SPECIAL COMPETITIVE STUDIES PROJECT

DEFENSE

Interim Panel Report

October 2022

Contributors

SCSP LEADERSHIP

Dr. Eric Schmidt, Chair
Ylli Bajraktari, President & CEO

BOARD OF ADVISORS

Michèle Flournoy
Dr. Nadia Schadlow
William "Mac" Thornberry III
Robert O. Work

DEFENSE PANEL

Justin Lynch, Senior Director
Luke Vannurden, Associate Director
Emma Morrison, Research Assistant
Ylber Bajraktari, Senior Policy Advisor

DEFENSE ADVISORS

Christine Fox
Mark Montgomery
Jack Shanahan

SPECIAL CONTRIBUTORS

Greg Grant

The Defense Panel Interim Panel Report (IPR) is the first of six interim reports from the overall work that the Special Competitive Studies Project (SCSP) has conducted over the past year and that was summarized in our Mid-Decade Challenges to National Competitiveness report published on 12 September 2022. This report benefited greatly from insights and expertise by a number of individuals 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, it is not a consensus document of all the experts who assisted.

DEFENSE PANEL INTERIM PANEL REPORT

The Future of Conflict and the New Requirements of Defense

The character of war is changing. Before the end of this decade, the United States and its allies will face a new kind of warfare. The emergence of new, advanced technologies – including artificial intelligence – combined with operational concepts that harness them in innovative and unexpected ways, are creating new ways to apply military force. America's principal rival, China, is determined to harness these changes with the aim of eroding or even leapfrogging the United States' military strengths. Meanwhile, the brittleness of America's defense industrial base, the slow transition in U.S. military capabilities from a small number of exquisite legacy systems to many lower-cost systems, and the struggle to shift from traditional operational concepts compound these challenges and risk strategic exposure for the United States. The stakes could not be higher. If the United States does not rise to this challenge, the consequences could be dire: 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.

The United States should respond neither with despair nor hubris. Throughout history, the American military has demonstrated an ability to develop new capabilities and employ them in new and innovative ways to confound adversaries. Moreover, the United States retains significant military-technological advantages – demonstrated consistently on the battlefield – that it can continue to leverage. Where our military overmatch has been compromised, we can rebuild it. Where our self-confidence has been shaken, we can regain it. But it will require decisive, determined, and durable action to reverse the ongoing erosion of U.S. military advantage.

This Defense Interim Panel Report (IPR) outlines a technology-centered strategic approach for the U.S. military. It starts by describing how the character of conflict has changed and is expected

to change over the next several years. It explains how China aspires to defeat the United States in conflict. It then identifies existing U.S. military-technological asymmetries that the U.S. military can leverage to create advantages that will be difficult for China to quickly duplicate. We conclude by outlining a new competitive strategy – what we term an Offset-X[1] strategy – that lays the groundwork for achieving and maintaining military-technological superiority over all potential adversaries, thwart China's theories of victory, restore America's ability to more freely project power in the Indo-Pacific region, and position the United States to honor its commitments to the stability of the region.

Offset-X is not an operational concept, a war plan, an acquisition wish list, or a research and development blueprint. It is a competitive strategy that seeks to identify some of the critical building blocks that the Department of Defense (DoD) should put in place to achieve and maintain military-technological superiority. We contend that by pursuing the Offset-X strategy, which should form the framework for the next National Defense Authorization Act (NDAA), the U.S. military would be better positioned to outsmart, outpace, outmaneuver, and – as necessary – outgun the People's Liberation Army (PLA).

Changing Conflict and Warfare

New military capabilities, their novel application, and intensifying geopolitical rivalry are changing the character of war and peace at both the strategic and operational level.

At the *strategic* level, we see the following eight dynamics:

> *Persistent conflict below the level of armed clashes.* Repeated acts of aggression by authoritarian governments in China and Russia, often enabled by advanced and emerging technologies, have blurred the line between war and peace. These acts include frequent cyber-attacks, unrelenting disinformation operations, aggressive theft of intellectual property, and sabotage.[2] China stole between $225 billion and $600 billion in 2017 of U.S. intellectual property, a theft of massive scale that has only increased since then.[3] FBI Director Christopher Wray describes the transfer of wealth as the greatest long-term

[1] We refer to the proposed strategic approach as Offset-X to draw an analogy with the past three Offset strategies that the U.S. military pursued from 1950 to 2017 with great results. We chose to use X rather than Fourth Offset to ensure that our proposed actions are viewed as only a partial, not a comprehensive list of actions and whose attainment should be viewed as a temporary achievement that needs further revisions and updating.
[2] 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).
[3] Findings Of The Investigation Into China's Acts, Policies, And Practices Related To Technology Transfer, Intellectual Property, And Innovation Under Section 301 Of The Trade Act Of 1974, Office of the U.S. Trade Representative at Appendix C at 9 (2018).

threat to the U.S. economy.[4] Russian cyberattacks have attacked social cohesion, in what the Office of the Director of National Intelligence describes as "a significant escalation in directness, level of activity, and scope of effort" intended to undermine faith in U.S. democratic processes.[5] Russian saboteurs have also attacked critical infrastructure in the United States and many other countries.[6]

Even if these actions are not kinetic in nature and most are invisible to many Americans, their consequences are significant and leave little doubt that the United States is now in a state of persistent *conflict* with Russia and China. To be sure, sharp conceptual divisions between war and peace, or between traditional and irregular warfare, were of questionable utility when they were written into U.S. joint doctrine.[7] But amid cyber and disinformation attacks, they are an even poorer description of reality today and as such end up stymieing the U.S government's ability to effectively respond to both provocations and real threats. Failing to acknowledge that the above-mentioned attacks are beyond the scope of peaceful competition binds the United States to peacetime patterns of behavior and can limit the menu of options that the U.S. government considers in response. A clear-eyed assessment of these acts of aggression, instead, would focus the efforts of American institutions and galvanize U.S. society towards protecting itself.

The individualization of war. The proliferation of sensors; the data exhaust that individuals leave on the Internet through everyday searching, reading, watching, shopping, and dating habits; the bulk collection of DNA and biometrics; and the speed with which AI-enabled systems can analyze vast amounts of harvested data allow militaries to micro-target individuals. Microtargeting is likely to entail denigration campaigns and psychological pressure, but under certain circumstances could also entail targeting of key individuals with biological warfare, traditional targeted killings, or even global strike platforms. As we have seen in the Ukraine war, the Ukrainians have effectively and repeatedly tracked and targeted Russian military leaders.[8] The effects can be delivered on the battlefield, close to it, or away from it.

---

[4] The Editorial Board, American is Struggling to Counter China's Intellectual Property Theft, Financial Times (2022) (citing FBI Director Christopher Wray's Opening Remarks: China Initiative Conference, Center for Strategic and International Studies (2020)).

[5] Assessing Russian Activities and Intentions in Recent US Elections, U.S. Office of the Director of National Intelligence at ii (2017).

[6] Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide, U.S. Department of Justice (2022); Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure, Cybersecurity and Infrastructure Security Agency (2022).

[7] Joint Publication 1: Doctrine for the Armed Forces of the United States, U.S. Department of Defense Joint Staff at I-5 - I-7 (2017).

[8] Julian E. Barnes, et al., U.S. Intelligence Is Helping Ukraine Kill Russian Generals, Officials Say, New York Times (2022).

The Individualization of war presents great threats to peacetime and crisis decision-making, but may also contribute to disrupting large-scale combat operations. Combatants can identify and target key leaders, action officers, contractors, and analysts with the intent to damage the U.S. military's ability to plan and execute complicated operations. While it is unlikely that doing so would cause U.S. operations to halt, it would significantly increase friction, potentially desync operations, and allow adversaries to gain a significant tactical advantage. While individual targeting is not new, the scale, precision, and speed at which individuals can be targeted is. Prior to recent advances in AI,[9] it would have been extremely difficult to use data to identify and micro-target a large number of individuals simultaneously at such a scale.

