetic attack, and reducing the threat of PLA missiles, including hypersonic missiles. Second, by focusing on the organization, decision-making processes, and capabilities needed to

[20] Roger Cliff, et al., Entering the Dragon's Lair: Chinese Antiaccess Strategies and Their Implications for the United States, RAND Corporation at xv (2007).

continue fighting effectively even if the PLA successfully executes system destruction warfare. In short, the U.S. military should prepare to fight to maintain battle network connectivity, but be designed and prepared to continue fighting effectively even if its network is degraded.

- **Increase the degree of unpredictability the PLA and CCP leadership must account for to be confident of military victory.** Due to a combination of Marxist-Leninist ideology[21] and a lack of confidence in its combat leadership, the PLA relies on the concept of extensively pre-planned warfare.[22] PLA military leaders are expected to follow algorithmically-developed branch plans for contingencies beyond their most likely situation.[23] Increasing the number of potential outcomes that PLA leaders must account for would challenge their ability to plan.

  The U.S. military can increase the PLA's perception of the unpredictability of U.S. forces by generating potential attack vectors along multiple axes and from multiple domains, improving and accelerating planning and decision-making processes so they can generate more courses of action, and allowing commanders to shift risk from humans to machines so they can take courses of action with previously unacceptable levels of risk. The U.S. military should also seek to undermine the PLA's confidence in their military systems and decisions, and the CCP's confidence in its ability to control the narrative for its population during a conflict. Combined, these would reduce the PLA's confidence in victory, and require them to create a greater preponderance of forces, spend more time planning, and expend attention and resources on tasks tangential to the battlefield.

- **Shift some risk from humans to machines, and from expensive and hard-to-replace systems to attritable systems.** As machine capabilities improve, U.S. commanders will increasingly be able to shift some risks from humans or expensive platforms to relatively low-cost machines.[24] This change would allow commanders to execute courses of action with levels of attrition that were previously unacceptable, including frontal attacks, penetrations, and against more determined defenses.

- **Strengthen U.S. and allied power projection.** Many of the PLA's capabilities, including its integrated air defense system, missile regime, and growing air and naval power, are intended to limit U.S. power projection in the Indo-Pacific.[25] To assure its allies and deter PRC aggression, the United States and its allies need to demonstrate their ability to access the

[21] Thomas G. Mahnken, Secrecy & Stratagem: Understanding Chinese Strategic Culture, Lowy Institute at 22-23 (2011).

[22] Wang Xueping, Focus on Cracking the Commanders' "Five Incapables" Problem, People's Liberation Army Daily (2019).

[23] Michael Dahm, Chinese Debates on the Military Utility of Artificial Intelligence, War On The Rocks (2020).

[24] John D. Winkler, et al., Reflections on the Future of Warfare and Implications for Personnel Policies of the U.S. Department of Defense, RAND Corporation at 16-20 (2019).

[25] Mike Yeo, China's Missile and Space Tech is Creating a Defensive Bubble Difficult to Penetrate, Defense News (2020).

region and sustain their forces once they are in the region. While this includes maneuvering within the PLA's range, it also includes the ability to destroy or block ships, boats, and aircraft involved in an amphibious assault of Taiwan while remaining outside the PLA's range. It also includes defending allied territories against crippling attacks from the PLA.

Deterring a PRC invasion of Taiwan from 2025 to 2030 would close a window of vulnerability. It would also likely usher a new, longer-term phase of strategic competition between the United States and PRC, with the United States having to be prepared to deter PRC military aggression, while the PRC attempts to bypass or defeat U.S. efforts. The United States needs to continue to out innovate the PRC, both to maintain the conditions for deterrence and to ensure it can do so without losing an economic, political, or technological competition.

PART THREE

The Foundations of a Competitive Strategy

Last year, SCSP proposed a new offset strategy to respond to the changing character of conflict and the PLA's theory of victory (Part 1) and provide for the objectives of a Future Joint Force (Part 2). Offset-X is a competitive strategy to achieve and maintain U.S. military-technology superiority over all potential adversaries. It is not a war plan, nor a comprehensive or definitive list of actions. Rather, it lays out the foundations and articulates guiding principles for the development of capabilities and design of forces needed to close any near-term deterrence gaps and prevail in the enduring competition. We constructed Offset-X on the pillars of persistent asymmetries of the U.S. military and our whole-of-nation strengths.

Persistent Asymmetries. While the United States faces unprecedented challenges, we also enjoy considerable operational and military-technological asymmetries that can be leveraged against the PRC. The persistent asymmetries described below are the product of democratic institutions, long-standing organizational biases, and experiences that are difficult to deliberately replicate. Using them to shape the way the U.S. military develops, deploys, and uses capabilities will make it difficult for the PLA to replicate U.S. performance, even if it reproduces the underlying technology.

- The U.S. military has unique and battle-tested experiences in joint, combined arms, and expeditionary operations. Combined arms operations are highly complex and demanding, but are necessary for achieving quicker military victory, especially against sophisticated adversaries.[26] The PLA lacks the experience, trust, and cross-domain communication needed to effectively conduct joint and combined operations.[27] It has, however, recognized these shortcomings and placed a high priority on making improvements.[28]
- The U.S. military empowers warfighters at the lowest tactical level to take operational initiative and to develop new solutions, especially in contrast to the PLA, which is constrained by a culture of conformity and a communist political system that typically does not reward initiative.[29] This is especially important in environments characterized by high levels of

[26] Stephen Biddle, Military Power: Explaining Victory and Defeat in Modern Battle, Princeton University Press at 28, 35 (2006).

[27] Testimony of Mark R. Cozad before the U.S.-China Economic and Security Review Commission, PLA Joint Training and Implications for Future Expeditionary Capabilities, RAND Corporation (2016).

[28] Military and Security Developments Involving the People's Republic of China, Annual Report to Congress, U.S. Department of Defense at 158 (2021).

[29] Mission Command: Insights and Best Practices Focus Paper, U.S. Department of Defense Joint Staff, Deployable Training Division at 3 (2020); Mark Cozad, Toward a More Joint, Combat-Ready PLA, National Defense University Press (2019).

uncertainty and degraded communication systems in which U.S. and PLA forces would operate.

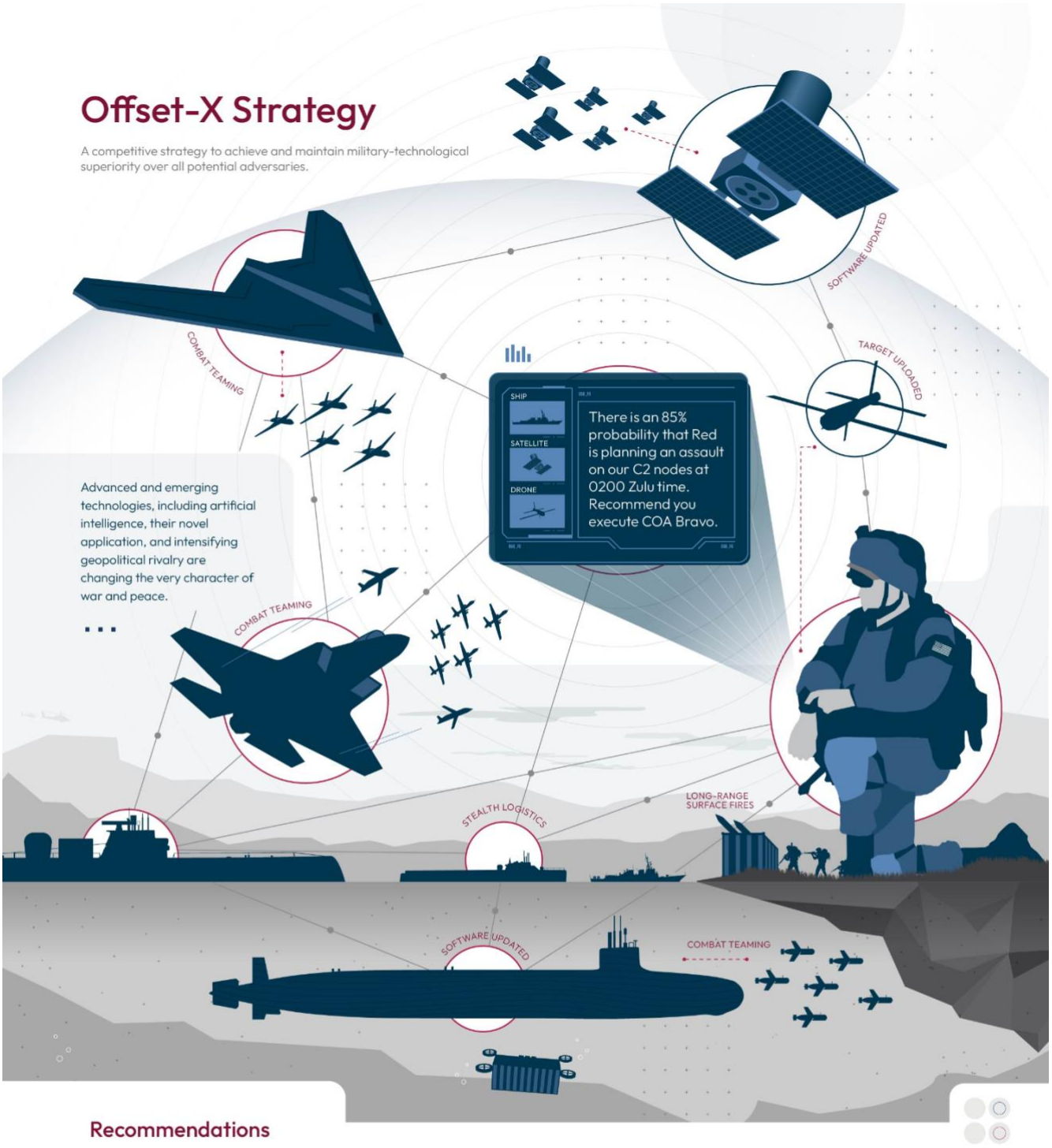
- The U.S. military-civilian logistics system has been one of America's greatest military strengths, both in its reach and in its ability to sustain continuous operations, and remains second to none. That being said, the conflict with China would likely see the PLA attack critical digital systems and physical operations in U.S. and foreign ports of embarkation and disembarkation, and the U.S. ability to produce and transport materials of a military necessity writ large. In short, the U.S. military has an impressive track record of conducting expeditionary logistics, but significant preparations need to be undertaken to retain this important advantage in the contested environment of an Indo-Pacific fight, where the vast distances involved, enemy attacks on infrastructure, and the limited logistical throughput of the region can cripple operations. The PLA for its part has made efforts to strengthen its own untested expeditionary logistical capabilities,[30] in addition to having the advantage of proximity to the potential theater of operations.
- Perhaps most importantly, the United States has far more numerous and deeper alliances than the PRC, which has only one formal ally, North Korea.[31] The U.S. network of alliances enables greater diplomatic legitimacy, builds military mass, creates broader and deeper multi-domain effects, opens up different axes of attacks, and generates intelligence across a much larger network.[32]
- The United States also does not suffer from several authoritarian pathologies,[33] such as coup-proofing, or the reliance on information and population control rather than consent and buy-in for political stability.
- The United States, as a nation, has out-innovated its adversaries over the last several generations. Not only does this underpin U.S. prosperity, it provides the foundation for other future offset strategies that may be required in the long-term competition with China.

[30] Chad Peltier, China's Logistics Capabilities for Expeditionary Operations, Jane's at 4 (2020).

[31] Charles Parton & James Byrne, China's Only Ally, Royal United Services Institute (2021).

[32] The Future of Conflict and the New Requirements of Defense, Special Competitive Studies Project at 19 (2022).

[33] Caitlin Talmadge, The Dictator's Army: Battlefield Effectiveness in Authoritarian Regimes, Cornell University Press (2015).



Recommendations

- Fully Embrace Distributed, Network-based Operations.
- Lead the World's Militaries in Human-Machine Collaboration and Human-Machine Teaming.
- Gain and Maintain Software Advantage.
- Ensure Resilience in Our Ability to Sense, Communicate, Attack, and Supply.
- Undermine Adversary's Censorship System.
- Undermine Adversary's C3 Systems.
- Evolve Deliberate War Planning.
- Help Allies and Partners Develop Interchangeability with U.S. Forces.
- Implement a New Public-Private Partnering Model with Industry, Academia, Investors, and Civil Society.
- Develop and Field Counter-Autonomy.

Components of a Competitive Strategy. Offset-X's ten components[34] describe the technologies and approaches the U.S. military should pursue in order to be in a position to build operational concepts and capabilities:

- **Fully embrace distributed, network-based operations to survive, out-maneuver, and overwhelm adversaries.** Confronted with adversaries that value rigid hierarchies, but that have exquisite sensing capabilities and have invested heavily in defenses against concentrated assaults, the U.S. military should continue to develop and experiment with the employment of smaller, organically resilient, multi-domain units that practice network-based decision-making.
- **Lead the world's militaries in Human-Machine Collaboration (HMC) and Teaming (HMT).** HMC will be critical to optimizing decision-making in warfare. HMT will be essential for more effective execution of complex tasks, especially higher risk missions, with lower human cost. The U.S. military must be the leader in both.
- **Gain and maintain software advantage.** A military's ability to deploy, employ, and update software, including Artificial Intelligence (AI) models, faster than its adversaries is likely to become one of the greatest determining factors in relative military strength. The U.S. must ensure its primacy in such software-enabled warfare.
- **Ensure resilience in the ability to sense, communicate, attack, and supply.** In a potential conflict with China, one of the PLA's opening moves will likely be directed at U.S. forces' ability to see, track, and locate them precisely. Simultaneous or follow-on attacks will likely target the ability of U.S. military leaders to command and control their forces. Additional attacks will almost certainly be aimed at the U.S. military's logistics. The U.S. military, therefore, needs to build resilience, including through redundancies and cyber hardening, across every link and node of its operations.
- **Undermine PRC censorship systems.** Authoritarian regimes rely predominantly on information control rather than popular buy-in to maintain domestic stability. The United States should be in a position to exploit this vulnerability and conduct operations that expose the adversary's population to information other than state propaganda.
- **Undermine PRC command systems.** The United States should also focus on subverting the effectiveness of PLA's command, control, and communication (C3) systems to cause disarray among its ranks, inhibit its ability to command forces, and desync its operations.
- **Develop counter-autonomy.** As the U.S. military integrates more AI, human-machine teaming, and autonomy in its systems and ranks, the PLA can be expected to do the same.

[34] This section is an abbreviated version of the components of Offset-X. A full version that includes actionable steps for the Department of Defense can be found in The Future of Conflict and the New Requirements of Defense, Special Competitive Studies Project at 19-31 (2022).

The U.S. military should, therefore, develop capabilities and concepts for countering adversary autonomy and adversary attacks on U.S. military's autonomous systems.

- **Help allies and partners develop and maintain interoperability and interchangeability with U.S. forces.** There is a risk that a gap in capabilities between the United States and its allies could become a serious impediment to combined operations. The U.S. government must accept far greater risks in information sharing and transfer of technologies to minimize this gap. In the near-term, the United States could pursue two promising actions – the development of a multilateral ISR network[35] and the development of a Joint and Combined All Domain Command and Control architecture.
- **Implement a new public-private partnering model between the U.S. government, industry, academia, investors, and civil society.** If the United States can unite all five stakeholders to pursue specific goals, America's dynamic capitalist market system and innovative commercial sector are much more likely to prevail over the state-led economic model of the PRC.
- **Evolve deliberate war planning.** Today's approaches to war planning do not sufficiently account for the resiliency of the defense industrial base and its ability to surge production. They also constrain the development of innovative concepts, and reduce the ability of combatant commanders to influence the development of new capabilities.

[35] Becca Wasser, Developing Integrated ISR Networks to Improve Coalition Responsiveness, Presented at SCSP Defense Panel Meeting (July 2022).

PART FOUR

From an Institutional Strategy to Capabilities

New force design takes time to take full effect. In 2027, DoD will largely operate with forces it has already designed. However, the military services and combatant commands can still adopt the capabilities[36] below to operationalize Offset-X and prepare our forces to deter, and if necessary, defeat PRC aggression in the Indo-Pacific. Notably, the capabilities are organized by warfighting function rather than the components of Offset-X to directly translate them into a vision of warfighting and operational capability.

Each warfighting function starts with a description of mission requirements, and then outlines the capabilities needed to deliver on those missions. The capabilities outlined are based on technologies that are already fielded or in development. A sample of new technology-based solutions can be found in Annex A. By themselves, the technology-based solutions will not necessarily lead the United States to prevail in peacetime, crisis, or conflict. However, individually or in combination, they can address parts of the challenge, and significantly strengthen the U.S. military's ability to meet the near-term challenge that it faces in the Indo-Pacific region.

Command and Control (C2)

Mission Requirements. To successfully command and control joint and coalition forces in a conflict in the Indo-Pacific, the United States and its allies and partners need to be able to make real-time, informed decisions; generate predictive and proactive insights about their adversaries, their own forces, and the environment; present the PLA with multiple dilemmas; and be able to coordinate and command efforts globally. The U.S. military, its allies, and partners need a C2 architecture that will enable them to be far more tactically flexible, interchangeable with allies, scale on demand, and adapt dynamically to changing conditions.[37]

[36] This section outlines the capabilities that will operationalize Offset-X and help invalidate the PLA's investments, increase their uncertainty, shift risk from humans to machines, and strengthen U.S. power projection. We admit, however, that it is far easier to propose capabilities than to understand how to develop them. For the next step in that direction, Annex A contains a selection of technology-based solutions for the proposed capabilities.

[37] Nand Mulchandani & John N.T. Shanahan, Software-Defined Warfare: Architecting the DoD's Transition to the Digital Age, Center for Strategic and International Studies (2022).

Capabilities Needed. To make such a C2 architecture function, the U.S. military needs a combination of resilient communications; an accurate and continuously-updated all-domain operational picture; ability to generate and assess feasible and creative courses of action faster than its adversaries; and more network-based decision-making.