This individualization of war could change the psychology of war. On one hand, it creates the possibility of war with fewer casualties. On the other hand, the reach of new tech-enabled systems means that individual combatants, leaders, and even their family members are more easily targetable. U.S. service members, commanders, and policymakers will find themselves operating under persistent, individualized threats.

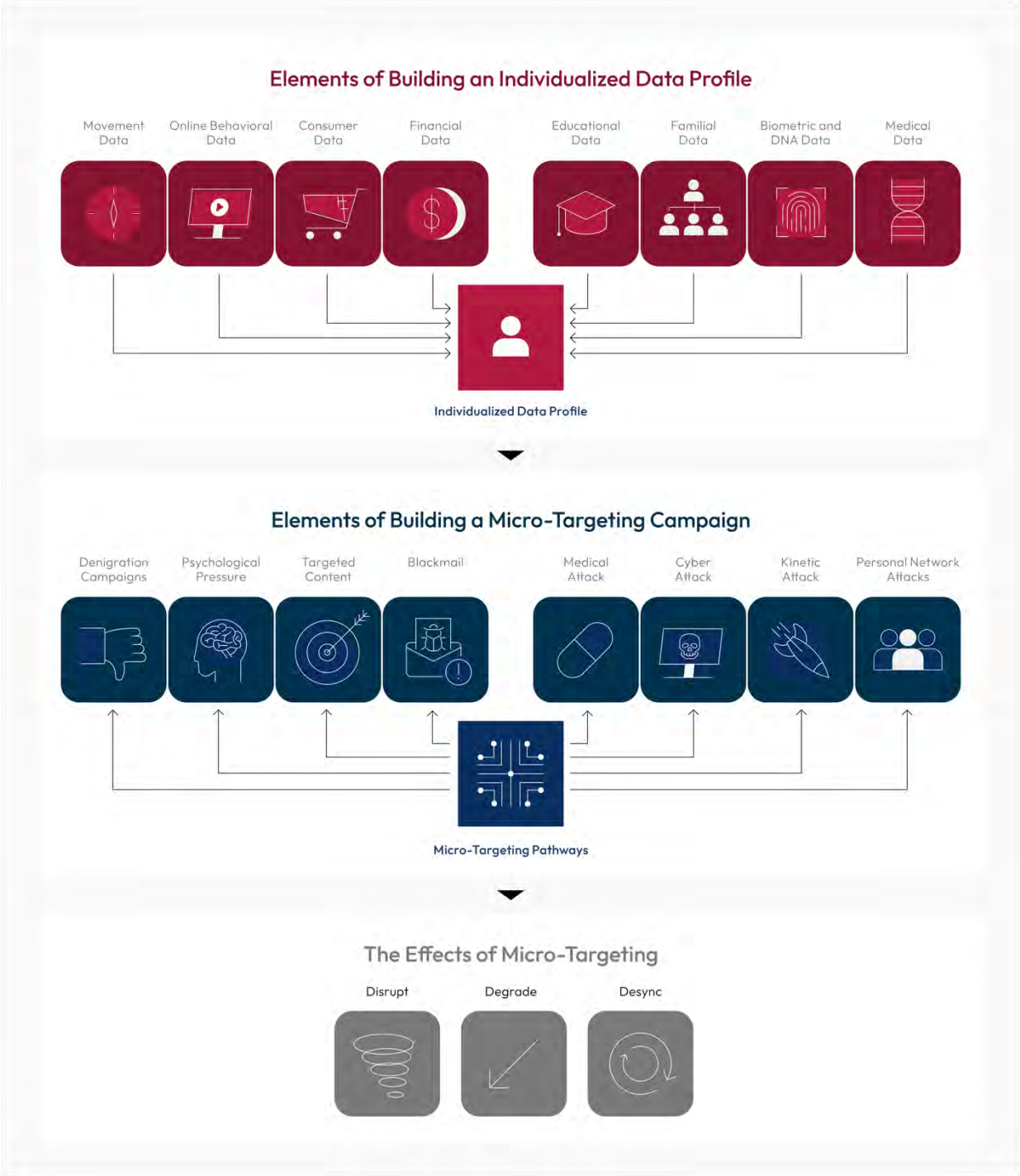
Individualization of war will also come about through further empowerment of individuals and small units who will be forward deployed in the theater of operations and have at their disposal, sometimes remotely, increasingly more sophisticated technologies to deliver tactical or even strategic effects. Individual service members are increasingly in control of a suite of kinetic or cyber strike platforms, whether organic to the unit or able to be called upon to conduct an attack. As synthetic biology advances, more people can create pathogens, either from synthetic or naturally occurring DNA.[10] And by expanding the power of individuals, technology will increase uncertainty about which actions are taken by a state, by those acting on behalf of a state, or by those acting on their own. This uncertainty around attribution is already seen clearly in the cyber domain.[11]

[9] For more discussion on AI-enabled micro-targeting, please see "Chapter 1: Emerging Threats in the AI Era" of report by the National Security Commission on Artificial Intelligence. https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf

[10] Benjamin Wittes & Gabriella Blum, The Future of Violence: Robots and Germs, Hackers and Drones, Basic Books at 311-352 (2015).

[11] Herbert Lin, Attribution of Malicious Cyber Incidents, Hoover Institution at 44-46 (2016).

The Individualization of War



The likelihood of war between great powers is rising. There is a somewhat common expectation and (mis)perception that great powers, particularly those that are economically entangled, do not fight each other anymore and that the cataclysmic wars of the first half of the twentieth century are firmly and exclusively in humanity's past.[12] However, the blurring of lines between war and peace, acts of aggression by China and Russia, intensifying geopolitical rivalries, the emergence of disruptive emerging technologies, and the high stakes involved in these rivalries increase the risk of major war for the United States.

The risk of war between great powers has increased in part because the threat of and actual instances of seizure of neighboring territory by force by great powers has reemerged. In 2008, Russia seized parts of Georgia. In 2014, Russia seized Crimea and parts of the Donbas region in Ukraine.[13] This year, Russia launched an even broader war of aggression against Ukraine. Meanwhile, China built and militarized artificial islands in the international waters of the South China Sea despite its public promises to the contrary,[14] engages in provocations in the East China Sea,[15] repeatedly violates Taiwan's air defense identification zone,[16] and refuses to rule out taking over the island by force.[17]

Emerging and disruptive technologies are also fueling the rise in risk of war between great powers, particularly in the cyber and space domains. Unlike traditional forms of kinetic actions, emerging technologies are not yet clearly addressed in international obligations and do not provide the same context for the drawing of red lines and the escalation that may follow.[18] In the cyber and space domains, these red lines may be misunderstood, are not fully established, or blatantly not adhered to – leading states to test the limits and resolve of their competitors in unfamiliar situations.

A modern great power war could be unlike anything Americans have ever experienced. For many contemporary Americans, war has been something that happens elsewhere – IEDs and ambushes on a desert road in the Middle East, warfare in eastern European cities and fields, and firefights in jungles an ocean away. When U.S. forces are involved, the

[12] Azar Gat, War in Human Civilization, Oxford University Press (2006); Stephen Pinker, The Better Angels of our Nature, Penguin Books (2012); Robert Jackson, Quasi-States: Sovereignty, International Relations and the Third World, Cambridge University Press (1993).
[13] Peter Dickinson, The 2008 Russo-Georgian War: Putin's Green Light, The Atlantic Council (2021).
[14] Center for Preventative Action, Territorial Disputes in the South China Sea, Council on Foreign Relations Global Conflict Tracker (2022).
[15] Center for Preventive Action, Tensions in the East China Sea, Council on Foreign Relations Global Conflict Tracker (2022).
[16] Zubaidah Abdul Jalil, China sends 30 Warplanes into Taiwan Air Defence Zone, BBC News (2022).
[17] Chris Buckley & Sui-Lee Wee, China Won't Hesitate to Fight for Taiwan, Defense Minister Warns, New York Times (2022).
[18] Joseph S. Nye, Will Biden's Red Lines Change Russia's Behaviour in Cyberspace?, Australian Strategic Policy Institute (2021).

expectations have grown that there will be fewer and fewer casualties than in past conflicts.

Today's technology, operational concepts, and strategic rivalries risk changing that. A war between two or more great powers could take place at a much greater scale and higher level of intensity than any previous wars. The national resources available on both sides would be unprecedented. The facets of society that such a war would touch could be all-encompassing. Unlike in recent wars, the United States would face the threat of large-scale cyber-attacks on the homeland that could paralyze society, the disablement or destruction of space-based assets that underpin the economy and military operations, and even missile strikes on U.S. soil that could destroy civilian and military headquarters.

Great power wars have the potential to devolve into prolonged contests that place a high premium on the strength of the industrial base, innovation ecosystem, and political will. Knockout blows, decapitation strikes, and decisive battles are often aspired to, but rarely materialize in wars between great powers. Instead, great powers are able to mobilize populations and resources in ways that cause wars to descend into long, grinding contests, in which political will and national resources play as large (or larger) a role as brilliant operational maneuver and deception. However, most Western economies – the United States included – lack the indigenous industrial capacity to rapidly replenish and sustain their forces. This includes the production of the necessary munitions, sensors, vessels, vehicles, and aircraft, possibly for months or even years into a conflict, as well as skilled personnel to produce and operate them. The brittleness of the defense industrial base can become a serious strategic liability for the United States in a great power war, presenting U.S. decision-makers with a tough dilemma of potentially having to escalate vertically.

In addition to the resilience of the industrial base, the vibrancy and responsiveness of the innovation ecosystem to conflict requirements will also be key in prolonged war scenarios. Quickly identifying the requirements, and then repurposing or developing new technologies and platforms could shift the tactical tide of war and prove to be of strategic importance. Finally, the industrial base and the innovation ecosystem, while necessary, are not sufficient. They are no substitute for political will to endure and persevere in a high-intensity and prolonged conflict.

Critical national infrastructures are vulnerable to cyber-attacks and are already being targeted.[19] Many critical sectors of American society and economy are heavily reliant on digital systems, software, and Internet connectivity that are not sufficiently secure; 2021

[19] 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).

witnessed 649 reported incidents of ransomware attacks on entities within critical infrastructure sectors.[20] This ever-expanding area of attack and its indispensable role make critical infrastructure an attractive target for offensive cyber-attacks. A large-scale attack would present serious challenges for our socio-economic functioning and ability to wage war.

The use of nuclear weapons cannot be discounted. As losses mount, as they may in a war in Eastern Europe or the Western Pacific, some nuclear powers may be tempted to use nuclear weapons to deter or compel, offset significant losses, or resolve attritional warfare. Other nuclear powers may threaten to use them even before losses mount, as a way of deterring the United States and its allies from getting involved in the conflict.

Recent actions by Russia and China signal the returning significance of nuclear weapons to their defense and foreign policies. The threat of nuclear escalation in Ukraine is one of several factors inhibiting broader intervention in Ukraine by other European states or the United States.[21] China is also expanding its nuclear weapons platforms at a scale unseen since the Cold War.[22] It is likely that the CCP views nuclear weapons as very salient for its ability to deter the United States from directly intervening in a conflict over Taiwan, in the East or South China seas, or in other potential scenarios.

Adversaries' applications of emerging technologies may not be ethically constrained. As new technologies are adopted, U.S. military operations will continue to be guided by U.S. and international laws as well as the Department of Defense's regulations and ethical guidelines. In addition, the DoD has also clearly established robust internal processes through which it runs new weapons and emerging technology systems for testing, evaluation, and adoption, including legal review.

However, America's adversaries may not necessarily be guided by similar principles, as we see with the appalling actions of the Russian military in Ukraine and Syria.[23] While China has not yet engaged in wars that have included emerging technologies, in a domestic law enforcement context their approach to indiscriminate data collection and the targeting of civilian populations in Xinjiang province raises fundamental concerns.[24] China, in contrast to the U.S. military,[25] has also not disclosed the existence or content of any

[20] 2021 Internet Crime Report, Federal Bureau of Investigation at 15 (2021).
[21] Gustav Gressel, Shadow of the Bomb: Russia's Nuclear Threats, European Council on Foreign Relations (2022).
[22] Military and Security Developments Involving the People's Republic of China, U.S. Department of Defense at VIII (2021).
[23] Sebastien Roblin, What Happened When Russia Tested Its Uran-9 Robot Tank in Syria, The National Interest (2021).
[24] Break Their Lineage, Break Their Roots, Human Rights Watch (2021).
[25] As an example, DoD published Department of Defense Directive 3000.09, addressing autonomy in weapon systems. See DoD Directive 3000.09, Autonomy in Weapon Systems, U.S. Department of Defense (2012).

regulations or policy directives that indicate how it intends to use emerging technologies in military operations in an ethically and legally-responsible way.

While the U.S. military should continue to follow all laws of war and established principles for its application of emerging technologies, it should not assume its adversaries will do the same – and it should be mindful of the advantages and disadvantages these differences create. This discrepancy in constraints around the application of emerging technologies may still enable the United States to claim the moral high grounds, but tactically – and possibly strategically – the military initiative could rest with the adversaries that opt to disregard ethical and legal considerations.

At the more *operational* level, we see the following four dynamics:

Emerging technologies are qualitatively changing the way we perceive our environment, communicate, and make decisions. Mass data generation and collection, behavioral tracking, commercial imagery, step-changes in intelligence fusion, and algorithms to analyze them are increasing the availability of data for decision-making, giving policymakers and military leaders much greater awareness. The application of AI and human-machine collaboration to this data will bypass many of the constraints imposed by human limitations, and accelerate, diffuse, and compress decision-making to such an extent that at times it will seem almost instantaneous. AI can identify novel patterns and generate unique insights by examining massive, many-dimension data sets and discovering patterns humans cannot perceive.

Militaries that change their processes and establish effective, integrated systems to take advantage of large data sets and emerging technologies can dominate the observe, orient, decide, act (OODA) loops[26] by reaching speeds and scale that are impossible through analog processes. The proliferation by type, number, and domain of sensors is helping militaries *observe* adversaries more quickly, in all phases of combat operations, including preparatory, and across the operating environment. Artificial intelligence then helps militaries *orient* themselves by fusing and making sense of the data from proliferated sensors. AI-enabled decision aids then help humans *decide* more quickly, and sometimes make decisions on their own under human supervision. Data-driven decisions also have a stronger empirical basis, improving their quality. Failure to adapt these technological aids, however, runs the risk of information overload, delayed decision-making, or even paralysis in decision-making.

Emerging technologies will make it increasingly difficult for military (and civilian) decision-

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

makers at all levels to distinguish truth from falsehood, possibly to strategic consequence. Manipulation and deception have always been part of warfare, but emerging technologies will likely take these dynamics to a new level. At the strategic level, deep fakes and other AI-enabled deception technologies will enable adversaries to develop increasingly sophisticated falsehoods that could span multiple days, or even weeks, and threaten to significantly derail military campaigns, feed false information or uncertainty into strategic planning processes, and undermine the national will to fight.

For military operations, the ability to hack and manipulate data links, intelligence, surveillance, and reconnaissance (ISR) platforms, or force trackers will allow adversaries to deceive with the goal of leading the U.S. military astray, fatally disrupting or derailing ongoing operations, and injecting uncertainty about the validity of reports, intelligence analysis, or performance of vital systems. Even when militaries have deep fake detectors, leaders will have to doubt the reports they receive, and their understanding of the world around them. Leaders that cannot determine the truth cannot fight effectively.

As human-machine collaboration and human-machine teaming become more common, so will the risk that adversaries can exploit the interfaces that enable human-machine interactions, undermining the human operator's trust in the machines, causing the United States and our allies and partners to be led astray or even paralyzed. Ensuring the integrity of interfaces between humans and machines will be paramount. Likewise, validating the authenticity of incoming information will be critical to maintaining uncorrupted situational awareness and the ability to make accurate tactical, operational, and strategic decisions.