Technology-Enabled Solutions. Adaptive communication systems and modular C2 are already in the R&D ecosystem, and have the potential to contribute to resilient communications, and to enabling distributed, network-based operations.[38] Human-machine enabled planning tools can improve situational awareness and empower a planning process that is faster, more creative, generates more options, and is better suited to creating a plan optimized for a specific challenge.[39] Mesh networks improve resiliency by connecting across many nodes based on availability, rather than using the more common hierarchical model where information flows up and down, but is not routed laterally. Software baselines enable communication between systems, and between militaries, and have been in use in the private sector and in some parts of the military for years, but have not yet been adopted at scale by the Department of Defense.

Intelligence

Mission Requirements. Intelligence provides analysis of the operating environment; an understanding of adversary capabilities, vulnerabilities, and future courses of actions; and a map of friendly, neutral, and threat networks.[40] While traditional intelligence for planning will still play a valuable role, the U.S. military also needs live, dynamic analysis for military operations. Networks, platforms, and sensors will also need to penetrate adversary defenses to attain geographic and virtual access to activity and data.[41] U.S. military services' intelligence chiefs have described a shift from a "manpower-intensive, permissive environment force to an automation-intensive, high-threat environment force" needed to gain and maintain information advantage across the gray zone and highly contested environments.[42]

Capabilities Needed. To meet these mission requirements in an Indo-Pacific contingency, the U.S. military needs a combination of data source integration, greater speed and scale for analysis, improved human-systems integration, human-machine collaboration for intelligence analysis,

[38] Cognitive Communications, U.S. National Aeronautics and Space Administration (last accessed 2023); New C2 Tech Enables Rapid Decision Making, Response, Booz Allen Hamilton (last accessed 2023).

[39] The Future of Conflict and the New Requirements of Defense, Special Competitive Studies Project at 24 (2022).

[40] JP 3-0, Joint Operations, U.S. Joint Chiefs of Staff at III-27, (2018).

[41] Richard B. Shermer & Christopher T. Lenick, Strengthening Intelligence, Surveillance, and Reconnaissance Employment in the Indo-Pacific Region, Journal of Indo-Pacific Affairs (2022).

[42] John R. Hoehn, Intelligence, Surveillance, and Reconnaissance Design for Great Power Competition, Congressional Research Service at 14 (2020).

intelligence dissemination for distributed forces, and enhanced deception against adversary AI-enabled and autonomous systems.

Technology-Enabled Solutions. Open-source intelligence, autonomous intelligence, surveillance, and reconnaissance (ISR) platforms, and micro-satellite constellations can provide for enhanced battlefield awareness, shorten the sensor-to-sensor cycle, and enable long-range precision fires in denied and degraded environments. Digital nervous systems capable of searching for patterns and connecting thousands of presumed anomalies across aggregate data streams can provide anticipatory indications and warning, and inform more sophisticated strategic decisions. Human-machine teams leveraging machine learning capabilities can optimize information collection, filtering, and prioritization of high-volume, multi-source information for human intelligence analysts.

Movement and Maneuver

Mission Requirements. Successful maneuver during a conflict in the Indo-Pacific would entail defending allied or partner territory from seizure, disrupting or destroying adversary forces on allied or partner territory, leveraging alternative operating bases for U.S and allied forces, and maneuvering as a distributed force within range of adversary attacks. The increasing transparency of the operating environment, combined with the PLA's long-range precision fires, makes it much more difficult to mass force. The U.S. military will need to coordinate effects from distributed forces, and find new ways to create effects that have traditionally relied on mass.

Capabilities Needed. To meet the above mission requirements for movement and maneuver in an Indo-Pacific contingency, the U.S. military needs attritable capabilities in large quantities and across several domains. It also needs access to allied bases and airspaces during the critical first few days of a conflict. Most if not all operations must begin with deception operations, or employ masking.[43] Partner forces, enabled by or alongside U.S. forces, must be able to impose large costs on PLA ground-based or amphibious offensive operations.

Technology-Enabled Solutions. Multi-agent swarms offer an opportunity to increase the cost to adversary offensive operations, as well as to attrit its defensive systems. HMT would allow the U.S. military to employ lower-cost, easier- and faster-to-manufacture AI-enabled machines, and to develop new operational concepts to permit operators and machines to overcome complex, high-risk challenges. Counter-autonomy efforts could include actions to manipulate the data or outputs of adversarial AI-enabled systems to inject mistrust between their forces and their machines, degrading the performance of their AI-enabled and autonomous systems, or

[43] John Antal, 7 Seconds to Die: A Military Analysis of the Second Nagorno-Karabakh War and the Future of Warfighting, Casemate at 156 (2022).

destroying them entirely through kinetic or non-kinetic means.[44] Prepositioned assets create more maneuver opportunities for U.S., allied, and partner forces. Decoys that raise background noise and confuse adversary sensors and operating pictures can mask efforts to maneuver.

Fires

Mission Requirements. Successful joint fires operations require the U.S. military to project power into denied space either from within or outside of the PLA's weapons engagement zone; destroy or disrupt PLA air, amphibious, and missile forces; achieve dynamic targeting and fire through multiple options; and disrupt PRC sensing and targeting networks.

Capabilities Needed. To meet the above mission requirements for fires in an Indo-Pacific contingency, the U.S. military needs a combination of long-range and deep strike capabilities, a high volume of both munitions and drones, multivector fires, and the simultaneous ability to disrupt or destroy adversary ISR and electromagnetic spectrum operations, while providing friendly disaggregated forces the connectivity and authorization they need to access fires, even when cut off from higher headquarters.

Technology-Enabled Solutions. Next-generation conventional cruise missiles capable of long-range strike would allow U.S. forces and allies to strike adversary assets from a standoff range. Hypersonic missiles would combine speed, accuracy, range, and survivability to neutralize adversary A2/AD systems outside of their range with high-accuracy and speed. Additive manufacturing of custom munitions and drone components could enable U.S. forces and allies to rapidly and remotely fabricate energetic material payloads and munitions.

Sustainment (Expeditionary Logistics)

Mission Requirements. The United States and its allies must be able to conduct distributed operations while under persistent surveillance and attacks by aircraft, missiles, undersea vessels, and in the electromagnetic spectrum.[45] The ability to project logistical support is central to achieving mobile and distributed forces, which require a depth of munitions, energy, personnel, replacement parts, and end items, such as drones, for combat success against a near-peer adversary like the PLA. It also has the potential to strengthen U.S. and allied power projection into the Indo-Pacific; invalidate PLA system destruction warfare operations against U.S. and allied

[44] Counter Autonomy: Executive Summary, U.S. Department of Defense, Defense Science Board at 3 (2020).

[45] Force Design 2030: Annual Update, U.S. Marine Corps (2022).

forces, assets, and infrastructure; and increase the degree of unpredictability that the PLA must account for by ensuring the continued operation of distributed forces.

Capabilities Needed. To meet the above mission requirements for expeditionary logistics in an Indo-Pacific contingency, the U.S. military needs to proactively distribute and preposition critical materials and supplies. U.S. forces should also improve their ability to sustain themselves from prepositioned or locally sourced materials. Sustainment operations should avoid detection by employing a combination of deception, masking, and undersea movement. Sustainment hubs and lines of communication also need to undergo cyber and physical hardening to reduce their vulnerability to attack, and strengthen their resilience.

Technology-Enabled Solutions. Low-profile, autonomous vessels are able to provide long-range, multi-ton resupply to U.S., ally, and partner forces in the Indo-Pacific with a reduced probability of detection.[46] Rapid, transportable runway repair kits would make air bridges significantly more resilient. Portable hydrogen fuel generators have the potential to fuel light battalion-size formations using only prepositioned and locally sourced supplies.[47] Metal 3D printing technology could provide rapid and cost-effective replacement parts for military applications.

Information

Mission Requirements. The United States and its allies and partners need to be proactive in the information domain, using information as an offensive capability and defending against increasingly sophisticated influence operations. At the strategic level, this entails undermining an adversary's ability to control its population's access to information, carefully and precisely injecting narratives among adversary leaders that undermine adversary offensive operations and popular will to fight, and reducing the spread of adversary-generated misinformation.[48] For military operations, it entails undermining adversary command systems to co-opt, disrupt, or cripple adversary information systems, and undermining adversary trust in autonomous systems and decision aids.

Capabilities Needed. The PRC's censorship regime is robust, and generally effective. To meet requirements for information in an Indo-Pacific contingency, the U.S. military needs the ability to saturate or bypass censorship regimes. The U.S. military and IC also need to invest in a variety of attack capabilities that target adversary artificial intelligence/machine learning (AI/ML) models.[49]

---

[46] Attritably may vary based on a vessel's cargo.

[47] Presentation to the Defense Panel on July 19, 2022.

[48] Intelligence in An Age of Data-Driven Competition, Special Competitive Studies Project at 34 (2022).

[49] Final Report, National Security Commission on Artificial Intelligence at 52 (2021).

Technology-Enabled Solutions. Existing technology can enable citizens in adversary countries to bypass censorship, either by avoiding automated censorship patterns or using alternate means to communicate without using the state-monitored internet or cell phone networks. Offline, peer-to-peer communication applications, especially with anonymous use built in, would help citizens of authoritarian nations avoid censorship.[50] Generative AI models may help overwhelm adversary censorship systems and to provide alternative, precision messaging mechanisms.

Protection

Mission Requirements. The maturation and diffusion of cyber and electromagnetic spectrum capabilities, uncrewed aerial vehicles, precision-guided, long-range ballistic and cruise missiles, and counterspace systems have significantly expanded the scope and complexity of defending forces.[51] Successful multi-layered force protection in the Indo-Pacific requires real-time threat detection and response; a credible tactical and strategic missile defense capable of withstanding attacks; and the ability to defend expensive platforms and reduce the effects of adversary long-range fire.

Capabilities Needed. To meet the above mission requirements for protection in an Indo-Pacific contingency, the U.S. military needs to develop a layered missile defense system capable of defending against a proliferating number and type of missile threats; integrate regional missile defenses with allies and partners to fill gaps and reinforce sensing and intercept capabilities; strengthen active and passive defense systems to protect assets, bases, and critical infrastructure against kinetic, cyber, and electronic threats; and autonomously predict, detect, and counter threats.

Technology-Enabled Solutions. Agent-based modeling and simulations of missile defense systems can inform and improve the design scheme of missile defenses. Cyber-hardening of networks, sensors, and operational systems using AI and automation tools reduces the attack surface of systems and increases the difficulty of access and exploitation by adversaries. Zero trust architecture for cybersecurity continuously validates access at every interaction and fortifies data, applications, assets, and services to achieve enhanced cyber resiliency. Counterspace weapons can protect friendly space systems from attack, interference, and unintentional hazards before, during, or after an attack, and compromise adversaries' ability to leverage the space domain to support warfighting or threaten U.S. and allied forces.

Adaptation

[50] Peter Shadbolt, FireChat in Hong Kong: How an App Tapped its Way into the Protests, CNN (2014).

[51] Vishal Giare & Gregory A. Miller, Air and Missile Defense: Defining the Future, Johns Hopkins APL Technical Digest at 506 (2021).

Mission Requirements. Adaptation is not currently a warfighting function. However, it is likely to become increasingly important in warfare as software and connectivity accelerate the adaptation of tactics and technology. Thus, it deserves as much specific focus as the other warfighting functions. In future near-peer conflicts characterized by extremely high operating tempos and even algorithmic warfare, battlespace advantage might be temporary and fleeting. The side that is capable of adapting faster to unanticipated developments by the other side, while inducing disorientation and mental paralysis in the adversary's forces, will likely gain the advantage. This includes software agility. Militaries that focus as much effort and structure towards adaptation as to the other warfighting functions will gain a marked advantage over those that do not.

Capabilities Needed. To meet the above mission requirements for adaptation in an Indo-Pacific contingency, the U.S. military needs to improve its digital infrastructure, place trained and authorized personnel in the right positions in the right organizations, create mechanisms and processes for continuous integration and continuous delivery (CI/CD), and create authorization to operate (ATO) processes that move at an operationally relevant pace.[52]

Technology-Enabled Solutions. Existing technologies, such as AutoML, can help accelerate and deskill some parts of the development process.[53] Doing so will help military units, especially those in field environments, adapt more quickly. Practices that are beginning in the military services, like open architectures, can further reduce the barriers to creating new software to solve problems.

[52] SCSP interviews with service members and defense technologists.

[53] What is Automated Machine Learning (AutoML)?, Microsoft Build (2023).

Capabilities of a Joint Force

Functions	Mission Requirements	Capabilities Needed	Tech-Enabled Solutions
Command & Control (C2)	• Make real-time, informed decisions • Generate predictive and proactive insights • Present PLA with dilemmas • Have structure to C2 globally • Generate and assess feasible and creative courses of action faster than adversaries	• Resilient communications • All-domain operational picture • More network-based decision-making	• Adaptive communication systems and modular C2 • HMC enabled planning tools • Mesh networks • Software baselines
Intelligence	• Live, dynamic analysis for military operations • Networks, platforms, and sensors that penetrate adversary defenses' • Shift from a “manpower-intensive, permissive environment force to an automation-intensive, high-threat environment force”	• Data source integration • Greater speed and scale for data analysis • Human-machine collaboration for intelligence analysis • Intelligence dissemination for distributed forces • Enhanced deception against adversary AI-systems	• Open-source intelligence, autonomous intelligence, surveillance, and reconnaissance (ISR) platforms • Micro-satellite constellations • Digital nervous systems • HMTs leveraging ML capabilities
Movement & Maneuvers	• Disrupt or destroy adversary forces • Defend allied or partner territory • Expand options for alternative bases • Maneuver as a distributed force	• Access to allied bases and airspaces • Improved deception operations or masking, including through the use of decoys • Impose large costs on PLA ground-based or amphibious offensive operations	• Multi-agent swarms • HMT • Counter-autonomy • Prepositioned assets
Fires	• Project power into denied space • Destroy or disrupt PLA air, amphibious, and missile forces • Achieve dynamic targeting and fire • Disrupt PRC sensing and targeting networks • Disrupt or destroy adversary ISR and electromagnetic spectrum operations	• Long-range, deep strike capabilities • High volume of munitions, drones, and multivector fires • Access to fire for disaggregated forces	• Next-generation conventional cruise missiles • Hypersonic weapons • 3D printing of custom munitions and drone components
Sustainment (Expeditionary Logistics)	• Project logistical support with a depth of munitions, energy, personnel, replacement parts, and end items, such as drones	• Proactively distribute critical materials and supplies • Reduce sustainment requirements • Avoid detection • Cyber and physical hardening	• Low-profile autonomous vessels (LPVs) • Rapid, transportable runway repair kits • Portable hydrogen fuel generators • Metal 3D printing
Information	• Undermine adversary’s censorship system • Inject narratives among leaders • Reduce the spread of misinformation and disinformation at home • Undermine adversary command systems and trust in autonomous systems	• Saturate or bypass censorship systems • The ability to attack AI/ML models	• Media Manipulation Monitor • Offline, peer-to-peer communication applications • Data poisoning injects and and other counter-AI methods
Protection	• Expand sensor network of real-time threat-detection and response • Tactical and strategic missile defense system • Defend platforms and reduce the effects of enemy long-range fire	• Layered missile defense systems • Integrate regional missile defense systems with allies and partners • Strengthen active and passive missile defense systems	• Agent-based modeling and simulations • Cyber-hardening of networks, sensors, and operational systems • Zero trust architecture • Counterspace weapons
Adaption	• Adapt faster to unanticipated developments • Place trained and authorized personnel in the right positions in the right organizations	• Improve digital Infrastructure • Place trained and authorized personnel in the right position • Create mechanisms and processes for continuous integration and continuous delivery (CI/CD) • Create an authorization to operate processes that move at an an operationally relevant space	• Automated machine learning (AutoML) • Open Architecture

PART FIVE

Characteristics of the Future Joint Force

Confronted with the changing character of warfare and the PLA's theory of victory, the U.S. military needs a new force design. This Future Joint Force must be defined by a set of Offset-X-derived characteristics and be able to field and employ the capabilities described in the previous section of this report.

To guide the execution of this force design, each characteristic below includes a description and explanation of how it contributes to the objectives of a Joint Force (Part 3), as well as actions with near-term impact to develop the Joint Force from now to 2027, and actions with medium-term impact to equip the Future Joint Force with an enduring advantage against the PLA.

Operates As a Distributed, Network-Based Organization

The U.S. military needs to draw on its history of empowering tactical leaders and successful joint operations to develop a highly-distributed, network-based force that can thrive in system destruction warfare. "Distributed" means spreading forces across geography. Network-based forces, as opposed to hierarchy-based forces, are characterized by localized decision-making and resources, and the cumulative creation of effects. It should be noted that network-based does not refer to connectivity to a centralized, digital network, and is unrelated to network-centric warfare. Instead, it emphasizes distributed decision-making that can still operate with intermittent connectivity.

Network-based, distributed forces tend to be more adaptive and resilient, and perform well when nodes are empowered and able to communicate laterally. Small units within a distributed, network-based force empowered by higher headquarters can employ judgment at the lowest level to fulfill mission type orders, leveraging the innovation and entrepreneurship that comes more naturally to democratic states. The Ukrainian forces' ability to employ network-based forces has been a significant factor in their ability to overcome intense Russian electromagnetic spectrum operations and attacks on their C2 network.[54]

[54] Azeem Azhar, The Russian vs. the Ukrainian Network, Exponential View (2022).

The PLA plans to defeat the U.S. military by systematically targeting the linkages and nodes that hold its advanced, highly-connected force together.[55] A distributed, network-based force could help invalidate these PLA concepts and blunt its capabilities. Organically resilient due to its network-based structure, such forces would be capable of preserving decision-making and effects while absorbing damage in degraded and denied environments. Geographic distribution would make it easier to mask or hide U.S. forces' signatures, and would force the PLA to diffuse its fires and attacks to degrade U.S. and allied forces. Acting in concert, these forces would also create mass, compound effects, and operate with greater adaptability than single systems to impose multiple dilemmas on the PLA. Distributed nodes with multi-domain capabilities would increase the tactical and operational unpredictability the PLA would need to account for by increasing the number of potential U.S. military attack vectors, and preserving options for the Joint Force even while it is being degraded.