The growing importance of software and connectivity to military operations will accelerate the adaptation of tactics and technology. Historically, adaptation in military operations has taken place when individuals or small teams transmitted lessons learned to a higher headquarters, and the headquarters then disseminated the lesson to other units, which re-trained their personnel and adopted the changes into their doctrine or directly into their tactics, techniques, and procedures.

Software, on the other hand, can be updated and adapted much more quickly. Lessons learned and software-based upgrades can be incorporated as quickly as programmers develop, transmit, and download new software. This allows software-based adaptation to bypass many of the physical, bureaucratic, and behavioral constraints of traditional adaptation. Over time, the combination of human expertise and self-learning machines will allow extremely rapid changes to military options. As one example, DARPA is experimenting with AI-enabled wargaming called Constructive Machine-Learning Battles

with Adversary Tactics (COMBAT)[27] that generate models of adversary behaviors that challenge and adapt to the U.S. military in simulated experiments. AI-enabled apps will likely continue to shape and generate tactics and operating concept options for humans to consider.

Militaries that collect useful data, quickly draw lessons, and integrate updates into their software more quickly than their competitors will have a marked advantage. Militaries will also benefit from denying their adversaries the ability to collect helpful data or use their software.[28]

The proliferation of sensors,[29] *analytical tools, precision-guided munitions,*[30] *and non-kinetic payloads (i.e., cyber, directed energy) are fundamentally altering the hider-finder contest.* As sensors and analytical tools continue to develop and proliferate, it will become increasingly difficult to hide in every domain, including space and undersea that have traditionally been the most opaque. Longer range platforms, proliferated precision-guided munitions, and distributed operations centers allow militaries to significantly compress the detection-to-destruction timeline, allowing them to strike the targets they detect almost instantaneously. If adversaries more easily detect and rapidly destroy opposing forces, especially while they are on the move, it will be difficult to employ operational surprise or tactics that rely on large formations consolidating or maneuvering, generally a key component of decisive victories.

This trend will also increase the probability of detection and attribution of preparations for war, potentially buying more time for deterrent efforts. But it will also drive a temptation for preemption, out of desire to blind or immobilize the enemy, particularly in cases of predictive intelligence. Restoring operational maneuver will require either subverting or overcoming adversary sensors, finding ways to restore the ability to surprise, or employing low-cost, attritable systems as part of an initial phase of operations to pave the way for subsequent attacks by regular formations.

[27] Paul Zablocky, COnstructive Machine-learning Battles with Adversary Tactics (COMBAT), Defense Advanced Research Projects Agency (last accessed 2022).
[28] Justin Lynch, Yet Another Article About Information Technology and the Character of War, War on the Rocks (2020).
[29] Nishawn S. Smagh, Intelligence, Surveillance and Reconnaissance Design for Great Power Competition, Congressional Research Service at 5, 7 (2020).
[30] John R. Hoehn, Precision-Guided Munitions: Background and Issues for Congress, Congressional Research Service at 6-25 (2021).

Early Observations of the War in Ukraine. The Russian government planned for the invasion of Ukraine to be a quick seizure of Kyiv, decapitation of President Zelensky's government, and creation of a pro-Kremlin puppet government.[31] That initial plan failed catastrophically. The Russian political and military leadership made a series of erroneous strategic and planning assumptions, relied on faulty intelligence, underestimated Ukrainian will and skills to fight,[32] and overestimated the effectiveness of their forces, especially for the unfolding changes in character of conflict. The Russian government also underestimated U.S.-led Western resolve and unity.

Ukrainian leadership and forces, on the other hand, proved much more resilient, frequently outsmarting and outmaneuvering Russian forces, thwarting their attempts to establish air supremacy, control the sea lanes, and seize strategic terrain. The Ukrainians effectively leveraged their informational upper-hand, mobilized much of their population to help the war effort through direct participation or via apps and messaging services, relied on distributed, network-based operations to outmaneuver Russian forces, utilized portable anti-tank and anti-aircraft missiles to blunt the Russian onslaught, and used drones and loitering munitions to bog down and attrit Russian forces.[33] The Ukrainian government also conducted a highly effective information campaign, garnering sympathy in the West and debunking Russian disinformation.

Militaries in every part of the world are likely observing the war in Ukraine to understand what the war may indicate about the future of conflict. Several phenomena can be understood using a theater-level battle networks framework:[34]

- *Command, control, communications, computers, and intelligence grid:* As the war began, the Ukrainian government moved to store critical government data in the cloud, transferring them from vulnerable government servers in Kyiv to the safety of cloud servers. The Ukrainian government, at the same time, worked with private companies and allied governments to thwart or defend against cyberattacks.[35] The Ukrainian

[31] Steven Pifer, The Russia-Ukraine War at Three Months, Brookings Institution (2022).
[32] Lucian Kim, Putin's Colossal Intelligence Failure, The Kennan Institute (2022).
[33] The First Networked War: Eric Schmidt's Ukraine Trip Report, Special Competitive Studies Project (2022). Gillian Tett, Inside Ukraine's Open Source War, Financial Times (2022).
[34] William T. Eliason, An Interview with Robert O. Work, Joint Force Quarterly (2017).
[35] Ryan White, How the Cloud Saved Ukraine's Data from Russian Attacks, C4ISRNet (2022); Brad Smith, Defending Ukraine: Early Lessons from the Cyber War, Microsoft (2022).

government also successfully partnered with SpaceX and its founder, Elon Musk, to acquire thousands of Starlink terminals, providing Ukrainians with secure, reliable internet access.[36]

- *Sensor grid:* With their data and connectivity secured, the Ukrainian government was able to utilize a government app used by much of its population, and a Swiss-developed secure messaging service to receive from its people battle damage assessments, reports of casualties, and the position of enemy forces.[37] The Ukrainian military then used artificial intelligence to verify and process the information, and integrate it into targeting. With the combination of these technologies and the C4I grid, Ukrainian armed forces maintained their ability to understand their environment, communicate, and make decisions far more effectively than they would be able to otherwise.[38] In other words, this digital *levee en masse* made Ukrainian sensors far more ubiquitous relative to that of the Russian forces, dramatically improving their awareness.

- *Effects grid:* Several noticeable trends have emerged in the Ukrainian effects grid. First, drones have become an important component of Ukrainian long-range precision fires by both finding and finishing Russian forces. Ukrainian forces have shown an astounding degree of effectiveness in using relatively inexpensive drones and loitering munitions, sometimes even hacking them to reconfigure their performance.[39] Drones had already played a prominent role in the 2020 Nagorno-Karabakh War by providing Azerbaijani forces an aerial advantage against Armenian armor.[40] In Ukraine, drones played a similar role during the first phase of war,[41] while loitering munitions have helped Ukrainian forces destroy light and armored targets cheaply from afar.[42] Both conflicts have challenged the role that armor has traditionally played on the battlefield. As drone use in combat continues to advance and as autonomy improves, these systems will continue to change warfare further. Second, more traditional long-range precision fires, such as those provided by High Mobility Artillery

[36] Vivek Wadhwa, How Elon Musk's Starlink got Battle Tested in Ukraine, Foreign Policy (2022).
[37] Gillian Tett, Inside Ukraine's Open Source War, Financial Times (2022).
[38] For more insights regarding technology's impact in Ukraine, see Eric Schmidt & Ylli Bajraktari, AI and National Security Report, Cyber Media Forum: Project for Media and National Security, George Washington School of Media and Public Affairs at 3-5, (2022).
[39] Tim Mak, From Warehouses to the Front Lines, National Public Radio (2022).
[40] Shaan Shaikh & Wes Rumbaugh, The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense, Center for Strategic and International Studies (2020).
[41] Jack Detsch, Drones Have Come of Age in the Russia-Ukraine War, Foreign Policy (2022).
[42] David Hambling, Failure or Savior? Busting Myths About Switchblade Loitering Munitions in Ukraine, Forbes (2022).

Rocket Systems (HIMARS), have helped Ukraine disrupt Russian supply lines and depots, especially for ammunition, laying the groundwork for Ukrainian counteroffensives.[43] Such systems are even more effective when partnered with Ukraine's crowd-sourced intelligence and creative use of drones for intelligence, surveillance, and reconnaissance. Third, the acquisition by Ukraine of portable, easy to use anti-tank, anti-aircraft, and anti-personnel weapons has enabled its light infantry units to defend against superior Russian armor,[44] helicopters,[45] and other platforms. These changes to effects, and the NATO training provided prior to the invasion,[46] has enabled the Ukrainian forces to operate in smaller, distributed, but empowered and networked formations against a much more rigid, and hierarchical Russian invading force.

- *Logistics and support grid:* Large-scale combat operations are qualitatively different and far more logistically challenging than smaller military operations, especially when fought against a well-trained, disciplined military. When Russia seized Crimea in 2014, the majority of operations in Ukraine were carried out by a small number of professional, well-trained soldiers, and Ukrainian forces provided little resistance.[47] By contrast, Russia's initial invasion force in 2022 had roughly 190,000 troops.[48] Despite their success in 2014, Russia's poorly supported supply units and weak non-commissioned officer corps left it unable to support larger maneuvers and formations in 2022. Russian troops quickly overwhelmed their supply lines, leaving them without enough fuel, food, or munitions to fight effectively.[49]

The People's Liberation Army's Theory of Victory to Defeat the U.S. Military

Over the last several decades, the United States has relied on Second Offset capabilities, such as superior intelligence collection platforms, battle networks, and precision-guided and stand-off

[43] C. Todd Lopez, U.S.-Provided HIMARS Effective in Ukraine, U.S. Department of Defense (2022).
[44] Ari Shapiro, et al., Retired Colonel on the Rise of Javelin Missiles, as Biden Seeks to Aid Ukraine, National Public Radio (2022).
[45] Mike Stone, U.S. Buys More Stingers After Missiles' Success in Ukraine, Reuters (2022).
[46] Jim Garamone, Training Key to Ukrainian Advantages in Defending Nation, U.S. Department of Defense (2022).
[47] Michael Kofman, et. al, Lessons from Russia's Operations in Crimea and Eastern Ukraine, RAND Corporation (2017).
[48] Mark Cancian, Russian Casualties in Ukraine: Reaching the Tipping Point, Center for Strategic and International Studies (2022).
[49] Michael Kofman and Rob Lee, Not Built for Purpose: The Russian Military's Ill-Fated Force Design, War on the Rocks (2022).

munitions, to defeat adversaries. As adversaries develop precision-strike regimes, the U.S. and NATO ability of faster, more effective maneuvering to realize military victory has diminished. Instead, warfare between great powers will increasingly see the confrontation of systems of sensors, networks, effects, and logistics.

For over two decades now, the PLA has closely studied the "American way of war" of guided munitions-battle networks warfare, which they refer to as informatized warfare, and has worked relentlessly to adopt it for its own purposes.[50] But the PLA has not only sought parity with the U.S. military in this regard. It has also developed a theory of victory centered around the idea of systems confrontation, whereby it would seek to destroy the battle networks of its adversaries, like the United States has done since Desert Storm, which the PLA refers to as operational systems. This *system destruction warfare* 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. PLA planners believe that immobilizing critical junctions in an opponent's operational systems will isolate subsystems from critical resources and decrease overall system effectiveness.[51] In short, they believe that military-technological parity in precision guided munitions-battle networks, and the application of their operating concept of system destruction warfare can lead them to military victory.[52]

In pursuit of a theory of victory for a potential confrontation today, the PLA has also sought to chart a path to leapfrog the United States for a potential confrontation of tomorrow. The PLA intends to capitalize on the growing capabilities of AI, big data, advanced computing, 5G, and supporting technologies to shift from informatized warfare to *intelligentized* warfare. By becoming the first movers in a new way of war, they hope to leapfrog the United States and become the world's dominant military power. Intelligentization includes seven trends: (1) shift from the strong beating the weak to the intelligent beating the dull, (2) from destructive power to manipulating cognition, (3) from human-based to human-machine collaboration, (4) from big eats small to fast eats slow, (5) from winning through integration to winning through clusters, (6) from military dominance to hybrid warfare, and (7) from practical test to experimental exercise.[53]

The PLA's weapons platforms and capabilities are also of increasing concern. The PLA has amassed a formidable, ever-expanding arsenal of medium- and long-range precision missiles,

[50] Rush Doshi, The Long Game: China's Grand Strategy to Displace American Order, Oxford University Press (2021).
[51] 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). 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.
[52] Ryan Fedasiuk, et al., Harnessed Lightning: How the Chinese Military is Adopting Artificial Intelligence, Center for Security and Emerging Technology at 38 (2021).
[53] Xie Kai, Zhang Dongrun, and Liang Xiaoping, A Perspective on the Evolution of the Winning Mechanism of Intelligent Warfare, China Military Network - PLA Daily (2022).

including hypersonic missiles, capable of striking U.S. land and sea bases throughout the region and delaying or even preventing the United States from rapidly intervening in a crisis.[54] The PLA has built a dense web of integrated air defense systems to challenge U.S. forces attempting to enter the theater of operations,[55] as part of its robust anti-access/area denial (A2/AD) efforts. The PRC also created the Strategic Support Force to merge information operations, including cyber, psychological operations, electronic warfare, and some space operations in an effort to operationalize system destruction warfare.[56] In total, 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 region, or once there, to enjoy freedom of movement and action.

U.S. Asymmetric Strengths that Offer Opportunities for Advantages

While the magnitude of today's challenges may be new, this is not the first time U.S. military primacy, its ability to project power, or its commitment to allies and partners have been called into question. Moreover, the U.S. military still enjoys considerable operational and military-technological asymmetries that can be leveraged against China. These and other asymmetries are the product of traits that are difficult to replicate, such as democratic institutions. Using those asymmetries to shape how the United States deploys and employs capabilities will make it difficult for the PRC to replicate U.S. performance, even if it reproduces the underlying technology.

Demonstrated Experience in Joint, Combined Arms, Expeditionary, and Networked Operations. Combined arms operations are highly complex and demanding, but are necessary for achieving quicker military victory, especially against sophisticated adversaries.[57] Militaries that cannot conduct joint operations struggle to establish domain supremacy and project their influence outside of their region.

Twenty years of combat in Afghanistan and Iraq, along with demanding rotations at Combat Training Centers, Fleet Training Exercises, and Red Flag exercises have rendered these inherently complex operations familiar to the U.S. military.[58] The PLA lacks the experience, trust, and cross-

[54] Christopher Mihal, Understanding the People's Liberation Army Rocket Force: Strategy, Armament, and Disposition, Military Review (2021).
[55] Derek Solen, PLA Army Air Defense Units Improve Effectiveness, Resiliency, and Jointness, China Aerospace Studies Institute (2021).
[56] John Costello & Joe McReynolds, China's Strategic Support Force: A Force for a New Era, National Defense University (2018).
[57] Stephen Biddle, Military Power: Explaining Victory and Defeat in Modern Battle, Princeton University Press at 28, 35 (2006).
[58] See e.g., Terri Moon Cronk, U.S. Forces Work With Partners in Numerous Military Exercises, U.S. Department of Defense (2017).

domain communication needed to effectively conduct joint and combined operations.[59] It has, however, recognized these shortcomings and placed a high priority on making improvements.[60]

Empowering Warfighters at the Lowest Tactical Levels. Individual and small unit initiative is critical in modern warfare, and increasingly so as the character of conflict continues to evolve. Militaries operate in environments characterized by high levels of uncertainty and a great degree of unpredictability that higher headquarters are hard pressed to track and quickly respond to. Under these circumstances, the ability of forward deployed units to adapt in order to execute the commanders' intent in changing circumstances is an imperative.[61] Just as importantly, tactics and technology will change quickly during war. Top-down guidance alone cannot drive the adaptation needed. Commanders in all domains must understand their opportunity space, generally how to develop new or employ differently existing capabilities, and the tactics needed to use them.[62] All of this requires empowerment at low levels.[63] The U.S. military better empowers its forces at the lowest level to take advantage of operational initiative and develop new solutions to fast-changing battlefield dynamics.[64] The rigid structures of the PLA, and the conformist nature of its communist political system and society, typically do not promote or reward tactical initiative and rapid adaptation.[65]