Actions with Near-Term Effects.

- **Stand up joint tactical units that are organically equipped to conduct distributed, multi-domain operations.** A distributed, network-based force would be capable of employing small, multi-domain units inside and outside the adversary's envisioned battlespace. This would include tactical mobility suited to the Indo-Pacific, including distributed and stealthy logistics, ISR, and organic firepower to support themselves and destroy sea and air-based PLA assets, along with connectivity and authorities for non-organic assets, including on-call fires from all domains.
- **Incorporate network-based decision-making into training exercises.** Training exercises, especially large-scale training, should feature local decision-making, lateral communication, and a lack of reliance on higher echelons of command in an environment with a shifting combination of effective and degraded communication systems. Network-based decision-making should be incorporated into live and virtual scenario-based training, and include incentives for local decision-making, the self-organization of teams, and risk-taking.
- **Ensure distributed units have access to all-source intelligence and AI-enabled analytic and decision aids.** Distributed, network-based units need to be able to make informed decisions independently, even when cut off from higher headquarters. The Future Joint Force needs to ensure that distributed units are equipped with communications systems and authorities needed to securely access tactical intelligence, as well as analytic tools powered by AI.

Actions with Medium-Term Effects.

- **Ensure distributed units are trained and equipped to employ counter-AI strategies to evade, overtake, or destroy PLA sensors.** The proliferation of sensors combined with AI-enabled

[55] Jeffery Engstrom, System Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare, RAND Corporation at 15-17 (2018).

analytical tools, UAVs, and satellite imagery data are leading to an increasingly transparent battlespace. The Future Joint Force needs to train and equip distributed units to employ counter AI-enabled sensors and improve their survivability, even as sensors continue to proliferate. Counter-AI and counter-autonomy will be addressed in more detail below.

Functions as a Human-Machine Team, Both as a Whole and as Individual Nodes on the Network-Based Force

A distributed, network-based Joint Force would rely on human-machine collaboration (HMC) and human-machine combat teaming (HMT) to empower the network as a whole and strengthen each individual node on the network. HMC and HMT are the combination of three elements: the human, the machine, and the interactions and interdependencies between them.[56] HMC focuses on optimizing cognitive tasks, particularly decision-making. HMT focuses on more effectively executing complex tasks, including in combat operations. HMC and HMT are not mutually exclusive and neatly separable. Many applications, especially more advanced applications, will include elements of both.

A core concept of HMC and HMT is that humans and machines have comparative advantages and excel in different areas.[57] Humans generally outperform machines on high-context tasks requiring intuition, and various types of creative exploration. Machines often outperform humans at tasks that require processing extremely large volumes of data, a high degree of precision, speed, or consistent repetition. Augmenting human weaknesses with machine strengths (and vice versa), can create interdependent human-machine teams that outperform both humans and machines individually.[58]

Militaries that have incorporated HMC and HMT can identify bottle-necks in their operations, delegate tasks to machines as much as possible, and move humans to the boundaries of machine capabilities, where they can perform tasks that humans can do more effectively than machines.[59] Both the overall network described above, and the individual nodes on the network would be able to make decisions and conduct operations more effectively, more quickly, and on a larger scale than if they do not incorporate HMC and HMT, all at a lower human cost. Machines can also perform tasks that are too dangerous for humans, allowing units to perform operations that would otherwise not be feasible.[60]

---

[56] Margarita Konaev & Husanjot Chahal, Building Trust in Human-Machine Teams, Tech Stream (2021).

[57] Tony Ojeda, The Algorithm – Human Tasks vs. Machine Tasks, District Data Labs (last accessed 2023).

[58] Edgar Jatho & Joshua A. Kroll, Artificial Intelligence: Too Fragile to Fight?, U.S. Naval Institute, (2022).

[59] Marco Iansiti & Karimi R. Lakhani, Competing in the Age of AI, Harvard Business Review at 40 (2020).

[60] John Laird, et al., Future Directions in Human Machine Teaming Workshop, U.S Department of Defense at 3 (2019).

HMC in particular could expand a military's ability to assess situations, quickly and effectively plan, and make decisions. A warfighter's mental bandwidth, as for every human, is limited. Military personnel collaborating with machines are able to break problems into their component pieces and task some to be optimized, automated, or performed at scale by a computer. Doing so will remove clutter that takes up cognitive bandwidth and free warfighters to focus on higher-order processing, gaining situational awareness, understanding enemy plans, and developing or selecting courses of action.[61] It will also allow military personnel to quickly and effectively perform cognitive tasks that would be difficult or impossible without machine collaboration.

HMC and HMT have the potential to contribute to all of the objectives in Part 2. HMT would allow the Future Joint Force to shift risk from humans to machines that would conduct reconnaissance, attacks, or defenses that might otherwise cost human lives. If the machines are low cost and uncrewed, they can also reduce the risk to expensive and hard-to-replace systems. By increasing planning capabilities and capacity, HMC would enable the U.S. military to generate more creative and a greater number of courses of action and increase the degree of unpredictability the PLA would face. HMC and HMT also have the potential to weaken system destruction warfare's effects, both by expanding the capabilities of each node of a network-based force, and by helping prepare for and react to attacks in the electromagnetic spectrum and cyber domain.

Actions with Near-Term Effects.

- **Develop novel warfighting concepts.** The Future Joint Force will not be able to capitalize on the potential of HMC and HMT if it only integrates them into existing ways of operating. It needs new warfighting concepts. To that end, each military service should develop novel warfighting and employment concepts for HMC and HMT that allow them to capture both human and machine strengths in their respective domains. The Joint Staff should lead the development of a joint doctrine for HMC and HMT.
- **Develop decision aids for operational units and incentivize unit-level development and use.** The Strategic Capabilities Office and service-based rapid capabilities offices should develop decision aid tools, with an initial operating capability of no later than 2025. Operational units can develop and use simple decision-aids for narrow tasks, many of which would require relatively little training to develop, or have commercially available solutions. Even such simple models would be able to tap into the advantages of machine speed and scale to improve or accelerate decision-making processes.[62]
- **Develop and field more effective interfaces.** Even the best tools can be ruined by ineffective interfaces, especially in combat environments where cognitive demands can already be very high. DoD needs to invest in improving human-machine interfaces to allow military personnel

[61] What Is Computational Thinking?, Center for Computational Thinking, Carnegie Mellon University (last accessed 2023).

[62] Justin Lynch & Alexander Mann, Your Laptop Does More than Powerpoint: Computational Thinking and Changing the Military's Mindset, Modern War Institute (2021).

to more efficiently input data, absorb information from machines, and assign or delegate tasks.

- **Train for HMC and HMT at combatant commands (CCMDs), major training centers, and regular unit training.** Every service and CCMD should develop and execute a training program that uses HMC and HMT. All major training centers should integrate HMC and HMT into every rotation, including integration into opposing force capabilities. Commanders should also immediately begin creating opportunities for tactical units to experiment, develop tactics, techniques, and procedures during local-level training. Such opportunities need to be separated from preparing for combat rotations, which places pressure on units to meet training objectives rather than to understand the implications of new capabilities. Results from training at every level should be collected to begin assessing the implications for capability development, equipment selection, and force structure. The results should then be integrated into further training.
- **Implement an HMC and HMT readiness scorecard.** DoD should design a readiness scorecard that tracks and encourages the integration of HMC and HMT capabilities across services.
- **Compete traditional platforms against new, uncrewed systems.** Experimentation with new technologies and operating concepts against the old is needed to push the envelope of warfighting capabilities. The AlphaDogfight Trials conducted by Defense Advanced Research Projects Agency (DARPA)'s Air Combat Evolution (ACE) program, which pitted AI agents against an experienced F-16 pilot in a series of simulated dogfights, is an example of how competition can delineate the respective set of functions and roles best performed by new and traditional systems.[63]
- **Allow combatant commands to reinvest HMC and HMT driven savings.** Combatant commands should be allowed to reinvest the money they save by integrating HMC and HMT, in addition to funds they would be eligible to receive through sources such as the Rapid Defense Experimentation Reserve (RDER) and the Pacific Deterrence Initiative (PDI).[64]

Actions with Medium-Term Effects.

- **Integrate HMC and HMT lessons into entry-level training and continuing education requirements.** The services should integrate computational thinking into entry-level training and continuing education requirements for commissioned and non-commissioned military and civilian personnel. This would have significant overlap with data-informed decision-making, and would include lessons in problem curation, data collection and management, the AI stack, probabilistic reasoning and data visualization, and data-informed decision-making.

[63] AlphaDogfight Trials Foreshadow Future of Human-Machine Symbiosis, U.S. Defense Advanced Research Projects Agency (2020).

[64] Sydney Freedberg, Hicks Seeks To Unify Service Experiments With New 'Raider' Fund (2021); Hibbah Kaileh & Luke Nicastro, The Pacific Deterrence Initiative: A Budgetary Overview, Congressional Research Service (2023).

- **Assess and change force structure based on HMC and HMT experimentation and novel warfighting concepts.** As HMC changes the speed, scale, and character of cognitive tasks and HMT creates new operational possibilities, the Future Joint Force will need to reconsider the tasks it is aligned to accomplish, and its force structure.

Gains and Maintains Software Advantage

Software is now integral to every component of combat, from sensing a target (sensor software), to decision-making (aggregation and analysis), targeting (weapons guidance system), and battle damage assessment.[65] As militaries around the world increasingly rely on platforms with advanced computing capacities, and supplement or even replace some functions of human service members with algorithms, software advantage will become an even greater determining factor.[66] The quality of software will determine a military's primacy in collecting and analyzing information, developing an operating picture, thwarting enemy attacks, identifying opportunities in time and space to most effectively attack, and aiding target selection and servicing.[67] This will be especially true as systems with autonomous components play a larger role.

Software advantage is the ability to develop, field, use, and update software that accomplishes critical tasks more effectively and quickly than competitors. Competing groups seek to adapt to each other's tactics and weapons, and as one side gains an edge, the other side seeks to neutralize it.[68] Commercial firms have long recognized that they can create a competitive advantage by iterating, updating, and deploying smart algorithms faster than their competition.[69] As software plays an increasingly important role in warfare, the importance of doing the same for military systems will only increase. Weapon guidance systems will need to better track adversaries that are using new camouflage, control systems will need to respond slightly faster to outpace enemies, and electronic warfare platforms will need to better assess and respond to enemy systems, all in real time.

Software advantage would contribute to all of the objectives listed above for the Future Joint Force by enabling it to generate new and improved capabilities faster and more effectively than the PLA and other adversaries. Most notably, software advantage would improve performance in virtually every aspect of HMC and HMT. Semi-autonomous systems, human-machine interfaces, decision support tools, and almost every other type of human-machine teaming is partially or entirely the product of software. Just as importantly, as human-machine teams

[65] Department of Defense Software Modernization Strategy, U.S. Department of Defense at 1-2 (2021).

[66] Software Acquisition and Practices (SWAP) Main Report, U.S. Department of Defense (2019).

[67] Nand Mulchandani & John N.T. "Jack" Shanahan, Software-Defined Warfare: Architecting the DOD's Transition to the Digital Age, Center for Strategic and International Studies at 1-2 (2022).

[68] Edward Luttwak, Strategy: The Logic of War and Peace, Harvard University Press at 28-31 (2001).

[69] Marco Iansiti & Karimi R. Lakhani, Competing in the Age of AI, Harvard Business Review (2020).

encounter unexpected challenges, much of their adaptation will take the form of software updates. This is especially true for potentially isolated units in a distributed, network-based force, whose access to new or additional hardware may be limited.

Software can also facilitate the shift from a small number of exquisite sensors and communication platforms to a large number of significantly less expensive and capable systems whose integration through software can produce the same information as existing, expensive sensors and communication platforms. This is particularly important for invalidating system destruction warfare. In the electromagnetic spectrum and cyber domains more broadly, software advantage will be critical for maintaining U.S. systems and attacking PLA systems.

Actions with Near-Term Effects.

- **Empower tactical-unit software development.** The services and CCMDs should empower tactical units to experiment with, develop, and deploy robust, reliable, and resilient software for select capabilities that they operate. This will allow the Future Joint Force to capitalize on the empowered tactical leaders and their experience in joint and combined arms warfare. Tactical units can also be expected to identify software-related problems that were not anticipated at the CCMD, service, or Department level, and that the enemy could have exploited in battle. It should be noted, however, that developing software that warfighters can responsibly use in operations requires deep expertise, for which there is not a substitute – and requisite investment in training, education, and partnership with industry and academia to develop it within the Force.
- **Streamline, scale, and accelerate the Authorization to Operate (ATO) Process.** ATOs are required to scale software solutions and integrate them into existing networks. They are necessary for maintaining the security of DoD systems, but represent one of the most significant bottlenecks in DoD's ability to rapidly develop and field warfighting software.[70] The length, costs, and complexity associated with the ATO process has hindered DoD's capacity to absorb innovation in real time, as well as made it difficult for less-resourced commercial providers to deliver software to warfighters. Without movement to help make the software authorization process easier, faster, and more efficient, DoD will not be able to adapt quickly enough to a changing technological environment, and warfighters will not be able to access the cutting-edge software that they need at the tactical edge. They will also struggle to transform into a software-centric organization.[71] DoD needs to streamline, scale, and accelerate the process. DoD should empower the Defense Information Security Agency with the authority to grant an ATO that can be immediately inherited by any agency that chooses to do so. DoD should also differentiate levels of ATO requirements, rather than continuing the current model of "setting the floor at the ceiling" for all software security. DoD

[70] SCSP interviews with service members and defense technologists (2022).

[71] Software Acquisition and Practices (SWAP) Main Report, U.S. Department of Defense (2019).

should also consider either internally developing or outsourcing a certified platform that would vet and clear software from a variety of sources.

Actions with Medium-Term Effects.

- **Complete a new information architecture.** A new information architecture would allow DoD to be far more flexible, scale on demand, and adapt dynamically to changing conditions. As recommended by the National Security Commission on Artificial Intelligence (NSCAI),[72] this would include (1) access to cloud computing and storage;[73] (2) a secure, federated system of data repositories with appropriate access controls; (3) a secure network with the bandwidth needed to support data transport; (4) common interfaces; (5) development environments; and (5) shared development resources that allow commands to quickly access the data, software, and models they need.[74] Such an architecture must be driven by use cases for the information – instances of the themes in previous sections around improving C2, common operating picture, agile use of automation – and aligned with a prioritized list of use cases.
- **Establish career fields for digital experts.** Digital talent already exists within the services but there are few mechanisms to identify and apply this talent to a military career that rewards, promotes, and retains service members for their technical skillset. The military services should create career fields for military personnel for software developers, data scientists, and AI engineers, with both management and specialist tracks.[75]

Equipment Should, by Design, Be Software-Defined, Updatable, Interoperable, Modular, and, Where Possible, Low-Cost

To create an effective Future Joint Force, as much equipment as possible should be software-defined, updatable, interoperable by design, and modular. Software-defined means that equipment is designed and procured with software as the core of capabilities, rather than basing the capabilities primarily or even exclusively around hardware. Software-defined systems need sufficient power, compute, and mechanical systems, but their performance envelope is defined by software more than hardware. For example, the performance of Tesla's software-defined vehicles is primarily shaped by the software that guides its systems.[76] Updatable means able to

[72] Final Report, National Security Commission on Artificial Intelligence at 59-69 (2021).

[73] Department of Defense Software Modernization Strategy, U.S. Department of Defense at ii (2022).

[74] U.S. Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway, U.S. Department of Defense (2022); Kathleen Hicks, Memorandum for Senior Pentagon Leaders on Implementing Responsible Artificial Intelligence in the Department of Defense, U.S. Department of Defense (2021); DoD Directive 3000.09, Autonomy in Weapon Systems, U.S. Department of Defense (2012).

[75] Final Report, National Security Commission on Artificial Intelligence at 372-375 (2021).

[76] Junko Yoshida, Software-Defined Vehicles. It's Elon's World. We Just Drive in It, AutoSens (2022).

quickly add to, adapt, or otherwise update the capabilities of weapon systems. This can range from adding an additional targeting sensor to a missile to updating software so that a communication system can bypass jamming, such as the upgrades that allowed Starlink to bypass Russian jamming efforts.[77] Interoperable by design means rather than patching together systems, the United States and its allies should further emphasize interoperability of communication systems, data sets, and processes.[78] This will require exercises that force the use of integrated rather than deconflicted information systems. And, finally, modular, as opposed to monolithic, means an architecture that has components whose functions do not directly depend on each other, but can communicate and interact. In general, modularity makes it easier to update old products by changing one component, create new products by combining modules, or improve an existing system by adding a new component.[79]

The result of designing new capabilities with all four traits would be a system that can easily adapt to unexpected challenges or opportunities, work with allied and partner systems or be employed by allies and partners, and would potentially be more cost-effective. This would strengthen power projection by expanding the number of allies that can effectively collaborate with U.S. forces. It would also increase unpredictability by accelerating adaptation and new capability development.

Actions with Near-Term Effects.

- **Develop and field a low-cost version of a Collaborative Combat Aircraft (CCA) at scale.** The CCA should follow the above principles to quickly develop and procure a low-cost version of a CCA in large numbers. Rather than relying on building exquisite capabilities from the start, the Joint Force should rely on software updates to strengthen its effectiveness, especially in sensing, advanced autonomy, electromagnetic spectrum operations, and cyber attacks. Doing so would showcase the potential of software-centric, updatable systems. It would also accelerate the delivery of a much-needed capability.
- **Transform legacy systems into AI platforms.** Converting legacy systems into autonomous or uncrewed systems would be helpful, but is very technically challenging, data-intensive, and is likely to take a significant amount of time. Instead, the services should convert legacy systems like trucks into platforms for hosting AI capabilities. The platform would provide energy, sensors, compute, and updatable software that allows for incremental improvements. As an example, the U.S. Army's Advanced Targeting and Lethality Aided System (ATLAS) partially automates target identification and engagement, helping operators "to engage three targets in the time it now takes to just engage one."[80] If aligned with the principles above, ATLAS and

[77] Valerie Insinna, SpaceX Beating Russian Jamming Attack was 'Eyewatering': DoD Official, Breaking Defense (2022).