Expeditionary Logistics. 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. This stands in stark contrast to the Russian military, which has struggled to provide logistical support for its forces in Ukraine.[66]

However, since World War II, trans-continental and trans-regional logistics operations by the U.S. military have taken place in uncontested settings, often relying on commercial contractors to move assets and forces in a lengthy and unchallenged buildup process. By contrast, a 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. Such attacks could thwart the United States'

[59] 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).
[60] Military and Security Developments Involving the People's Republic of China, Annual Report to Congress, U.S. Department of Defense at 158 (2021).
[61] Joint Operating Environment: The Joint Force in a Contested and Disordered World, U.S. Department of Defense Joint Staff at 40 (2016).
[62] Frank Hoffman, Mars Adapting: Military Change During War, Naval Institute Press at 248-252 (2021).
[63] Joint Operating Environment: The Joint Force in a Contested and Disordered World, U.S. Department of Defense Joint Staff (2016).
[64] Mission Command: Insights and Best Practices Focus Paper, U.S. Department of Defense Joint Staff, Deployable Training Division at 3 (2020).
[65] Mark Cozad, Toward a More Joint, Combat-Ready PLA, National Defense University Press (2019).
[66] Jim Garamone, Ukrainian Resistance, Logistics Nightmares Plague Russian Invaders, U.S. Department of Defense (2022).

ability to maintain the flow of supplies to a complex conflict abroad, particularly if the U.S. military has not prepositioned sufficient materiel and forces in advance of a crisis. 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,[67] in addition to having the advantage of proximity to the potential theater of operations.

Allies, Partners, and Global Posture. The United States has far more and much deeper alliances and partnerships than China, which has only one formal alliance, North Korea.[68] This advantage would enable the United States to generate greater diplomatic legitimacy, build military mass, create broader and deeper multi-domain effects, attack from different axes, and coordinate intelligence across a much larger network. The strength of U.S. alliances enables a high degree of cooperation globally as exemplified by the multi-nation sanction response to the Russian invasion of Ukraine.[69] China would struggle to generate cooperation to this degree, though it may be able to keep a considerable number of countries sitting on the fence.

The U.S. military's expeditionary capabilities and consistent forward presence in key regions, particularly astride critical global choke points, further strengthen the U.S. global posture,[70] and diversity of response options. This makes it easier for the United States to rapidly deploy capabilities, employ military assets and forces, and sustain expeditionary logistics. At the same time, the United States military must be prepared for the possibility that not all allies or partners would join in a potential conflict with China, or even allow U.S. military forces to operate from their territories. Developing in peacetime a more precise understanding of which nations may or may not grant U.S. access during wartime and identifying those which are essential to U.S. military operations is essential to mitigating some of the operational risks.

The Strengths of a Democratic Society. Individual freedoms and empowerment – characteristic of democratic societies – foster innovation, entrepreneurship, and initiative. This makes the United States more resilient, agile, and more likely to adapt successfully to changing conditions. This empowerment of the individual and encouragement of initiative is also reflected in the U.S. military services.

---

[67] Chad Peltier, China's Logistics Capabilities for Expeditionary Operations, Jane's at 4 (2020).
[68] Charles Parton & James Byrne, China's Only Ally, Royal United Services Institute (2021).
[69] FACT Sheet: Joined by Allies and Partners, the United States Imposes Devastating Costs on Russia, The White House (2022).
[70] Michael Tanchum, China's New Military Base in Africa: What it Means for Europe and America, European Council on Foreign Relations (2021); Hal Brands, America and China Are in a Global Fight Over Military Bases, Bloomberg (2021); Where Are U.S. And Russian Military Bases In The World, RadioFreeEurope (2015).

The United States also does not suffer from several authoritarian pathologies that appear to have plagued the Russian military,[71] and the Iraqi military before that,[72] and may also hinder the effectiveness of the PLA. The United States has deliberately pursued and built a professional and apolitical military force, which stands in stark contrast to the PLA. The PLA has a long history of corruption and coup-proofing.[73] Both tendencies lead to promotions based on political loyalty rather than competency, a lack of trust in junior leaders, a lack of tactical initiative, an aversion to speaking truth to power, and ineffective decision-making due to less candid discussion during the planning process.[74] They also contribute to the wasting of resources, and uncertainty in performance during conflict. These political constraints lead militaries to struggle to perform in chaotic conditions and during communication breakdowns, or to make significant, on-the-fly adjustments during combat missions. Phrased differently, in the Chinese system, regime security overrides national security.[75] Authoritarian state stability also relies on near total control, not resiliency. Finally, China's long-time pursuit of the one child policy weakens its military strength.[76] While the PLA will not necessarily suffer a shortage of military personnel, any contingency that results in casualties will also cause many families to lose their only child, resulting in demoralization of the population and, possibly, political blowback.

From Asymmetries to Advantages: An Offset-X Strategy

As we look towards 2025-2030, a war between great powers is more likely than it has been in generations. Emerging technologies are impacting the way militaries understand their environment and make decisions. Some of these same technologies will continue to change the tools of war, operational concepts, and how violence can be employed for political outcomes. While combat in traditional domains will likely play a significant role, warfare will also be waged with and against industrial and financial power, pitting national innovation ecosystems, across continents and borders, and will be determined by political will as much as any other single factor.

Over the last several decades, the United States has relied heavily on its superior intelligence collection assets, stand-off platforms, precision-guided munitions, highly-trained and tactically empowered personnel, and expeditionary operations and logistics to defeat adversaries. But advanced and emerging technologies are changing the reliability and effectiveness of these systems. Moreover, adversaries have developed some of the same capabilities, invested heavily

[71] Sam Cranny-Evans & Olga Ivshina, Corruption in the Russian Armed Forces, Royal United Services Institute (2022).
[72] Erica De Bruin, Coup-Proofing for Dummies, Foreign Affairs (2014).
[73] Dennis J. Blasko, Corruption in China's Military: One of Many Problems, War on the Rocks (2015).
[74] Thomas Carothers & David Wong, Authoritarian Weaknesses and the Pandemic, Carnegie Endowment for International Peace (2020).
[75] Caitlin Talmadge, The Dictator's Army: Battlefield Effectiveness in Authoritarian Regimes, Cornell University Press (2015).
[76] Feng Wang, et al., The End of China's One-Child Policy, Brookings Institution (2016); see also One-Child Policy 'Weakens China's Military,' Radio Free Asia (2012); China Grappling with Effects of 'One-Child Army', Adds Unmanned Aircraft, Ballistic Missiles, Says Experts, Yahoo News (2021).

in neutralizing America's operational superiority, and focused on diminishing the ability of the U.S. military to rapidly move from detection to destruction. In this changing technological-military landscape, the PLA aims to, in a crisis or war, paralyze the U.S. body politic, bring America's economy to a standstill, immobilize the U.S. military by destroying its battle networks, and present U.S. leaders with serious doubts about their ability to support partners and allies, leaving them with no almost other option but to concede.

The United States and its allies and partners need to restore the confidence in their ability to deter Chinese military aggression in the Western Pacific. Any war between the United States and the PRC, would have a massive human, economic, and environmental cost. If the United States were to lose, it would suffer a loss of influence in the Western Pacific, damaging the region's hard-won stability, advancing authoritarian systems, and likely leading to further wars.

With uncertain overmatch of traditional U.S. military capabilities, the outcome of a potential war with the PLA will increasingly come down to superiority and resilience of sensors, networks, software, interfaces between humans and machines, logistics, and – especially – the systems that connect or empower them all together. It will also come down to the U.S. willingness and ability to insert itself now within the PLA's envisioned future battlespace.[77]

In response to these challenges, we outline a new approach – an Offset-X strategy – that could begin to lay the groundwork for the United States to restore its military-technological superiority, and in the process circumvent China's military advancements, thwart its theories of victory, restore America's ability to project power in the Indo-Pacific region, and position the United States to honor its commitments to the stability of the region. This competitive strategy is derived from and grounded in America's persistent, asymmetric strengths, and envisions the development, deployment, and employment of new capabilities in ways that China will struggle to match or quickly duplicate. It aims to minimize the human and political cost the United States and its allies would suffer during a war with China, while driving up the political costs of war and creating serious dilemmas for Chinese leadership.