[78] The Future of Conflict and the New Requirements of Defense, Special Competitive Studies Project at 32 (2022).

[79] Oleksandr Kruglyak, What is Modular Software Architecture, Triare (2023).

[80] Nathan Strout, How the Army Plans to Revolutionize Tanks with Artificial Intelligence, C4ISRNET (2020).

similar systems would be able to communicate with and contribute to the performance of other systems built onto armored vehicles and receive software updates that improve their performance. They would also have the potential to contribute to the virtuous cycles described in the data-informed decision-making section.

- **Equip units to adapt uncrewed systems using in-situ collected data.** Uncrewed systems need to be less predictable and more flexible, or they will struggle to compete against human adversaries. Today, the process to change AI-enabled systems requires collecting and transporting data, developing a new set of algorithms, and redeploying the software – a process that typically takes months or years. To enable units to adapt uncrewed systems, DoD can field high-fidelity simulations of AI systems at the tactical edge, create operator focused analysis tools to evaluate and deploy new tactics, and deploy synthetic imagery generation tools to adapt AI systems based on in-situ data. This technology is all already in production. Doing this would help build an appreciation for software-centric systems, and processes for adaptation in field environments.[81]

Actions with Medium-Term Effects.

- **Create a live, virtual, and dynamic test platform for AI-enabled systems that blends modeling and simulation, augmented reality, and cyber-physical system environments.**[82] A combination of a lack of data and poor data management challenge DoD's efforts to develop and regularly update AI-enabled systems. Rather than trying to collect data entirely from real-world environments, DoD should develop a platform that allows developers, both within DoD and contracted, to develop and train AI-enabled systems in a high-fidelity environment. Doing so would significantly decrease data collection requirements, and therefore accelerate the development and fielding of autonomy software.[83] This would increase the effectiveness of software-defined systems, and allow them to be updated more quickly.

Makes Data-Informed Decisions at Every Level and for Most Tasks

According to the National Security Commission on Artificial Intelligence (NSCAI), "Data-informed decision-making uses data to generate insights and act on them. Data-driven organizations often make decisions more quickly, at lower levels in the organization, and with a stronger empirical foundation than organizations that rely primarily on intuitive or experience-based decision-

[81] This recommendation is based on a discussion with industry experts on December 8, 2022.

[82] Final Report, National Security Commission on Artificial Intelligence at 386 (2021). For a commercial industry example of unprecedented use of a synthetic environment to virtually 'build' and evaluate an entire automobile factory and production line two years before physical production begins, see BMW Group at NVIDIA GTC: Virtual Production Under way in Future Plan Debrecen, BMW Group (2023).

[83] This recommendation is based on confidential discussions with industry experts (2022-2023).

making."[84] Many of the most competitive companies in the technology sector are defined by data-driven cultures. Not only do these companies amass and organize data, and employ algorithms to analyze and act on their data, they are structured and organized to "live, breathe, and act" according to data.[85]

For the military, a culture and structure of data-informed decision-making would have several advantages. A stronger empirical base would enable better personnel decisions, training assessments, prediction of maintenance and supply requirements, and many other administrative, training, and logistical requirements. For operations, a data-informed approach would add more rigor to the operational research and systems analysis approach needed to most effectively shift risk from humans to machines. It would also enable individual nodes on a network-based force by empowering junior leaders to make more tactical decisions based on data, and require less intuition honed by experience.

To establish a culture of data-informed decision-making, DoD would need engineers to procure, build, and manage the necessary infrastructure and software; senior leaders to guide the transformation of business processes and to manage personnel; and end users informed about how to collect, manage, and use data to make decisions every day. It is especially important for business processes to change to produce virtuous cycles, in which data generated from multiple sources is used to refine algorithms and make predictions. The predictions drive outcomes. Data from the outcomes is then used to further refine algorithms and make better predictions.[86] Engineers must constantly push to design or automate processes in a way that contributes to virtuous cycles, and senior leaders must incentivize their use.

Actions with Near-Term Effects.

- **Make commercial decision-making tools available to military units.** Data-informed decision-making software and dashboards are common in much of industry, but are often not accessible on DoD systems. Units should have access to an approved list of data-informed decision-making tools that can help improve decision-making, begin building a data culture, and initiate a virtuous cycle.
- **Require local-level data collection and management, guided by common standards.** DoD and military services have common standards and requirements for many maintenance, administrative, and training tasks. They should have the same requirements for data collection and management for an initial list of data sets that have been identified as most useful.

[84] Final Report, National Security Commission on Artificial Intelligence at 297 (2021).

[85] Becky Frankiewicz & Tomas Chamorro-Premuzic, Digital Transformation Is About Talent, Not Technology, Harvard Business Review (2020).

[86] Marco Iansiti & Karimi R. Lakhani, Competing in the Age of AI, Harvard Business Review Press at 53 (2020).

- **Integrate computational thinking into entry-level training and continuing education requirements.** This should be a requirement for both commissioned officers and enlisted personnel, as well as civilians, and would include lessons in problem curation, data collection and management, the AI stack, probabilistic reasoning and data visualization, and data-informed decision-making.[87] Such a curriculum would help military personnel collect and operationalize data and fight more effectively against adversaries doing the same. Notably, multiple courses for each lesson are commercially available.

Actions with Medium-Term Effects.

- **Build Department-wide data architecture.** As described by NSCAI, a DoD-wide data architecture would need to be "composed of a secure, federated system of distributed repositories linked by a data catalog and appropriate access controls that facilitates finding, accessing, and moving desired data across DoD."[88] Such an architecture would "facilitate finding, accessing, and moving desired data across the Department including data sets, associated data models, and trained AI models along with supporting documentation."[89]

Prioritizes Payloads (Including Sensors, Munitions, Networks, and Others) Over Platforms

A conflict with a peer competitor will test the inventory and industrial depth of the United States and its allies, and their ability to adapt limited weapons systems and platforms to regenerate capability and fulfill a diverse set of missions in a grinding contest. Because of extremely lengthy development and production timelines of major platforms, DoD will be unable to field new platforms in significant numbers quickly. For that reason, the near-term deterrence credibility challenge is more effectively addressed with an emphasis on fielding more advanced payloads to equip existing platforms. To meet capacity and capability needs in a war of attrition against a great power, the United States and its allies need to prioritize payloads over platforms while evolving both to enhance Joint Force operations. Effectively matching platforms to missions in the future requires integrating capabilities into the payload rather than the platform itself.

DoD needs to build modular and interchangeable payloads that are hosted on platforms optimized to deliver a range of standardized packages – including sensors, networks, and weapons. These platforms need to be purposefully designed to plug in and swap out generations of payloads over time to deploy new capabilities at speed, scale, and cost. Where possible, low-cost payloads should be selected to allow the Joint Force to field attritable systems, and to produce and replenish inventory with high volumes of payloads. It should be noted that this moves

[87] Final Report, National Security Commission on Artificial Intelligence at 297 (2021).

[88] Final Report, National Security Commission on Artificial Intelligence at 63 (2021).

[89] Final Report, National Security Commission on Artificial Intelligence at 293 (2021).

beyond munitions, which have some platform limitations. Payloads also include electronic warfare, communication, sensing and cyber systems.

By prioritizing payloads, the United States and its allies can expand each platform's multi-mission utility and adaptability, strengthening power projection and imposing additional uncertainty on the PLA. The incorporation of autonomy into payload capabilities over time will also provide the Joint Force with more options to reach and threaten adversaries' assets while reducing risk to its own assets and platforms.

Actions with Near-Term Effects.

- **Standardize platform-to-payload interfaces for multi-mission.** Platforms need to eventually be designed to seamlessly integrate many generations and types of payloads over their lifecycle to deliver lethal capability across multiple missions at effective cost.[90] DoD needs to first standardize the payload-to-platform interface to achieve a modular open system architecture for rapidly reconfiguring and swapping modified and new payloads from mission to mission. This includes making military payloads – including those of allies – compatible with commercial platforms and systems.
- **Swap out platforms.** A combination of expanding mission requirements and limited industrial production capacity, especially in crisis, requires novel approaches to rapidly distributing and optimizing payloads across existing and future platforms. DARPA's System of Systems Integration Technology and Experimentation (SoSITE) is one such concept for combining aircraft, weapons, sensors, and mission systems to distribute and integrate capabilities across many interoperable crewed and uncrewed platforms faster than the PLA can counter them.[91] Until platforms purpose-built or re-designed to host a range of payloads can be deployed at scale, the U.S. military and its allies need to develop similar system-of-systems architectures for swapping out platforms – particularly those that are low-cost and attritable – from among heterogeneous mixes of systems to reliably deliver effects even when certain platforms are lost.

Actions with Medium-Term Effects.

- **Develop self-contained, platform-agnostic payloads.** DoD needs to design and scale self-contained payloads capable of easily attaching to different platforms without relying on interfacing platform specific capabilities. These payloads will need to be capable of seamlessly integrating into higher-level networks to deliver both kinetic and non-kinetic effects and act in concert with platforms across multiple domains.

[90] Naval Aviation Vision 2014-2025, Naval Aviation Enterprise at 7 (2015).

[91] System of Systems (SoS) Integration Technology and Experimentation (SoSITE), U.S. Department of Defense (last accessed 2023).

Achieves Information Advantage

A conflict between the United States and PRC will be the greatest information war in history. To outcompete the PRC in conditions with high information velocity, variety, and volume – often conflicting and ambiguous – the Future Joint Force must achieve information advantage in highly contested environments through offensive and defensive information operations, including but not limited to electromagnetic spectrum (EMS), cyber, influence, and psychological operations.

Information advantage is the ability to understand, shape, and leverage – both overtly and covertly, using both unclassified and classified information – the information and narrative environment faster and more accurately than our rivals. It involves the use of information effects to achieve a more complete operational picture to gain decision advantage over the PLA while shaping friendly, neutral, and enemy perception, cognition, and behaviors to achieve tactical, operational, and strategic advantage. Through information advantage, the United States and allies can call into question PLA concepts and capabilities, particularly system destruction warfare, which heavily relies on the quality and speed of information flowing through AI systems, and increase the unpredictability that the PLA and CCP must account for.

It is important to emphasize the central role AI-driven decision-making has taken in the PLA's vision of future warfare. The Future Joint Force can exploit the PLA's dependency on AI to undermine its overall confidence in its systems and threaten the PLA's performance at the strategic and operational levels.[92] This requires the ability to manipulate data and outputs of the PLA's AI-enabled systems, inject mistrust between the PLA's forces and their machines and distrust between PLA forces and political leaders, and degrade the performance of AI-enabled and autonomous systems – or destroy them entirely through kinetic and non-kinetic means.[93] Offensive operations will also need to be accompanied by defensive preparations, preferably with AI-enabled capabilities, to detect and defend against operations that flood U.S. society with misinformation, disinformation, or malinformation, or undermine U.S. C3 systems.

The United States and its allies should generate negative feed-forward and feedback closed loops to create disorientation, disorder, chaos, and mental paralysis in PLA forces. Simultaneously, the United States and its allies should protect their forces from the same effects.[94] Doing so would increase the uncertainty the PLA must account for, invalidate its investments, and force it to direct energy from offensive operations.

---

[92] Chris Bassler & Benjamin Noon, China's Ambitions for AI-Driven Future Warfare, Center for Strategic and Budgetary Assessments (2022).

[93] Counter Autonomy: Executive Summary, U.S. Department of Defense, Defense Science Board at 3 (2020).

[94] For a detailed examination of the OODA Loop as it pertains to AI-enabled command and control, see James Johnson, Automating the OODA Loop in the Age of AI, Defence Studies (2022).

Actions with Near-Term Effects.

- **Employ AI-enabled tools for automatic censorship evasion.** Authoritarian regimes, which rely on information control rather than buy-in to maintain domestic stability, are particularly vulnerable to operations that allow their populations to bypass censorship systems and access information beyond state propaganda. The U.S. government needs to use AI-enabled tools – to include generative AI – to exploit gaps in censors' logic and automatically evolve algorithms to rapidly identify multiple evasion strategies.[95] Alternative forms of communication, such as offline communication networking applications, would further help bypass censorship rather than only challenging it.
- **Work with Taiwanese and other allied military and intelligence agencies to aggressively counter disinformation on Western and allied social media platforms.** The PRC heavily relies on content farms and social media to distribute misinformation to influence foreign audiences. These information operations can include election interference to positive narrative curation and messaging about the PRC regime's activities, which can have military repercussions in a potential conflict with the PRC.[96] The U.S. military and intelligence agencies should immediately work with Taiwanese and other allied counterparts to develop coalition capabilities to aggressively counter disinformation on Western, Taiwanese, and other allied media. This should include developing defenses against the inevitable use of generative AI against the U.S. and its allies and partners.
- **Generate access to take-over adversaries' AI-enabled systems.** In the near term, the focus of U.S. counter-autonomy efforts could include identifying means and generating access to take over the PLA's AI-enabled systems to extend our sensing deep inside their territory and within their decision-making.

Actions with Medium-Term Effects.

- **Expand DoD investment in counter-AI and counter-autonomy capabilities.** The Future Joint Force will require novel AI techniques and tools to counter existing and future advanced adversarial AI systems in all phases of combat, but there is a marked lack of DoD counter-autonomy programs currently in existence.[97] DoD must proactively invest in counter-AI and counter-autonomy capabilities, such as adversarial machine learning (ML) techniques, to find and exploit weaknesses in Chinese AI models and systems in a potential conflict.[98] DoD should establish an office to integrate and direct military counter-autonomy efforts and funding across DoD in close collaboration with the private sector.

[95] See, e.g., Geneva: Evolving Censorship Evasion, censorship.ai (2022).

[96] Ben Sando, Taiwan Local Elections Are Where China's Disinformation Strategies Begin, Council on Foreign Relations (2022).

[97] Counter Autonomy: Executive Summary, U.S. Department of Defense, Defense Science Board (2020).

[98] Alex Stephenson & Ryan Fedasiuk, How AI Would – and Wouldn't – Factor into a U.S.-Chinese War, War on the Rocks (2022).

Maneuvers in the Electromagnetic Spectrum (EMS)

As part of achieving information advantage, the Future Joint Force must be able to effectively maneuver in an increasingly congested, contested, and constrained EMS in response to adversary counter-EMS capabilities. After years of underinvestment and operating in highly permissive environments, Joint Force EMS capabilities have dramatically declined. At the same time, our adversaries have invested heavily in EMS concepts and capabilities to disrupt kill chains and to detect low-observable U.S. fighters and bombers.[99] The Russians have effectively employed electronic warfare capabilities in Ukraine, particularly against Ukraine's air defense system, as an effective countermeasure to UAVs, and to degrade Ukrainian precision munitions.[100] For their part, the PLA has long treated the EMS as a core component of information advantage,[101] an offensive maneuver space to attack U.S. communications, datalinks, and decision cycles, and a complement to A2/AD capabilities meant to keep U.S. forces at distance.[102] The creation of the PLA Strategic Support Force is in part meant to institutionalize what the PLA sees as an asymmetric advantage in their concept of "networked electromagnetic spectrum warfare" or "integrated network and electronic warfare" for system destruction warfare.[103] As Air Force Gen. Mark Kelly, head of Air Combat Command (ACC), recently said: "If we lose the war on the electromagnetic spectrum, we're going to lose the war and lose it quickly."[104]

Electromagnetic warfare is a very dynamic and fluid form of warfare that requires constant and rapid adaptation to adversary countermeasures; so much so, that the Joint Force will have to rely on AI-enabled capabilities to adapt continuously to the evolving EMS environment. Electromagnetic spectrum maneuver will require the Joint Force to effectively control and manipulate the EMS environment to degrade adversary use of the spectrum while coordinating access and use by friendly forces, even in highly contested conditions. This will involve degrading adversary ability to develop a common operating picture and to effectively command and control their forces while simultaneously providing friendly forces the ability to communicate with each other, and locate and target adversary forces, assets, and frequencies used for communications and radar.

The Joint Force must be prepared to continually fight for advantage in the EMS domain and be able to exploit fleeting windows of opportunity. By developing countermeasures capable of out-

[99] John Christianson, Fighting and Winning in the Electromagnetic Spectrum, War on the Rocks (2022).

[100] Mykhaylo Zabrodskyi, et al., Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February-July 2022, Royal United Services Institute (2022).

[101] Joe McReynolds, China's Evolving Military Strategy, The Jamestown Foundation at 63-77 (2016).

[102] John Christianson, Fighting and Winning in the Electromagnetic Spectrum, War on the Rocks (2022).

[103] Marcus Clay, To Rule the Invisible Battlefield: the Electromagnetic Spectrum and Chinese Military Power, War on the Rocks (2021).

[104] Joseph Trevithick, Big Emphasis On "Spectral Warfare" In Air Force's Next Generation Air Dominance Plans, The War Zone (2023).

adapting and defeating increasingly intelligent adversarial sensors and measures that change frequencies, waveforms, and passive/active modes to avoid detection, the United States and allies would be able to undermine the PLA's investment in electromagnetic warfare, impose dilemmas, and inject uncertainty into the reliability of their A2/AD. The United States and allies can further enhance these objectives by developing systems to avoid detection and attacks themselves while penetrating enemy A2/AD and generating effects over wider frequency ranges.[105] As the war in Ukraine has demonstrated, survival on the battlefield will require effective employment of electromagnetic spectrum operations at both operational and tactical levels.

Actions with Near-Term Effects.