Offset-X is not a war plan and the initiatives we outline below are by no means a comprehensive or definitive list of actions. Rather, they jointly embody a competitive strategy to achieve and maintain military-technical superiority over all potential adversaries much like we did with stealth, precision strike systems, and networks in our previous offset strategies.[78] No offset strategy against China should be treated as fixed in stone. Rather, offsets need to be regularly reassessed against the PLA's adaptations, and should continuously seek to leverage emerging technologies. But we believe that the following ten initiatives provide a good starting point.

[77] The U.S. Marine Corps Force Design 2030, intended to help prevent the People's Liberation Army Navy from pushing past the First Island Chain, is a first effort to confront the PLA's systems, rather than just close kill chains. SCSP Defense Panel Meeting (July 2022). See also Force Design 2030, U.S. Marine Corps (last accessed 2022).
[78] Shawn Brimley, Offset Strategies and Warfighting Regimes, War on the Rocks (2014).

Offset-X Strategy

A competitive strategy to achieve and maintain military-technological superiority over all potential adversaries.

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.

Fully Embrace Distributed, Network-based Operations to Survive, Out-Maneuver, and Overwhelm Adversaries. Confronted with adversaries that value rigid hierarchies and have invested in capabilities that could provide them with some protection against concentrated, frontal assaults, the U.S. military should continue to develop and experiment with how it will employ smaller, highly-connected, and organically resilient, multi-domain units that practice network-based decision-making and effects.[79] Such units would operate in a distributed fashion, inside and outside an adversary's envisioned battlespace, leveraging U.S. global posture and access arrangements with partners and allies.

Such a network could generate significant dilemmas for adversaries by subverting their operations and creating multiple attack vectors and cross-domain effects. When acting in concert, forces that are distributed and networked can create mass, generate compounding effects, and operate with greater adaptability than single systems. They are also more resilient, and able to preserve decision-making and attack capabilities while experiencing damage that would degrade a hierarchical system much more. When acting in isolation, they can distract and create new windows of operational opportunities, especially for follow-on, more conventional formations. Essential to this concept of distributed, but highly-networked forces will be their empowerment with attritable unmanned systems operating at sea, in the air, in space, and on the ground to expand attack surfaces and absorb lethality, bolstered by an extensive network of low-cost sensors, satellites, and reconnaissance platforms.

To be sure, hierarchical structures have advantages. They empower top-down leadership, a clear order of command, and organizational efficiency. However, network-based structures adapt more quickly to rapid changes and operate more effectively in conditions of uncertainty.[80] While both structures are important for overall organizational effectiveness, emerging technologies are tilting the balance further towards networked-based military power. Technology is improving communications, increasing firepower, strengthening information collection and processing at the small unit level, and significantly compressing the time between detection and destruction of enemy forces. This reinforces network-based militaries' advantages by strengthening their situational awareness, further empowering their local decision-making, and enabling them to create or seize the initiative. These strengths have recently been demonstrated by the Ukrainian military, which has put up a strong network-based defense against the more hierarchical Russian military.[81]

The U.S. military can capitalize on network-based resilience and decision-making through the use of distributed operations, which allow small units to operate independently and separately from

[79] Force Design 2030, U.S. Department of the Navy at 6 (2020).
[80] John P. Kotter, Hierarchy and Network: Two Structures, One Organization, Harvard Business Review (2011).
[81] Julian E. Barnes, et al., U.S. Intelligence is Helping Ukraine Kill Russian Generals, Officials Say, New York Times (2022); Azeem Azhar, The Russian vs. the Ukrainian Network, Exponential View (2022).

large forces.[82] Drawing on its history of empowered tactical leaders and successful joint operations, the U.S. military would be well-positioned to continue conducting operations when tactical echelons are disconnected from their higher commands. In a future conflict, this distribution of forces would be better suited against rapidly improving ISR capabilities and anti-access and area denial (A2AD) concepts that make it increasingly hard for U.S. forces to create substantial mass.

The DoD should fully embrace distributed, networked operations to both circumvent proliferated A2AD systems and deliver surprise effects through the following efforts:

- Ensure select, joint tactical units are organically equipped to conduct distributed, multi-domain operations. This would include tactical mobility suited to the Western Pacific, stealth logistics, ISR, organic firepower to support themselves and destroy sea and air-based PLA assets, and connectivity to non-organic assets including fires.

- 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 their higher headquarters. They should have the communications equipment and authorities needed to securely access tactical intelligence.

- Ensure distributed units are able to employ counter-AI strategies to evade, overtake, or destroy adversary sensors. This will help distributed U.S. forces improve their survivability, even as sensors continue to proliferate.

> While the components of Offset-X strategy outlined here do not contain any recommendations on lethal autonomous weapon systems (LAWS), SCSP maintains that any application of emerging technologies for military purposes can and should be done in ways that are consistent with the laws of armed conflict. The U.S. Department of Defense has taken serious steps to ensure they have procedures and policies in place to responsibly field these capabilities.[83]

Lead the World's Militaries in Human-Machine Collaboration and Human-Machine Teaming. Essential to the concept of distributed, but highly-networked forces will be an extensive network

[82] Mark F. Cancian, The Marine Corps' Radical Shift toward China, Center for Strategic and International Studies (2020).
[83] U.S. Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway, U.S. Department of Defense (2022); Kathleen Hicks, Deputy Secretary, 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).

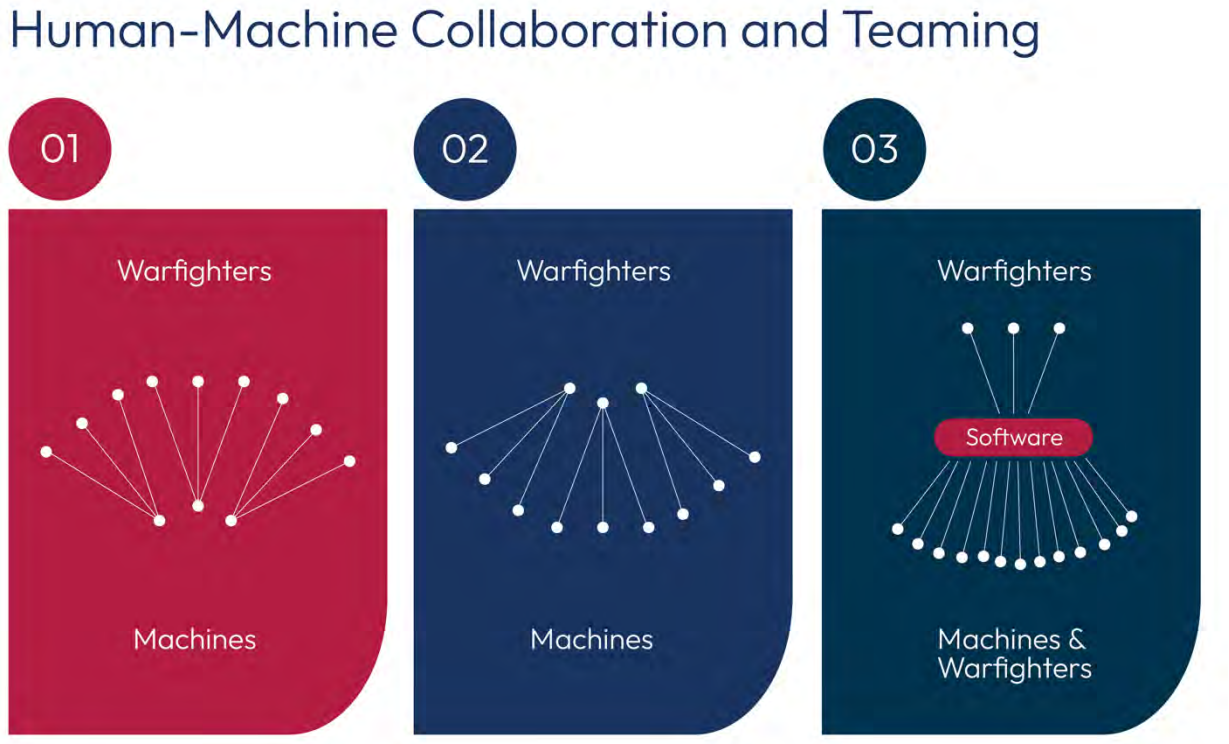
of low-cost sensors, satellites, and reconnaissance platforms, as well as large numbers of attritable unmanned systems operating at sea, in the air, and on the ground to diversify attack vectors, expand attack surfaces, and absorb lethality. Employing them effectively, however, will require mastering human-machine cognitive collaboration (HMC) and human-machine combat teaming (HMT). HMC and HMT are assuming center stage in several states' visions for the future of warfighting, and have the potential to considerably change warfare. For the U.S. military, human-machine cognitive collaboration will be critical to optimizing decision-making. Human-machine combat teaming, meanwhile, will be essential for more effective execution of complex tasks, especially higher-risk missions at lower human costs, or in confronting an adversary with dense defenses or sophisticated autonomous systems.