- **Deconflict military and commercial use of critical frequency bands.** For many years, DoD and major telecommunications companies have competed over access to critical spectrum bands. The emergence of 5G wireless phone and internet technologies, in particular, poses growing challenges to DoD's access to parts of the S-band used primarily for military ground, air, and sea-based radars at the center of ballistic missile defense – particularly the Aegis Combat System, which is one of the few systems capable of tracking hypersonic missiles.[106] The U.S. government must prioritize improving coordination between government and industry to deconflict the use of the EMS spectrum needed to sustain and expand critical military function, without hindering the rollout of 5G and next-generation network capabilities.
- **Implement DoD EMS Superiority Strategy 2020 by 2025.** In 2020, DoD released the EMS Superiority Strategy, which outlined strategic goals for achieving freedom of action in the EMS, including evolving to an agile and fully integrated EMS infrastructure and pursuing total force EMS readiness.[107] However, implementation has been slow with efforts ongoing in 2023 to develop a strategic EMS roadmap.[108] The U.S. military must achieve implementation of the strategy by 2025 to train and equip warfighters with the capabilities and operating concepts to fight offensively in a highly contested EMS environment against the PLA. DoD needs to particularly focus on the adoption of AI for data validation, modeling, and simulation of EMS operations. DoD also needs to lead the development of a standard international spectrum architecture for joint and coalition interoperability and information-sharing. Implementation of the strategy must be done in close partnership with allies from the beginning to reinforce interoperability and capabilities development across the alliance.

---

[105] Bryan Clark & Mark Gunzinger, Winning the Airwaves: Regaining America's Dominance in the Electromagnetic Spectrum, Center for Strategic and Budgetary Assessments at 24 (2017).

[106] Theresa Hitchens, STRATCOM Wrapping Spectrum Ops Center Plan, As Military Faces Bandwidth Grab by 5G Firms, Breaking Defense (2023).

[107] Electromagnetic Spectrum Superiority Strategy, U.S. Department of Defense (2020).

[108] Next-Generation Electromagnetic Spectrum Strategic Roadmap, SAM.gov (2023).

- **Integrate signals from spatially distributed EMS platforms.** Integrating sensor information from spatially distributed EMS platforms across multiple domains will enable the Joint Force to rapidly resolve ambiguities in signals and develop a superior understanding of the EMS environment. DoD also needs to use these distributed EMS systems offensively to dilute the PLA's own understanding of the real environment and degrade or delay their operational decision-making.

Actions with Medium-Term Effects.

- **Employ AI/ML to accurately visualize the EMS operating environment (EMOE).** In a contested or congested EMOE, the ability to accurately visualize signatures and distinguish unintentional EMS fratricide by friendly forces from intentional interference by the PLA is low. DoD needs to employ AI/ML systems capable of autonomously sensing, inter-communicating, and visualizing the complex EMOE to allow the Joint Force to adapt systems to adversarial interference, and enable optimal decision-making in a disrupted EMS environment.[109]
- **Actively deceive PLA sensors to undermine trust.** The Joint Force today needs to focus on reducing signatures and/or raising the ambient noise across the EMS – particularly the electro-optical and infrared – to penetrate denied areas. In the future, the Joint Force will need to develop more sophisticated countermeasures for characterizing, adapting to, and creating effects that actively deceive sensors and degrade overall trust and safety of adversaries' systems, rather than destroying or avoiding detection by sensors.[110]

Effective Leadership in a Technology-Driven Environment

The Future Joint Force requires leadership that can bring all national and international levers of power to bear on a common strategic purpose and prepare the next generation of allied warfighters for a future of persistent conflict characterized by advanced and emerging technologies and new operational concepts amid intensifying geopolitical rivalries. At the strategic level, it entails fundamental changes to how the U.S. military operates.

To achieve business transformation, senior military leadership must first articulate and instill strategic purpose behind rapid change and clarify the connection between strategic and operational levels of war to achieve national objectives. Otherwise, no amount of technological advantage will result in success.[111] Leaders must also deeply understand the human and political dimensions of conflict. As the war in Ukraine has shown, an effective narrative is key to instilling

[109] Matthew J. Florenzen, et al., Unmasking the Spectrum with Artificial Intelligence, National Defense University Press (2019).

[110] Bryan Clark & Mark Gunzinger, Winning the Airwaves: Regaining America's Dominance in the Electromagnetic Spectrum, Center for Strategic and Budgetary Assessments at 17-18 (2017).

[111] The U.S. military had an unusually strong military-technological advantage in both Afghanistan and Iraq, but struggled to accomplish its policy objectives.

purpose and rapidly mobilizing and employing national and international resources – human and material – in innovative ways.[112] With growing connectivity and means of capturing, sharing, and shaping the information landscape, narrative shaping "to create psychological effects may be the sine qua non of future strategic leadership" that our leadership must master.[113]

Good leadership also nurtures innovation, especially nonlinear, self-reinforcing transformation that would allow the Future Joint Force to continuously out-learn and out-innovate adversaries. United States and allies' political and military leadership must create a virtuous cycle of research and development in alignment with defense requirements and reinvest into military innovation to deliver new capabilities faster than adversaries can learn and adapt. This involves integrating a larger coalition of society and industry, allies, and partners into capability and capacity-building efforts. Over time, the tech stack will grow tighter and create a virtuous feedback cycle the United States and its allies can use to achieve decision-advantage[114] and apply transformational technologies ahead of adversaries. At the same time, military leadership must transform the business models and processes themselves to enable and incentivize the use of data-informed decision-making and AI/ML at scale to improve the ability of the Future Joint Force to rapidly communicate, iterate, and actually field new capabilities.

At the operational level, the United States and allies need to enhance the capacity of warfighters to conceive new and effective operational concepts for advanced and emerging technologies, anticipate and rapidly out-innovate measures and countermeasures of adversaries who have studied our methods, and use technologies to achieve joint effects.[115] Leaders must also transform business models and processes to enable and incentivize the use of data-informed decision-making and AI/ML at scale.

Empowerment is a constant theme in this report, not only in terms of how the United States can use its advantages to enhance the Future Joint Force, but also how it can provide an asymmetric advantage against the more structured and hierarchical approach expected from PLA forces. It does require a level of risk acceptance that is likely to generate discomfort at times for some elements of the U.S. chain of command. The United States needs technologically literate leaders who understand risk analysis and risk management in ways that allow them to empower subordinates as much as possible, including during experimentation and testing, not just in operational environments.

---

[112] James Farwell, How Zelensky Seized Control Over the Narrative in Ukraine, The Defense Post (2022).

[113] Steven Metz, The Future of Strategic Leadership, The US Army War College Quarterly: Parameters at 63 (2020).

[114] C. Todd Lopez, Leadership Key to Moving Defense Department Toward Data-Driven Future, U.S. Department of Defense (2022) (quoting Deputy Secretary of Defense Kathleen Hicks).

[115] For a PLA view of the importance of the cognitive dimension of the future fight, see e.g., Megha Pardi, Guard against the "White Elephant Effect", Cognitive Battle in the "Post-Truth Era", Cloud Training, China Tech Dispatch (2022).

Lastly, jointness must be built-in from the very beginning of education, planning, and concept development rather than bolted on. Allied forces must develop not only new joint operational concepts but new ways of developing these concepts, and foster a competition of ideas across services, functions, and combatant commands.[116] Allied forces must also develop incentives and institutional processes for empowering subordinates, managing risks, and involving more stakeholders – including the combatant commands and industry experts – early in the development process, generate feedback, and incorporate joint concepts into training and experimentation with new technologies.[117] DoD should also put in place a support architecture to generate and test ideas during crises and conflict, capture operational lessons rapidly, and absorb those lessons across the Department as quickly as possible.

Actions with Near-Term Effects.

- **Require a senior leader emerging technology course.** Today's O-7s and above are proficient in the tasks they have been required to perform or learn about. However, they have not been required to learn enough about emerging technologies and their influence on geopolitics, the character of warfare, and how to lead their organizations through integrating the technologies that are needed to win peacetime competitions, and to deter, and if necessary, win wars. The current education requirements for senior leaders include CAPSTONE and Pinnacle, and courses for O-7 through O-9s that teach general and flag officers effective joint and combined operations and corporate management of their services.[118] There is no comparable mandated course on emerging technology for O-7s or SES.

  DoD should require O-7s through O-9s to take a one to two-week course on the impact of emerging technologies on geopolitics, conflict, and military-relevant economics, and include sections on how senior leaders should guide their organizations through transforming their infrastructure, business processes, personnel systems, and capabilities to capitalize on emerging technologies, and the employment of emerging technologies during war. The initial set of emerging technologies should include advanced computing, software and artificial intelligence, networks, energy generation and storage, biotechnology, and some military specific technologies, such as directed energy. The list of emerging technologies and instruction provided about them should be updated annually.

Actions with Medium-Term Effects.

- **Create an emerging and disruptive technology qualification process and coded billets.** DoD already designates that certain critical billets must be filled by Joint Qualified Officers and different levels of joint qualification. To follow this model for emerging and disruptive

[116] Paul Benfield & Greg Grant, Improving Joint Operational Concept Development within the U.S. Department of Defense, Center for a New American Security at 4 (2021).

[117] Implementing Joint Force Development and Design, U.S. Joint Chiefs of Staff at B2-B3 (2022).

[118] Joint Warfighter Development Program, Naval Postgraduate School (last accessed 2023).

technologies, the military services should create emerging and disruptive technology designated billets for officers that require an emerging and disruptive technology qualification prior to assignment. They should also create a process for military leaders to become emerging and disruptive technology qualified. Emerging and disruptive technology qualified officers would add value in a number of areas for the services, including: (1) assisting with acquisition of emerging technology; (2) helping integrate technology into field units; (3) developing organizational and operational concepts; and (4) developing training and education plans.[119]

[119] Final Report, National Security Commission on Artificial Intelligence at 300 (2021).

Characteristics of the Future Joint Force

Characteristics	Actions with Near-Term Effects	Actions with Medium-Term Effects
Operates as a Distributed, Networked-Based Organization	• Stand up joint tactical units that are organically equipped to conduct distributed, multi-domain operations • Incorporate network-based decision-making into training exercises • Ensure distributed units have access to all-source intelligence and AI-enabled analytic and decision aids	• Ensure distributed units are trained and equipped to employ counter-AI strategies to evade, overtake, or destroy PLA sensors
Functions as a Human-Machine Team, Both as a Whole and as Individual Nodes on the Network-Based Force	• Develop novel warfighting concepts • Develop decision aids for operational units, both centrally and by incentivizing unit-level development and use • Develop and field more effective interfaces • Train for HMC and HMT at Combatant Commands (CCMDs), major training centers, and regular unit training • Implement an HMC and HMT readiness scorecard • Compete traditional platforms against new, uncrewed systems • Allow combatant commands to reinvest HMC and HMT driven savings	• Integrate HMC and HMT lessons into entry-level training and continuing education requirements • Assess and change forces structure based on HMC and HMT experimentation and novel warfighting concepts
Gains & Maintains Software Advantage	• Empower tactical-unit software development • Streamline, scale, and accelerate the Authorization to Operate (ATO) Process	• Complete a new information architecture • Develop career fields for digital experts
Equipment Should, by Design, Be Software-Defined, Updatable, Interoperable, Modular, and, Where Possible, Low-Cost	• Develop and field a low-cost version of a Collaborative Combat Aircraft (CCA) at scale • Transform legacy systems into AI platforms • Equip units to adapt uncrewed systems using in-situ collected data	• Create a live, virtual, and dynamic test platform for AI-enabled systems that blends modeling and simulation, augmented reality, and cyber physical system environments
Makes Data-Informed Decisions at Every Level, and for Most Tasks	• Make commercial data-informed decision-making tools available to military units • Require local-level data collection and management, guided by common standards • Integrate computational thinking into entry-level training and continuing education requirements	• Build Department-wide data architecture
Prioritizes Payloads Over Platforms (Including Sensors, Munitions, Networks, and Others)	• Standardize platform-to-payload interfaces for multi-mission • Swap out platforms	• Develop self-contained, platform-agnostic payloads
Achieves Information Advantage	• Employ AI-enabled tools for automatic censorship evasion • Work with Taiwanese and other allied military and intelligence agencies to aggressively counter disinformation on Western and allied social media platforms • Generate access to take-over adversaries' AI-enabled systems	• Expand DoD investment in counter-AI and counter-autonomy capabilities
Maneuvers in the Electromagnetic Spectrum (EMS)	• Deconflict military and commercial use of critical frequency bands • Implement the DoD EMS Superiority Strategy 2020 by 2025 • Integrate signals from spatially distributed EMS platforms	• Employ AI/ML to accurately visualize the EMS operating environment (EMOE) • Actively deceive adversarial sensors to undermine trust
Effective Leadership in a Technology-Driven Environment	• Require a senior leader emerging technology course	• Create an emerging and disruptive technology qualification process and coded billets

PART SIX

Call to Action

The character of warfare and the international security environment are changing, and the stakes for the United States could not be higher. In the first Defense Interim Panel Report (IPR), we noted that by the end of this decade, the United States will likely face a new kind of warfare. The convergence of emerging and advanced technologies with innovative operational concepts that employ them are creating new ways to employ force. The tragic war of Russian aggression in Ukraine illustrates that daily.

The People's Republic of China (PRC) continues to amass the capacity to reshape the international order. It already has the intent. A core component of this capacity are its focused efforts to integrate by 2027 mechanization, informatization, and intelligentization of its armed forces, putting itself in a position to reunify Taiwan by force, if necessary, and setting the stage to elevate the PRC to a position of strength, prosperity, and leadership on the world stage.[120]

The United States has overcome challenges by ambitious rivals before. During the Cold War, the United States was determined to deter the Soviet Union from invading Europe, starting a nuclear war, and ruling the world. At the outset of the Cold War, the Soviet Union had far more conventional military power in Europe than the allies. The United States responded with the First Offset Strategy. The U.S. military created systems and trained personnel to keep bomber aircraft in the air at all times, empowered junior officers to man nuclear silos, and developed capabilities to stand watch on land, at sea, and below its surface.

While the United States focused on the war in Vietnam, the Soviet Union reached nuclear parity, and built a three to one conventional advantage over North Atlantic Treaty Organization (NATO) forces in Europe.[121] Rather than responding with inertia or paralysis, the U.S. military invested in the technologies, concepts, and training that led to the Second Offset Strategy.[122] By the mid-1980s, the Soviet Union realized the Second Offset left it without a viable route to military victory in Europe.[123] While many factors contributed to the end of the Cold War, the Second Offset successfully deterred the Soviet Union from attacking a NATO member state until the Cold War

[120] Military and Security Developments Involving the People's Republic of China, U.S. Department of Defense (2022).

[121] Rebecca Grant, The Second Offset, Air and Space Forces Magazine (2016).

[122] Robert R. Tomes, US Defense Strategy from Vietnam to Operation Iraqi Freedom: Military Innovation and the New American Way of War, 1973- 2003, Routledge (2007).

[123] Rebecca Grant, The Second Offset, Air and Space Forces Magazine (2016).

ended.[124] The Soviets were right to fear America's conventional capabilities of stealth and precision-guided munitions regime. It was put on display in 1991 when the U.S. military, with support from coalition partners, quickly ejected the Iraqi army from Kuwait and crippled its ability to threaten regional security.

Today, there is a growing realization that the PRC is the challenge of our lifetimes. Yet, the magnitude and pace of our actions are still not reflective of the urgency of the matter. A lack of wealth or power, and competing priorities are not the issue. The United States is far wealthier and more powerful than it was during the Cold War. Blame is often placed on the acquisition system. There is some truth to that argument. The acquisition system is sluggish, poorly suited for software, and plagued by a host of other problems. However, when priorities are clearly articulated and there is accountability for delivering results, the American system can produce remarkable results, remarkably quickly. But we are not there yet. We are not yet approaching the challenge with the all-out-dedication that it requires.

If the United States does not rise to the challenge, the consequences could be dire. Most Americans alive today have only known a world in which the U.S. military is dominant. For generations, it has been capable of both protecting our homeland against invasion and underwriting an international order that has fostered peace and prosperity on a scale that humanity had never before experienced. Our military primacy allowed us to shape the global economy, unlocking trillions of dollars for U.S. companies and citizens, and secure the free flow of commerce that enabled supply chains to function and globalization to flourish. It also allowed us to establish the international data network that powers the digital economy and international communication. Most important, our military primacy has helped protect democracy worldwide against challenges from authoritarianism. Losing our military edge could threaten these gains and trigger irreversible consequences. This is not about the anxiety of no longer being the dominant power in the world; it is about the risks of living in a world in which the Chinese Communist Party becomes the dominant power.

This report is an effort to map a path towards a Joint Force that can deter war – and if necessary, win. Our initial report on Offset-X was about the why and the what. This more detailed report now provides the how. Specifically, how does the U.S. military remain the most lethal and innovative fighting force the world has ever known. If DoD, the services, and Congress combine their efforts, the United States will be techno-militarily superior.

[124] Shawn Brimley, Offset Strategies & Warfighting Regimes, *War on the Rocks (*2014).

ANNEX A

Capabilities and Technology-Based Solutions

Part 5 of this report outlines capabilities that will help invalidate the PLA's investments, increase their uncertainty, shift risk from humans to machines, and strengthen U.S. power projection. It is far easier to propose capabilities than to understand how to develop them. For the next step in that direction, this Annex contains a selection of technology-based solutions for the proposed capabilities.

Command and Control (C2)

Capabilities Needed. The U.S. military, its allies, and partners need a new C2 design and architecture that will enable them to be far more tactically flexible, be interchangeable with allies, scale on demand, and adapt dynamically to changing conditions.[125] To meet mission requirements for C2 in the Indo-Pacific, the U.S. military needs a combination of resilient communications; an accurate and continuously-updated all-domain operational picture; to generate and assess feasible and creative courses of action faster than its adversaries; and more network-based decision-making.

- **Resilient communications.** In line with system destruction warfare, the PLA intends to use cyber attacks, electronic warfare, and kinetic attacks on C2 infrastructure to degrade and destroy U.S. and allied communication networks.[126] U.S. and allied forces need to communicate between and within joint and combined formations, and connect sensors to decision-makers and shooters, all while undergoing attacks that are likely to achieve at least a degree of success. This requires an architecture for integrated and resilient communications for all U.S. and allied forces. It also requires the U.S. military to focus on software advantage so that it can deploy, employ, and update software, including AI models that help it predict, defend against, and recover from attacks.[127]

[125] Nand Mulchandani & John N.T. Shanahan, Software-Defined Warfare: Architecting the DoD's Transition to the Digital Age, Center for Strategic and International Studies (2022).

[126] Jeffery Engstrom, System Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare, RAND Corporation at 15-17 (2018).

[127] The Future of Conflict and the New Requirements of Defense, Special Competitive Studies Project at 27 (2022).

- **Common all-domain operational picture (COP).** For effective C2, the military needs to fuse operational, logistical, and intelligence information into a tailorable, real-time COP.[128] While a COP is a long-standing requirement, the military increasingly needs to fuse large volumes of information, coming from disparate sources including allies, from all domains, at all classification levels including open-source information, through pipelines with limited bandwidth,[129] all of which are subject to adversary attack and influence and deception operations.[130]
- **Course of action generation and analysis.** Presenting dilemmas at a rate that overwhelms the PLA or limits their decision space requires generating feasible courses of action quickly and creatively.
- **Greater network-based decision-making.** One method for building resilient command and control while networks are under attack is to shift from hierarchy-based decision-making processes to more network-based decision-making processes, in line with Offset-X's recommendation to fully embrace distributed, network-based operations.[131] Hierarchy-based processes are characterized by top-down decisions, vertical information flows, and clear tiers of authority within an organization.[132] Hierarchies typically have an advantage when exacting standards are necessary, or for the coordination of large, tightly-coupled groups for complex tasks. They are less well-suited for environments that require rapid change, or when communication along the hierarchy is likely to break down. Network-based processes are characterized by distributed and localized decision-making and resources, and create effects cumulatively. On average, they are more adaptive and more resilient, and perform well when nodes are empowered, able to communicate laterally.[133] Militaries operate on a spectrum of hierarchy to network-based decision-making, and need to be able to move along the spectrum as needed.

Technology-Based Solutions.

- **Adaptive communication systems** have the potential to contribute to resilient communications, and to help enable distributed, network-based operations. They use a decision-making algorithm to "overcome obstacles, respond to and learn from its environment, and achieve beneficial goals to the completion of its primary mission with minimal to no human interaction" by shifting which part of the network it relies on.[134] As an example, a drone employing adaptive communications that was transmitting and receiving

[128] Joint Publication 3-0: Joint Operations, Joint Chiefs of Staff at GL-8 (2018).

[129] Department of Defense Outside the Continental United States (OCONUS) Cloud Strategy, U.S. Department of Defense at 2 (2021).

[130] Koichiro Takagi, The Future of China's Cognitive Warfare: Lessons from the War in Ukraine, War on the Rocks (2022).

[131] The Future of Conflict and the New Requirements of Defense, Special Competitive Studies Project at 22 (2022).

[132] John P. Ketter, Hierarchy and Network: Two Structures, One Organization, Harvard Business Review (2011).

[133] Azeem Azhar, The Russian vs. the Ukrainian Network, Exponential View (2022).

[134] Cognitive Communications, U.S National Aeronautics and Space Administration (last accessed 2023).

data from a satellite, when jammed, would autonomously shift to the next most optimal node on the network, whether that's another satellite, a ship, or other drone. One form of adaptive communications, National Aeronautical and Space Administration (NASA)'s cognitive communications program, includes: 1) cognitive links for point-to-point connections, 2) cognitive networks for routing information, 3) cognitive systems that affect how devices interact with each other and with infrastructure, and 4) enabling technology.[135] Other organizations, such as Johns Hopkins University Applied Physics Laboratory and private sector companies are also developing adaptive communication systems.[136]

- **Modular C2** "can be scaled up or down depending on capacity demands and tailored at the sub-component level depending on operational need" for rapid decision-making and response, and would enhance small units' ability to participate in distributed operations.[137] Modular C2 system consists of tailorable modules capable of providing a comprehensive operational picture of the joint all-domain environment from a single laptop, which can have a suite of systems for supporting theater-level area of responsibility. The system is also based on an open, vendor-agnostic approach for hosting newer tracking equipment and components as needed by the Services.[138]
- **Human-machine collaboration enabled planning tools** can process vast amounts and types of data, aggregate and turn it into useful information, and prioritize it for decision-making. AI-enabled machines can identify novel patterns that humans have not, and in many cases, cannot identify. Tapping into human-machine capabilities would improve situational awareness and empower a planning process that is faster, more creative, able to generate more options, and is better suited to creating a plan optimized for a specific challenge. The ability to plan with smaller headquarters or staffs will also enable smaller units, operating as a distributed force on an information-denied battlefield, to conduct operations based on horizontal collaboration with those units they can communicate with, rather than relying on top-down direction from higher echelons that may not be viable. If and when communications are restored, units at all levels can regain a shared understanding of the battlespace.
- **Mesh networks** connect across many nodes based on availability, rather than using the more common hierarchical model where information flows up and down, but is not routed laterally. Each node acts as host and a router, allowing them to relay information between nodes that cannot directly connect. They therefore require very little infrastructure, and self-organize even in very dynamic environments. Mesh networks are most useful in environments where

[135] Cognitive Communications, U.S National Aeronautics and Space Administration (last accessed 2023).

[136] SCSP staff engagement with Johns Hopkins University Applied Physics Laboratory (November 2022).

[137] New C2 Tech Enables Rapid Decision Making, Response, Booz Allen Hamilton (last accessed 2023).

[138] New C2 Tech Enables Rapid Decision Making, Response, Booz Allen Hamilton (last accessed 2023).

key nodes in hierarchy or tree-based networks are likely to be blocked or destroyed,[139] and would improve the resilience of U.S. and allied networks.

- **Software baselines or architectures** to enable communication between systems and militaries are needed to enable interoperability. DoD needs to adopt either application program interfaces (APIs) or another form of integration software, such as the System-of-systems Technology Integration Tool Chain for Heterogeneous Electronic Systems (STITCHES), to enable all systems in its network to communicate with each other when appropriate, even if those systems are owned by different services, or by allied militaries.
- **Micro-satellite constellations** consist of small, low-cost satellites under 100 kilograms capable of multiple rapid-launch and high-resolution imagery. DARPA's Blackjack is a program under development to demonstrate an orbital mesh network of autonomous Low-Earth Orbit (LEO) commercial and military microsatellites[140] capable of providing low-latency internet connectivity between sensors and weapons for military missions.[141]

Intelligence

Capabilities Needed. Outpacing peer adversaries in highly contested environments will require U.S. military intelligence to seamlessly access and fuse information from sensors collecting information across all domains, organizational levels, and sources to include open-source information, and organizational levels at machine speed to enhance situational awareness and decision advantage for real-time analysis and targeting. To meet the above mission requirements in an Indo-Pacific contingency, the U.S. military needs a combination of data source integration, greater speed and scale for data analysis, improved human-systems integration, low-cost airborne sensor platforms that can be deployed en masse, human-machine collaboration for intelligence analysis, intelligence dissemination for distributed forces, and enhanced deception against PLA AI-enabled and autonomous systems.

- **Access to and integration of ally and partner data sources.** U.S. intelligence needs to integrate potentially relevant data trapped across disparate systems or lying untapped within nontraditional sources to improve the accuracy and quality of intelligence to achieve software advantage.[142] This entails improving agreements on data-sharing and releasability, and translating data collected using different methodology, processes, and systems across domestic and foreign intelligence entities.

---

[139] Antonio Cilfone, et al., Wireless Mesh Networking: An IoT-Oriented Perspective Survey on Relevant Technologies, Future Internet (2019).

[140] Rajesh Uppal, DARPA Blackjack is Autonomous LEO Satellite Constellation With Mix of Commercial and Military Microsatellites for Space, International Defense, Security, and Technology (2022).

[141] Nathan Strout, Is Project Blackjack Still Relevant?, C4ISRNET (2022).

[142] Intelligence in An Age of Data-Driven Competition, Special Competitive Studies Project (2022).

- **Enhanced collection.** Intelligence collection needs to evolve to maintain persistent access to and aggregate information in near real-time to respond to rapidly changing adversary behavior and operational environments. U.S. intelligence needs to explore new ways to upgrade existing intelligence assets such as satellites, UAVs, and sensor systems with AI-enabled edge capabilities and processing devices while expanding the range and resiliency of smaller, cheaper platforms.[143] Nontraditional and open-source information are also increasingly important sources for delivering value, particularly where classified data cannot be shared, or shared quickly. A new generation of intelligence collectors and analysts need to be trained to access and evaluate nontraditional sources and data, including publicly available information generated by commercial space systems and social media applications.[144]
- **AI-enabled data analysis speed and scale.** U.S. military and intelligence communities must adopt and adapt AI-enabled capabilities, which will become indispensable to the intelligence enterprise. Rather than serving as mere tools, AI-enabled systems can adopt a teammate role in joint problem-solving by (1) optimizing information collection, filtering, and prioritization of high-volume, multi-source information and (2) supporting human intelligence in batch analysis of structured and unstructured data, to push selected data of interest for analysis by human intelligence analysts.[145] To achieve these effects, AI-enabled intelligence analysis needs to be supported by new forms of data management and sets of expertise. The current closed, proprietary architecture and single collection streams of data pose obstacles to rapid ingestion of data at scale. New cloud-based architectures capable of reconciling single, multi-, and all-source intelligence collection and analysis enable knowledge integration at the data layer and data dissemination through multiple – rather than a single – intelligence disciplines.[146]
- **Human-Systems Integration (HSI).** Redesigning human-machine interfaces and recalibrating the optimal allocation of human and machine roles and responsibilities will be one of the most important and defining features of future military and intelligence operations. To get the most out of human-machine teaming and collaboration for intelligence, intelligence system design and development must evolve to train humans to work with "smart" machines and acquire understanding of how humans and machines improve over time through repeated interactions and interventions. Machine teammates over time may also develop the ability to tailor themselves according to analysts' peak cognitive load and preferences for certain levels and types of information. Human judgment at the junior personnel level will also need to become more sophisticated, distributed, and complex to

[143] Jake Harrington & Riley McCabe, Modernizing Intelligence, Surveillance, and Reconnaissance to 'Find' in the Era of Security Competition, Center for Strategic & International Studies (2021).

[144] Mid-Decade Challenges to National Competitiveness, Special Competitive Studies Project at 157-158 (2022); Catherine Johnston, et al., Transforming Defense Analysis, Joint Force Quarterly (2015).

[145] Anna Knack, et al., Human-Machine Teaming in Intelligence Analysis, Center for Emerging Technology and Security at 14-16 (2022).

[146] Anna Knack, et al., Human-Machine Teaming in Intelligence Analysis, Center for Emerging Technology and Security at 14-16 (2022).

constantly reconfigure and repair AI systems that must handle misleading or missing metadata.[147]

- **Low-cost, jet propulsion, airborne sensor platforms.** Identifying PRC amphibious surface vessels and fighter aircraft will depend upon a proliferation of ISR sensors of various modalities – which becomes the 'sensing grid'. Because legacy ISR aircraft (e.g., E-3, E-8, RC-135, RQ-4) aircraft will likely not be survivable in the early phases of a conflict with a peer adversary, an adequate sensing grid must include sensors on airborne platforms of sufficiently low cost to render them attritable and able to achieve mass. The airborne sensing grid should integrate low-cost systems launched from Taiwan to the maximum extent possible. Achieving mass in ISR sensors will improve target identification and track quality, and thereby improve munition effectiveness and efficiency. Though joint interoperability is imperative, this interoperability need not take place at the data link level. In the near term, even if military services and departments develop ISR sensor platforms that are not interoperable, joint data transmissibility and interpretability can be added at a data aggregation layer. This low-cost airborne sensing grid should rely to the maximum extent feasible on existing commercial technology.[148]
- **Dissemination of intelligence for distributed, network-based operations.** Closing, and where necessary, accelerating the sensor-to-shooter gap increasingly relies on data processing at the tactical edge, enabled by ML capabilities that have been moved as far forward as possible, preferably to the location of the data source. This involves increasing the resiliency and performance of tactical networks through a modular open system approach (MOSA) and data management architecture capable of handling massive volumes of sensor data in real-time.
- **Denial and Deception.** Growing reliance on AI/MLfor information collection and fusion creates vulnerabilities to denial and deception on both sides. AI-enabled, hidden networks of sensors and shooters central to A2/AD, can be exploited to find PLA targeting assets by corrupting fielded models to trigger the deployment of long-range sensors and strike assets prematurely or against phantom targets.[149] Altering and manipulating PRC AI training datasets requires U.S. intelligence to build a comprehensive profile of both friendly and PRC signatures and methods for securing reliable access to PRC AI systems during war and peacetime, bolstered by the use of independent highly-trained red teams during model training, testing, and fielding.[150] These same red teams will be instrumental in protecting U.S. training datasets and AI models from corruption, denial, and deception attempts by PRC

[147] Avi Goldfarb & Jon Lindsay, Artificial Intelligence in War: Human Judgment as an Organizational Strength and a Strategic Liability, Foreign Policy at Brookings at 6-7 (2020).

[148] David Ochmanek, Determining the Military Capabilities Most Needed to Counter China and Russia, RAND Corporation at 7-8 (2022).

[149] Stephan Pikner, Leveraging Multi-Domain Military Deception to Expose the Enemy in 2035, Military Review (2021).

[150] Stephan Pikner, Leveraging Multi-Domain Military Deception to Expose the Enemy in 2035, Military Review (2021).

forces. Exquisite sensor systems and other intelligence assets need not only to hide from detection and counter-operations but also evolve in response to PRC adaptations.

- **Predictive intelligence.** U.S. intelligence must develop predictive intelligence capabilities using AI-enabled live modeling and simulation tools to enter the PRC's decision cycle and achieve real-time sense-making of the rapidly evolving threat environment.

Technology-Based Solutions.

- **Autonomous ISR platforms** can enable immediate intelligence-gathering and analysis to inform warfighters' decision-making even in electronically contested and denied environments. Collaborative networks of satellites and UAS equipped with edge processors capable of running AI-enabled software suites can bring advanced computing power and artificial intelligence tools to the tactical edge and enable real-time processing of optical, radar, infrared images, and electronic signals to deliver actionable intelligence in real-time.[151] In the future, AI/ML-enabled software would allow requests for intelligence data by warfighters in the field to be distributed to space and air layer sensors capable of collaborating to find, fix, target, and track objects in response to the request.[152] Satellite data would cue and refine air search patterns and update satellites on the availability of tactical air platforms to maximize focus on areas of interest.[153]
- **Open-source intelligence technologies** and techniques can collect, process, and analyze publicly available information to rapidly deliver insights into nonpermissive environments. Tools and techniques such as geotagging, georeferencing, web scraping, sentiment analysis, and lexical analysis, can utilize data generated by citizen smartphones, internal Global Positioning System (GPS) devices, and Twitter accounts to provide insights, including the disposition, composition, and strength of adversary forces, events, and status of infrastructure.[154]
- **Micro-satellite constellations** consist of small, low-cost satellites under 100 kilograms capable of multiple rapid-launch and high-resolution imagery. Microsatellites provide an advantage over exquisite, high-end space assets, which have become increasingly vulnerable in the contested space domain. The Tactical Space Layer (TSL) is an Army program that will provide tactical space-based deep-area sensing, rapid targeting information, and enhanced battlefield situational awareness to shorten the sensor-to-sensor cycle and enable long-range precision fires in GPS-challenged environments.[155] SpaceX's Starlink satellite constellation has significantly altered the domain of high-resolution imagery, which was once

[151] Ryan Schradin, Nations Look to Futuristic ISR Solutions for National Defense and Security in War Time, Modern Battlespace (2022).

[152] Lisa Daigle, AI-Enabled Autonomous Systems for ISR Garner Army Demo Contract, Military Embedded Systems (2022).

[153] Lisa Daigle, AI-Enabled Autonomous Systems for ISR Garner Army Demo Contract, Military Embedded Systems (2022).

[154] Michael Rasak, Event Barraging and the Death of Tactical Level Open-Source Intelligence, The Military Review (2021).

[155] Theresa Hitchens & Sydney J. Freedberg Jr., Exclusive: Army Plan May Loosen IC Grip On Sat-Based ISR, Breaking Defense (2021); U.S. Army Approves Rapid Development, Delivery of Tactical Space Layer, U.S. Army (2021).

reserved for military space powers.[156] In 2021, intelligence company Umbra launched the first radar-imaging microsatellite of its planned constellation on the SpaceX Transporter-2 mission.[157]

- **A digital nervous system** capable of searching for patterns and connecting thousands of presumed anomalies across aggregate data streams can provide anticipatory indications and warning, and inform more sophisticated strategic decisions.[158] Guardian is an example of a platform that can identify gathering trends and flashpoints before they become imminent to inform military planning and decision-making at the speed of relevance.
- **HMT for intelligence analysis.** ML-enabled systems can adopt a teammate role in joint problem-solving by (1) optimizing information collection, filtering, and prioritization of high-volume, multi-source information and (2) supporting human intelligence in batch analysis of structured and unstructured data, to push selected data of interest for analysis by human intelligence analysts. Over time, machine teammates may be able to tailor themselves according to analysts' peak cognitive load and preferences for certain levels and types of information.

Movement and Maneuver

Capabilities Needed. To meet the above mission requirements for movement and maneuver in an Indo-Pacific contingency, the U.S. military needs access to allied bases and airspaces during the critical first few days of a conflict. Most, if not all, operations must begin with deception operations, or employ masking.[159] Allies, enabled by or alongside U.S. forces, must be able to impose large costs on PLA ground-based or amphibious offensive operations.

- **Access to allied bases and airspace.** Access to allied bases and airspace during the critical first few days of deployment can be more important than allied platforms and weapons contributions.[160] With allied infrastructure, U.S. forces can be rapidly deployed to limit PLA incursion in the early stages of conflict when assets are limited and needed to respond to competing areas of operation.[161]
- **Deception operations.** The PLA increasingly has the potential to deny U.S. forces access to the Indo-Pacific, reducing their ability to mass force or bring combat power to bear at decisive points through the use of conventional means. To succeed, most if not all operations

[156] Matthew Holland, UkraineX: How Elon Musk's space satellites changed the war on the ground, Politico (2022).

[157] Umbra Launches World's Most Capable Commercial Radar-Imaging Satellite, Umbra (2021).

[158] AI-Powered Decisions at the Speed of Relevance, Rhombus (last accessed 2023).

[159] John Antal, 7 Seconds to Die: A Military Analysis of the Second Nagorno-Karabakh War and the Future of Warfighting, Casemate at 156 (2022).

[160] Myron Hura, et al., Interoperability: A Continuing Challenge in Coalition Air Operations, RAND Corporation at 170-172 (2000).

[161] Myron Hura, et al., Interoperability: A Continuing Challenge in Coalition Air Operations, RAND Corporation at 171 (2000).

must begin with deception operations that lead the PLA astray, disrupt or derail their ongoing operations, and inject uncertainty about the validity of their reports, intelligence analysis, and the performance of vital systems. This will likely include the use of decoys.

- **Masking.** The proliferation of sensors, analytical tools, precision-guided munitions, and non-kinetic payloads are making it easier for the PLA to find and attack U.S. and allied forces operating in the Indo-Pacific, making it difficult to employ operational surprise or tactics that rely on large formations consolidating or maneuvering to achieve decisive results. Masking is the "full-spectrum, multi-domain effort to deceive PLA sensors and disrupt PLA targeting. It is the active and passive ability to make military systems difficult or impossible to identify, locate, and target."[162] Similar to deception operations, this is likely to include the use of decoys.
- **Imposition of cost on ground-based or amphibious offensive operations.** Given the short distance between the PRC and Taiwan and the preponderance of forces the PLA will bring to bear, it will be very difficult to prevent PLA ground forces from reaching Taiwan. If the PLA does establish a lodgment on Taiwan, it will also have to breakout of their lodgment and seize Taiwan's highly defensible terrain – much of it urban[163] – all with ever growing logistical demands. Urban warfare's extremely heavy logistical demands would also increase the PLA's cross-strait logistical requirements, creating additional opportunities for Taiwan and others to disrupt PLA operations.[164]

Technology-Based Solutions.

- **Multi-agent swarms** would consist of a combination of drone and human agents that would disrupt adversary logistics and mobility. Drones such as the Bayraktar TB-2 and loitering munitions such as the Switchblade 300/600 or Harop can engage adversary light and heavy vehicles, hindering their ability to move out of any lodgments, or to seize urban terrain.[165] Self-organizing ground forces would continue attacking dismounted forces, particularly in highly defensible urban terrain. Due to being self-organizing, they would be able to make decisions much more quickly than hierarchically-organized adversary forces, and would not need to communicate on the electromagnetic spectrum.[166] The employment of multi-agent swarms can be assisted greatly by the use of agent-based simulation software that would allow allied forces to experiment with swarm compositions and self-organizing behaviors in different terrains and against different adversary orders of battle.

---

[162] John Antal, 7 Seconds to Die: A Military Analysis of the Second Nagorno-Karabakh War and the Future of Warfighting, Casemate at 156 (2022).

[163] See Ian Easton, The Chinese Invasion Threat: Taiwan's Defense and American Strategy in Asia, CreateSpace (2017).

[164] See John Spencer, The Urban Warfare Project's Christmas Wish List, 2021 Edition, Modern War Institute (2017).

[165] Ken Dilanian, et al., Biden Admin Will Provide Ukraine with Killer Drones Called Switchblades, NBC News (2022); Ken Dilian & Courtney Kube, Why Are Ukraine's Cheap, Slow Drones So Successful Against Russian Targets?, NBC News (2022).

[166] Justin Lynch & Lauren Fish, Soldier Swarm: New Ground Combat Tactics for the Era of Multi-Domain Battle, Modern War Institute (2018).

- **Employ HMT to achieve mass.** By employing lower-cost, easier- and faster-to-manufacture, and AI-enabled machines, new operational concepts can be developed that leverage autonomy to permit operators and machines to overcome complex, high-risk challenges. Massed machines, assigned tasks by their human teammates, could overwhelm traditional defenses, often at a relatively smaller cost in human lives compared to more traditional offensive operations.
- **Counter-autonomy.** As the U.S. military integrates more AI, human-machine teaming, and autonomy, adversaries can be expected to do the same. The U.S. military must work with allies to develop interchangeable capabilities and concepts for countering adversary autonomy. In the near term, the focus of U.S. counter-autonomy efforts could include identifying means and generating access to take over adversaries' AI-enabled systems to extend our sensing deep inside their territory and within their decision-making. During conflict, counter-autonomy efforts could include actions to manipulate the data or outputs of adversarial AI-enabled systems so as to inject mistrust between their forces and their machines, degrading the performance of their AI-enabled and autonomous systems, or destroying them entirely through kinetic or non-kinetic means.[167]
- **Prepositioned assets** such as containerized weapon systems, containerized ammunition systems, and submersible stocks of weapon systems can greatly enable maneuver forces. Maneuver forces can access additional weapon systems without receiving resupply, arm regional allies and partners, and maneuver and fight with a less burdensome logistical tail.

Fires

Capabilities Needed. To meet the above mission requirements for fires in an Indo-Pacific contingency, the U.S. military needs a combination of long-range and deep strike capabilities, a high volume of both munitions and drones, multivector fires, as well as the ability to disrupt or destroy adversary ISR and electromagnetic spectrum operations, and provide disaggregated forces the connectivity and authorization they need to access fires, even when cut off from higher headquarters.

- **Long-range, deep strike.** Destroying weapons and assets underpinning A2/AD requires U.S. air strikes to penetrate heavily defended airspace and find distant targets – including mobile missile launchers, command posts, sensors, and communications systems – dispersed across millions of miles of the interior.[168] U.S. forces need to modernize artillery, bomber, missile, and electromagnetic spectrum operation systems to interoperate with allies and increase the range of fire and counterfire capability, which includes augmented over-the-horizon

[167] Counter Autonomy: Executive Summary, U.S. Department of Defense, Defense Science Board at 3 (2020).

[168] Stephen Biddle & Ivan Oelrich, Future Warfare in the Western Pacific: Chinese Antiaccess/Area Denial, U.S. AirSea Battle, and Command of the Commons in East Asia, International Security at 8 (2016).

targeting using cheap loitering munitions employing AI-enabled targeting systems that can target adversary fighter and bomber aircraft, both in the air and on the ground, and amphibious surface vessels in the Taiwan Strait. These aircraft should be jet propelled to attain the necessary ranges and should be inexpensive enough to achieve the required volume. Posturing missile batteries in forward locations on allied soil will also lower the cost of delivery and bring mass within range of targets from the early onset of conflict.[169]

- **High volume of munitions and drones.** A2/AD zones of near-peer competitors are capable of absorbing tremendous amounts of conventional firepower and replacing losses after repeated strikes without long-term effect.[170] Deploying exquisite systems against adversaries' increasingly capable layered anti-aircraft defenses has become prohibitively costly and needs to be replaced with cheap, self-contained options for penetrating adversary air and missile defense systems, including commercial off the shelf drones.[171] Employing greater quantity, variety, and distribution of decoys and other deceptive assets that mimic the profiles of aerial and surface platforms can force the adversary to reveal and expend A2/AD assets.[172] In the face of fiscal and capacity constraints, U.S. forces, in partnership with allies, will need to deliberately develop the depth of cost-effective munitions and drones needed to saturate PRC A2/AD and deplete its industrial capacity. This involves deliberate planning and prioritization and working closely with allied forces to improve the ability to collectively develop and manage munitions stockpiles.
- **Multiple attack vectors and cross-domain effects.** As part of the need to limit adversary options and generate dilemmas, U.S. and allied and partner forces need the ability to coordinate and mass fires from many vectors, and across multiple domains.
- **Disruption or destruction of ISR and electromagnetic spectrum operations.** U.S. forces need to employ lethal and nonlethal effects, including counter-autonomy systems, to disrupt or destroy adversary electromagnetic spectrum operations, and space and cyber capabilities that block access to or undermine the reliability of adversary command and control, communications, tracking, and targeting data for lethal strike. Communications, sensors, and other ISR assets will also need to be destroyed to degrade adversary early warning and targeting capabilities, and prevent the adversary from building their own multi-domain common operational picture.[173]
- **Connectivity and authorization for disaggregated force.** Joint fires need to maximize connectivity across the Services and disparate platforms to keep pace in an operational

[169] Richard B. Shermer & Christopher T. Lenick, Strengthening Intelligence, Surveillance, and Reconnaissance Employment in the Indo-Pacific Region, Journal of Indo-Pacific Affairs at 4-5 (2022).

[170] Alex Vershinin, The Challenge of Dis-Integrating A2/AD Zone: How Emerging Technologies Are Shifting the Balance Back to the Defense, Joint Force Quarterly (2020).

[171] David Ingels-Thompson, Rethinking SEAD for A2/AD, Proceedings (2021).

[172] James Taylor, Dazzle: Disguise and Deception in War and Art, Naval Institute Press (2016).

[173] Ben Wermeling, Defeating Anti-Access/Area Denial in the West Pacific, Strategy Bridge (2016).

environment in which adversary weapons systems present "ephemeral windows of targetable vulnerability."[174] Current service-specific C2 architectures and authorities are not synchronized in ways that allow targeting information in one domain to interoperate with and seamlessly extend to platforms in another to inform fire and counter-fire kill chains at the speed of relevance. Joint fires will need improved interoperability, decentralized architecture, AI-enabled real-time data exchange, automation of fire control functions,[175] and automated integration with the sensing grid. A sensing grid should include an AI-enabled optimization engine for sensor-to-target and weapon-to-target pairing, to fuse discrete kill chains and compress the sensor-to-shooter cycle. These systems must be capable of targeting certain classes of adversary systems (e.g., amphibious surface vehicles and adversary fighter and bomber aircraft) automatically, when certain thresholds of certainty are achieved in accordance with rules of engagement. At the same time, fires must be operationally decentralized and geographically distributed to provide a credible, offensive, and conventional deterrent to assure U.S. freedom of action.[176]

Technology-Based Solutions.

- **Joint Air to Surface Standoff Missile – Extended Range (JASSM-ER)** is a next-generation, stealth cruise missile that extends the range of the standard JASSM from 370 km to 1,000 km[177] to "destroy high-value, well-defended, fixed and relocatable targets from significant standoff range."[178] The JASSM-ER in 2022 was integrated as the B2 bomber's "first long-range stealth missile" and derivatives are currently under development to enhance resistance to jamming and spoofing and enable a two-way data link for "retargeting post-launch, against relocatable or higher priority targets during mission execution."[179]
- **Hypersonic missiles** capable of maneuvering at Mach 5 and above can enable rapid-response, long-range strike options against distant, defended, and/or time-critical threats in denied environments.[180] Hypersonic weapons may be able to provide the combination of speed, accuracy, range, and survivability needed to neutralize the A2/AD zones being developed by adversaries.[181]

[174] Pablo Kruger, et al., The Future of Air-Ground Integration: Linking Sensor to Shooter in the Deep Fight, Air Land Sea Application Center (2021).

[175] Pablo Kruger, et al., The Future of Air-Ground Integration: Linking Sensor to Shooter in the Deep Fight, Air Land Sea Application Center (2021).

[176] Philip S. Davidson, Transforming the Joint Force: A Warfighting Concept for Great Power Competition, U.S. Indo-Pacific Command (2020).

[177] Missile Defense Project, JASSM/JASSM-ER, Center for Strategic and International Studies: Missile Threat (2016).

[178] Joint Air-to-Surface Standoff Missile (JASSM), Lockheed Martin (2023).

[179] Joseph Trevithick & Thomas Newdick, B-2's First Launch of Stealthy JASSM-ER Cruise Missile Disclosed, The Drive (2022).

[180] Kelley M. Sayler, Hypersonic Weapons: background and Issues for Congress, Congressional Research Service (2023).

[181] U.S. Hypersonic Weapons and Alternatives, Congressional Budget Office (2023).

- **3D printing of custom munitions and drone components** could enable rapidly and remotely fabricated energetic material payloads and munitions[182] with double the range and increased lethality. Researchers are currently working to optimize feedstocks of metals, ceramics, composites and polymers for munition components to yield novel geometries and production techniques for optimized performance.[183] For example, printed gun propellant charges and rocket motors could help achieve higher muzzle velocity and longer range, and better metal feedstocks may increase munition penetration to augment lethality.[184]

Sustainment (Expeditionary Logistics)

Capabilities Needed. To meet the above mission requirements for expeditionary logistics in an Indo-Pacific contingency, the U.S. military needs to proactively distribute critical materials and supplies. U.S. forces should also improve their ability to sustain themselves from prepositioned or locally sourced materials. Sustainment operations should avoid detection by employing a combination of deception, masking, and undersea movement.

- **Cyber and physical hardening.** Sustainment hubs and lines of communication are vulnerable to cyber and kinetic attacks. The PLA has the potential to attack hubs at Kadena, in the Philippines, and in Guam. If the PLA disables such forward logistic hubs, it could be debilitating to U.S. operations in the region. The United States needs work with its allies to disperse and harden its logistics posture. Where forces simply cannot become more agile, harden, mask, and create redundancies. While active defenses can have some effect, assume adversary weapons get through and be prepared to rapidly restore basic capabilities to support combat operations whether from airfields or logistics sites.
- **Proactive distribution.** Conflicts in the Indo-Pacific are likely to be characterized by long supply lines for U.S. forces, firing rates that expend prepositioned munitions and outpace resupply capabilities, and the attrition of forces.[185] To optimize sustainment, U.S. forces need to develop data-informed systems that actively monitor and project usage, project requirements for future operations, and dynamically prioritize resupply. AI/ML solutions offer potential for deriving optimal solutions to dynamic supply-demand imbalances (delivering the right material to the right place at the right time).
- **Reduce sustainment requirements.** To alleviate the burden placed on resupply, U.S. forces should also improve their ability to sustain themselves from prepositioned or locally sourced materials. Doing so would not only reduce the number of trips made into contested spaces. It

[182] Science of Additive Manufacturing for Next Generation Munitions (SAMM) – DEVCOM Army Research Laboratory, Army Research Laboratory (2023).

[183] Additive Manufacturing to Provide Soldiers with Cutting-Edge Munitions, U.S. Army (2020).

[184] Additive Manufacturing to Provide Soldiers with Cutting-Edge Munitions, U.S. Army (2020).

[185] Robert Haddick, Defeat China's Navy, Defeat China's War Plan, War on the Rocks (2021).

would also reduce U.S. force footprint and visibility, therefore decreasing the odds of detection and attack.[186]

- **Avoiding detection.** As noted above, adversaries are likely to target sustainment forces operating in the Indo-Pacific, which should employ a combination of dispersion, deception, masking, and undersea movement to reach U.S. forces.

Technology-Enabled Solutions.

- **Low-profile, autonomous vessels (LPVs)** are able to provide long-range, multi-ton resupply to U.S. forces in the Indo-Pacific. Inspired by narco submarines, semi-submersible vessels are low-cost, attritable, and difficult to detect.[187] While LPVs do not have enough capacity to conduct bulk resupply, they can carry replacement parts, some critical munitions, and some end items.
- **Rapid, transportable runway repair** enables militaries and civilian authorities to repair bomb and other types of damage to allow supply and other aircraft to quickly use runways after attack.
- **Portable hydrogen fuel generators** use local resources to produce hydrogen fuel.[188] Aluminum and water, combined with small amounts of gallium and indium, can be converted into hydrogen fuel for use by U.S. military vehicles and ships. Students at Massachusetts Institute of Technology (MIT) have already produced an aluminum-fueled car,[189] and researchers on the project argue that it would be possible to fuel light battalion-size formations using only prepositioned and locally sourced supplies.[190]
- **Metal 3D printing technology** by companies such as Spee3D and MELD Manufacturing provides rapid and cost-effective replacement parts for military applications. MELD technology was selected by the U.S. Army in 2021 to be used to print jointless vehicle hulls, and the U.S. Navy in 2022 to launch the Navy Additive Manufacturing Center of Excellence.[191] Spee3D's WarpSPEE3D machine has been used to design spare parts for the Australian Army's armored vehicles and rapidly print 3D parts in the field across a range of rough terrain.[192]

Information

[186] John Sattely & Jason A. Paredes, Sustainment of Stand-in Force, War on the Rocks (2022).

[187] Attritably may vary based on a vessel's cargo.

[188] These Marine-Generated Tech Ideas are Becoming Prototypes for Actual Field Use, Massachusetts Institute of Technology Lincoln Laboratory (2022).

[189] Walker Mills & Erik Limpaecher, Need Fuel? Marines Should Make Moonshine Hydrogen, Proceedings (2021).

[190] Presentation to the Defense Panel on July 19, 2022.

[191] Edward Wakefield, MELD Additive Manufacturing Technology Selected by US Navy, 3D Printing Media Network (2022).

[192] Edward Wakefield, Nupress Brings SPEE3D's Cold Spray Technology to Australian Manufacturers, 3D Printing Media Network (2022); SPEE3D Chosen by British Army for the US Army's Project Convergence, Digital Engineering (2022).

Capabilities Needed. The PRC government's censorship regime is sophisticated, and generally effective. To meet strategic mission requirements for information in an Indo-Pacific contingency, the U.S. military needs to occupy or saturate autonomous censorship systems, and give populations communication systems that bypass censorship regimes entirely. For military operations, the U.S. military and IC need to invest in a variety of adversarial attack capabilities that target adversary information systems and AI/ML models, in peacetime, crisis, and conflict.[193]

- **Saturate or bypass censorship regimes.** Authoritarian regimes rely heavily on information control to shape their messaging, crush dissenting voices, and deny population-wide access to alternative sources of information. As such, they are vulnerable to operations that allow their populations to more easily and consistently bypass censorship systems and access information other than state propaganda. In the context of war, such operations – including AI-enabled messaging to circumvent censorship – have the potential to distract authoritarian regimes by increasing their focus on domestic security, to the detriment of their offensive operations. There is evidence that broader exposure to different sources of international information about the PRC also, on average, causes PRC citizens to reduce their belief that their government should pursue ambitious foreign policy goals.[194]
- **Adversarial attacks against information systems and AI/ML models.** According to the NSCAI Final Report, "Given the reliance of AI systems on large data sets and algorithms, even small manipulations of these data sets or algorithms can lead to consequential changes for how AI systems operate. The threat is not hypothetical: adversarial attacks are happening and already impacting commercial ML systems."[195] The U.S. military and IC need to invest in a variety of adversarial attack capabilities that target adversary information systems and AI/ML models, in peacetime, crisis, and conflict.

Technology-Enabled Solutions.

- **Media Manipulation Monitor** "uses signal-rich proprietary data… to decode foreign governments' efforts to manipulate the narrative — including censorship, disinformation, and propaganda campaigns — revealing the intentions, information, and priorities they would rather keep hidden."[196] Tracking automated and manual censorship creates opportunities to create messages that avoid automated censorship, and adapt them in real time in response to changes in censorship patterns.
- **Offline, peer-to-peer communication applications.** During pro-democracy protests in Hong Kong, protesters used applications like FireChat to communicate on cell phones without using

[193] Final Report, National Security Commission on Artificial Intelligence at 52 (2021).

[194] Haifeng Huang, How Information Bubble Drives the Chinese Public's Views of China's Global Standing and Fuels Grassroots Nationalism, ChinaDataLab (2020).

[195] Final Report, National Security Commission on Artificial Intelligence at 52 (2021).

[196] M3: Decoding Foreign Markets through Data, Analytics and Insights, TwoSix Technologies (last accessed 2023).

the Internet.[197] Similar applications, especially with anonymous use built in, would help citizens of authoritarian nations avoid censorship.

- **Generative AI models.** While generative AI models such as GPT-4 and ChatGPT are in their infancy, we should anticipate rapid maturation of similar models over the next few years. The U.S. needs to develop a strategy for using generative AI to overwhelm adversary censorship systems and to provide alternative, precision messaging mechanisms.

Protection

Capabilities Needed. To meet the above mission requirements for protection in a Western Pacific or Indian Ocean contingency, the U.S. military needs to develop a layered missile defense system capable of defending against a proliferating number and type of missile threats, integrate regional missile defenses with allies and partners to fill gaps and reinforce sensing and intercept capabilities, strengthen active and passive defense systems to protect assets, bases, and critical infrastructure against kinetic, cyber, and electronic threats, and autonomously predict, detect, and counter threats.

- **Cooperative and integrated regional missile defense.** U.S. forces can no longer rely solely on its own integrated air and missile defense (IAMD) to defend fixed main operating bases and high-value assets amid adversaries' growing arsenal of ballistic missiles, uncrewed aerial vehicles, and hypersonic weapons capabilities.[198] Extending limited IAMD capability and survivability of combat forces requires moving beyond coordination to seamlessly integrate and interoperate sensors and interceptors with regional allies and partners. Combining ally and partner sensor coverage into an integrated network architecture will help to increase regional situational awareness and build a redundant web of sensors to complicate adversary targeting.[199]
- **Layered missile defense.** U.S. Strategic Command commander Admiral Charles Richard in 2021 articulated: "A robust and credible layered missile defense system paired with our conventional and nuclear force capabilities provide the ability to deter strategic attacks, deny benefits, and impose costs against any potential adversary."[200] The U.S. military must develop defensive capabilities against a proliferating number and types of missile threats at all ranges and in all phases of flight before they reach their target through: (1) networked sensors and ground and sea-based radars for target detection and tracking and (2) ground, sea, and space-based interceptors, directed energy weapon systems, and other systems

[197] Peter Shadbolt, FireChat in Hong Kong: How an App Tapped its Way into the Protests, CNN (2014).

[198] Lynn Savage, US INDOPACOM's Integrated Air and Missile Defense Vision 2028, Journal of Indo-Pacific Affairs (2022).

[199] Lynn Savage, US INDOPACOM's Integrated Air and Missile Defense Vision 2028, Journal of Indo-Pacific Affairs (2022).

[200] Punch Moulton & Francis Mahon, Robust, credible and layered missile defense is the foundation of deterrence, DefenseNews (2021).

connected by (3) command, control, battle management, and communications networks.[201] A resilient space-based missile warning and tracking sensor architecture will be increasingly important for high-quality fire control data.

- **Active and passive defense of critical assets.** Missile defense requires a combination of passive and active measures to protect critical assets and infrastructure against adversary attack. Passive defenses include hardened air bases and sites, infrastructure to disperse forces; camouflage, concealment, and deception; and rapid reconstitution.[202] U.S. and allied forces must ensure rapidly recoverable, redundant energy, transport, financial services, and water systems that support the rapid movement of forces in a crisis or contingency. Active defense includes kinetic hit-to-kill interceptors, directed energy weapons, blast fragmentation warheads,[203] counter- uncrewed aerial systems (C-UAS), and left-of-launch counter-offensive operations using non-kinetic effects, such as electromagnetic propagation and cyber offense to defeat missile threats before they are launched.[204] Offensive cyber operations against missile systems include exploiting missile designs, altering software or hardware, and creating clandestine pathways to missile C2 systems. Targets extend to spaced-based and space-dependent assets that relay critical data to missile defense systems, such as communications, positioning, navigation, and timing (PNT), weather data and launch conditions, and remote imagery for targeting.[205]
- **Autonomous threat detection and predictive risk estimation.** U.S. forces need to leverage AI/ML capabilities to defend against cyber operations that exploit missile designs, alter software or hardware, and create clandestine pathways to missile C2 systems. Targets extend to space-based and space-dependent assets that relay critical data to missile defense systems, such as communications, PNT, weather data and launch conditions, and remote imagery for targeting.[206] Sensing layers need to be capable of fusing and passing information from one sensor to the next without ground intervention to keep unbroken custody of high-speed, maneuverable threats with low emission signatures. As adversaries' missile capabilities mature, U.S. missile defense systems need to bake in autonomy and predictive analytics capabilities into the sensing architecture to enable real-time detection of sophisticated missile threats.[207] AI/ML to detect, recognize intent, understand threat capability, and communicate between sensors will become an embedded feature of missile defense.

[201] MDA – The Ballistic Missile Defense System, U.S. Missile Defense Agency (last accessed 2023).

[202] Carl Rehberg, Integrated Air And Missile Defense: Early Lessons From The Russia-Ukraine War, Center for Strategic and Budgetary Assessment (2022); Kingston Reif, Current U.S. Missile Defense Programs at a Glance, Arms Control Association (2019).

[203] Kingston Reif, Current U.S. Missile Defense Programs at a Glance, Arms Control Association (2019).

[204] Riki Ellison, Left of Launch, Missile Defense Advocacy Alliance (2015).

[205] Patricia Lewis, The Destabilizing Danger of Cyberattacks on Missile Systems, Chatham House (2019).

[206] Patricia Lewis, The Destabilizing Danger of Cyberattacks on Missile Systems, Chatham House (2019).

[207] Lockheed Martin, The Future Will Rely on Autonomous Threat Detection for All Domains, Defense One (2022).

- **AI-Enabled Counter-Sensing.** A high-end adversary will rely on AI-enabled ISR. While generating a 100% denial of an adversary's ability to sense and make sense might seem ideal, an adversary's reliance upon AI models creates the opportunity for increased fog and friction. While outright denial may be the right choice at times, U.S. forces should consider the advantages inherent in using capabilities that degrade an adversary's AI models in such a way that operators can no longer trust system outputs, generating doubt and injecting friction into decision-making processes. This approach may provide greater advantages than blunter techniques.

Technology-Enabled Solutions.

- **Agent-based modeling and simulation** of missile defense systems, which include use of digital twins, the Joint Simulation Environment,[208] and live-constructive-virtual integration, can represent actions and interactions of autonomous individuals, threats, and the command and control, battle management, and communications (C2BMC) network in a shared environment to inform and improve the design scheme of missile defenses.[209]
- **Cyber-hardening** of networks, sensors, and operational systems reduces the attack surface of a system and increases the difficulty of system access and exploitation.[210] As cyberattack patterns advance in speed and complexity, automation tools and analytics are force multipliers for raising the cost of aggression for adversaries. As an example, the "electronic armor" automation tool prevents attacks from disrupting missions on vehicles and systems by detecting system penetrations from any source through image recognition.[211] Advanced AI tools can accelerate incident response and threat-hunting and detection through constant collection and analysis of threat intelligence, and automation tools can rapidly filter false alerts, and find and fix security gaps. Built-in cybersecurity for software and hardware components and subsystems can also provide multiple layers of defense as they are assembled together.[212]
- **Zero trust** is an approach to cybersecurity that assumes no one inside or outside the network can be trusted by default and limits user access with the least-privilege access to required access to perform tasks. The architecture builds multi-attribute-based levels of confidence using techniques – including continuous multi-factor authentication, micro-segmentation, advanced encryption, endpoint security, analytics, and robust auditing – to continuously

[208] The Joint Simulation Environment or JSE is a scalable, expandable, high-fidelity, government-owned non-proprietary modeling and simulation environment. While designed originally for testing fifth-generation aircraft in a simulation environment, its use is expanding to fulfill other integrated testing requirements. Giancarlo Casem, Joint Simulation Environment inches closer to reality, Air Force (2019).

[209] Christopher J. Lynch, et al., Representing the Ballistic Missile Defense System Using Agent-Based Modeling, Proceedings of the Military Modeling & Simulation Symposium (2013); Shangyan Zhang, et al., A Multi-Agent-Based Defense System Design for Multiple Unmanned Surface Vehicles, Electronics (2022).

[210] Sally Cole, "Cyber Hardening" DoD Networks, Sensors, and Systems for Mission Resiliency, Military Embedded Systems (2016).

[211] Sally Cole, "Cyber Hardening" DoD Networks, Sensors, and Systems for Mission Resiliency, Military Embedded Systems (2016).

[212] J.R. Wilson, Military Cyber Security: Threats and Solutions, Military+Aerospace Electronics (2019).

validate access at every interaction and fortify data, applications, assets, and services to achieve enhanced cyber resiliency. Military cybersecurity forces must explore new techniques and technologies for applying and improving Zero Trust security.[213]

- **Counterspace weapons** can be used defensively to protect friendly space systems from attack, interference, and unintentional hazards before, during, or after an attack, and offensively to prevent the adversary's use of space capabilities and counterspace weapons to threaten friendly forces or support its own forces on Earth. A demonstration of capabilities that can compromise PLA space systems, through measures such as enhanced cyberhacking, spoofing, jamming, dazzling, and kinetic effects could support deterrence by causing the PLA to question its ability to leverage the space domain in support of system-of-systems concept of modern warfare and terrestrial-based joint operations.

Adaptation

Capabilities Needed. To meet the above mission requirements for adaptation in an Indo-Pacific contingency, the U.S. military needs to improve its digital infrastructure, place trained and authorized personnel in the right positions in the right organizations, create mechanisms and processes for continuous integration and continuous delivery (CI/CD), and create an authorization to operate processes that move at an operationally relevant pace.[214]

- **Digital infrastructure.** As recommended by NSCAI,[215] the military needs access to cloud computing and storage;[216] a secure, federated system of data repositories with appropriate access controls; a secure network with the bandwidth needed to support data transport; common interfaces; development environments; and shared development resources that allow commands to quickly access the data, software, and models they need.[217] Such a system must support rapid information collection, improved and accelerated operational analysis, lessons learned distribution, and improved means to ensure that operational lessons are automatically included in operational planning.
- **Trained personnel in the right location, with the necessary authorities.** DoD needs highly skilled personnel at the tactical and operational levels to perform three roles for software-based adaptation: 1) a centralized group of experts to create high-quality software, set standards, perform testing and evaluation when needed, and exercise quality assurance; 2) personnel distributed to operational units to recognize new challenges and opportunities, and

[213] DoD Zero Trust Strategy, U.S. Department of Defense (2022).

[214] SCSP interviews with service members and defense technologists.

[215] Final Report, National Security Commission on Artificial Intelligence at 56-69 (2021).

[216] Department of Defense Software Modernization Strategy, U.S. Department of Defense at ii (2021).

[217] Final Report, National Security Commission on Artificial Intelligence at 56-69 (2021).

to create local versions of new software for testing; and 3) personnel to quickly build and update networks for new capabilities.[218]

- **Continuous integration and continuous delivery.** The U.S. military, with its allies and partners, needs to build mechanisms and processes to continuously deliver software updates in response to unexpected environments, and adversary behavior.
- **Operationally relevant authorization to operate processes.** In recent years, advisory bodies such as the Defense Innovation Board have highlighted the importance of quickly implementing software and building security into the development process, modeling off of successful software processes in the private sector such as Agile and DevSecOps.[219] ATOs are required in order to scale software solutions and integrate them into existing networks. They are necessary for maintaining the security of DoD's systems, but represent one of the most significant bottlenecks in DoD's ability to rapidly develop and field warfighting software.[220] Without movement to help make the software authorization process easier, faster, and more efficient, DoD will not be able to adapt quickly enough to a changing technological environment, and warfighters will not be able to access the cutting-edge software that they need at the tactical edge.

Technology-Enabled Solutions.

- **Automated machine learning (AutoML)** is "the task of automating the process of engineering a 'machine learning pipeline' specifically tailored to a problem at hand, that is, to a dataset on which a (predictive) model ought to be induced. This includes the selection, combination, and parameterization of machine learning (ML) algorithms as basic constituents of the pipeline, which is the main output produced by an AutoML tool, and which can then be used to train a concrete model on the dataset."[221] By automating parts of the ML pipeline, AutoML tools can help accelerate and de-skill some parts of the development process. Doing so will help military units, especially those in field environments, adapt more quickly.
- **Open architecture designs** for equipment, systems, and platforms allow subsystems to be easily and rapidly added, replaced, or upgraded in the field to bring new technical capabilities to force in response to changing missions. Open architecture is particularly applicable to networked environments where it enables modular, configurable fleets of interconnected platforms to exchange data and information irrespective of size and composition.[222] Multinational operations requiring interoperability would also benefit from military equipment built on shared technical standards and protocols of open architecture, which

[218] Justin Lynch, Accelerating Adaptation on the Western Front and Today, Joint Force Quarterly (2021).

[219] Software Acquisition and Practices (SWAP) Main Report, U.S. Department of Defense (2019).

[220] SCSP interviews with service members and defense technologists.

[221] Marcel Wever, et al., AutoML for Multi-Label Classification: Overview and Empirical Evaluation, IEEE Transactions on Pattern Analysis and Machine Intelligence (2021).

[222] Building Open System Architecture for Military Land Vehicles, European Defense Matters at 11 (2016).

provide the functionality and performance of a fully integrated and comprehensive system without sacrificing modularity and flexibility.[223] Once matured and deployed, these designs would shorten technology development cycles, extend the life of systems and platforms, simplify logistics and training, and reduce equipment downtime, manufacturing, and sustainment costs.[224] For example, OpenVPX for embedded computing systems creates an open architecture that allows interoperability of VPX[225] across multiple vendors and products.[226]

[223] Building Open System Architecture for Military Land Vehicles, European Defense Matters at 11 (2016).

[224] Matthew Breen & Eunice Sohn, Questions for the Army's Open Architecture Approach, National Defense (2022).

[225] VPX is a set of standards for connecting components of a computer, typically for defense and aerospace applications. See Dan Taylor, VPX and OpenVPX: A Guide to Major Players, Military Applications, and More, Military Embedded Systems (2022).

[226] Justin Moll, What's the Difference Between VPX and OpenVPX?, Electronic Design (2016).

ANNEX B

Contributors

The SCSP Defense Panel convened two panel meetings this year that included 66 experts, government officials, academic leaders, and many others. The SCSP staff also conducted engagements with leaders from the private sector, academia, civil society, and government. We are grateful for the time and effort of those we have consulted. This report is the culmination of the SCSP staff's work up to this point in its mandate and its effort to synthesize the wealth of information gathered from all of the individuals and entities with whom we have engaged. Although not everyone we have engaged with may endorse this report, we hope it reflects the key points we have learned and charts a path for action.

Audrey Adams
Stephanie Ahern
Lucia Alonzo
Krista Auchenbach
Anthony Bak
Joe Bartlett
Paul Benfield
Erik Berdy
Hal Brands
Colin Carroll
Bryan Clark
Bridge Colby
Thomas Creely
Kim Crider
Mike Dahm
Tony DeMartino
Ryan Farris
Dan Folliard
Brenden Groves
T.X. Hammes
Todd Harrison
S. Clinton Hinote
Frank Hoffman
Frederick Kagan
Kimberly Kagan
Alexander Kott
Sarah Kreps
Dave Kriete
Matt Kroenig
Scott Lacy
Erik Limpaecher
Erik Lin-Greenberg
Joshua Marcuse
Kirk McConnell
Michael McQuade
Frank Miller
Walker Mills
James Mismash
Jim Mitre
Nand Mulchandani
Anu Narayanan
David Ochmanek
Enrique Oti
Kenneth Payne
Eric Redmond
James Ryseff
David Sandson
Mark Seip
Clementine Starling
Joshua Stiefel
James Swartout
Chris Taylor
Brett Vaughan
Rick Waddell
Thomas Walsh
Tim Walton
Becca Wasser
Joshua Watkins
Sean Williams