A core concept of HMC and HMT is that humans and machines have comparative advantages and therefore excel in different areas.[84] Humans outperform machines on many sensory tasks, certain types of communication, 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, memory, and consistent repetition. Augmenting human limitations with machine strengths (and vice versa), can create human-machine collaboration and teaming that outperform both humans and machines in many of their individual tasks. This may involve rapid processing and analysis of ISR data, faster decision-making, and quicker combat tasking with autonomous systems, such as AI co-pilots.[85] Also, machines are vastly better suited for high risk-to-force missions, and may ultimately enable even more precise strikes that reduce the risks of collateral damage.

HMC focuses primarily on cognitive tasks. A warfighter's mental bandwidth, as for every human, is limited. A decision to spend time solving one problem is a decision not to spend time on an equally critical task. The growth of HMC will enable individuals to break problems into their component pieces[86] and task some to be optimized, automated, or performed at scale by a computer in order to remove some of the clutter that taxes so much cognitive energy and free that up for higher order processing and decision-making. It will also allow individuals to refocus their mental bandwidth towards gaining situational awareness, understanding enemy plans, developing courses of action, accomplishing far more than they would otherwise, and mastering the tasks that humans do best.

[84] Tony Ojeda, The Algorithm - Human Tasks vs Machine Tasks, District Data Labs (last accessed 2022).
[85] Julie Obenauer Motley, The Testing and Explainability Challenge Facing Human-machine Teaming, Brookings Tech Stream (2022).
[86] What Is Computational Thinking?, Center for Computational Thinking, Carnegie Mellon University (last accessed 2022).

Meanwhile, human-machine combat teaming could enable the U.S. military to generate and employ mass in contested environments and do so in a way that reduces the risk to humans,[87] including risks of collateral damage. 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 challenges. Single, expensive platforms cannot achieve the same diversity of use as swarms of inexpensive systems and at the same degree of risk. Massed machines, assigned tasks by their human teammates, could overwhelm traditional defenses, often at a relatively smaller cost in human casualties compared to more traditional offensive operations. Machines could also serve as the "eyes and ears" of their human teammates, particularly in urban warfare, by helping them gain more information about their environment and taking risks in their place.



Another change that HMT can bring is in the balance of mass and effects delivery away from humans and towards machines, particularly low-cost ones. Today, in most cases, many warfighters collectively control one platform, such as a ship. While this relationship is unlikely to vanish, another human-machine relationship is developing that could begin to chip away at the dominant warfighter-platform relationship: swarms. AI-powered architectures that leverage

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

the contextual awareness and complex reasoning of human operators to manage large numbers of autonomous and semi-autonomous unmanned systems. An example of the potential of such an approach can be seen in DARPA's OFFensive Swarm-Enabled Tactics (OFFSET) program.[88] Another, less discussed relationship, is one wherein a small number of warfighters, skilled at software development, could create an application that optimizes the performance of many warfighters or machines down the line.

Using machines to provide mass and deliver effects may reduce the risk to humans. If the machines are relatively low-cost, it will also reduce the budgetary burden on the United States. At the tactical and operational levels, this will embolden commanders to design new concepts of operations and approach risk in previously unimaginable ways. At the strategic level, it will enable the United States to significantly increase the relative cost of war for its adversaries, while reducing its own.

HMC and HMT are not mutually exclusive, nor strictly delineated concepts. Many applications, especially more advanced applications, will include elements of both. Also, while HMC and HMT are not synonymous with autonomy, they will in certain circumstances rely on autonomy for their effectiveness, especially during high-intensity conflicts. Autonomous systems, with human supervision, will be essential in executing tasks and missions in increasingly compressed timelines. HMC and HMT, thus, can serve as an engine of greater autonomy, where appropriate, by helping develop and test capabilities, human-machine interfaces, and the military's ability to employ semi-autonomous or autonomous systems effectively and responsibly.

By 2030, the U.S. military should fully integrate HMC and HMT into daily operations at the tactical, operational, and strategic levels. The military services should prioritize development, accelerate adoption, and integrate training on HMC and HMT in military schools and training centers. Combatant Commands should identify opportunities and take actions to integrate HMC and HMT into their operations at all levels, irrespective of progress at the level of services or Department. The near-term priority should be to develop the most sophisticated interfaces for HMC and HMT while exploring the degree of autonomy assigned to unmanned systems, consistent with U.S. Department of Defense policy and international law.

The Department of Defense's efforts could be best advanced along three core lines of efforts. In the *development* realm, each military service should develop novel warfighting concepts and employment concepts for human-machine teaming. The Joint Staff should lead the development of a joint doctrine for HMC and HMT. DARPA should develop advanced HMC capabilities that can be fielded by 2027 at the latest. And, lastly, the Strategic Capabilities Office and services-based rapid capabilities offices should develop HMT capabilities for the next five years, with first capabilities at initial operating capability no later than 2025.

[88] OFFSET Swarms Take Flight in Final Field Experiment, Defense Advanced Research Projects Agency (2021).

In the *fielding* realms, DoD should design a readiness scorecard that tracks and encourages the integration of HMC and HMT capabilities across services. Services and Combatant Commands (CCMDs) 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 the Rapid Defense Experimentation Reserve (RDER).[89] Finally, the integration of HMC at the tactical level should begin immediately via the creation of opportunities for tactical units to experiment, develop tactics, techniques, and procedures, and become familiar with HMC.

In the *training* realm, DoD should require every CCMD to develop and execute a training program that uses HMC and HMT. Human-machine collaboration and human-machine teaming should also be integrated into all major training centers, including among the opposing forces. Finally, the Department should integrate computational thinking and HMC/HMT skills into entry-level training and continuing education requirements for commissioned and non-commissioned military personnel. This would include lessons in problem curation, data collection and management, the AI stack, probabilistic reasoning and data visualization, and data-informed decision-making.[90]

Gain and Maintain Software Advantage. A military's ability to deploy, employ, and update software, including AI models, faster than its adversaries is likely to become one of the greatest determining factors in relative military strength. In future crises and conflicts, the side that adapts faster and demonstrates the greatest agility, to include rapidly updating fielded software and AI models, may well gain a significant tactical and operational advantage. Software is now integral to every component of decision-making and operations, from sensing a target (sensor software), to decision-making (aggregation and analysis), targeting (weapons guidance system), and battle damage assessment.[91] The importance of software will only continue to increase. 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 superiority will become an even greater determining factor.[92] 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 helping with target selection and servicing.[93]

---

[89] Friedberg, Sidney. "Hicks Seeks To Unify Service Experiments With New 'Raider' Fund." 21 June 2021. https://breakingdefense.com/2021/06/hicks-seeks-to-unify-service-experiments-with-new-raider-fund/

[90] NSCAI Interim Report and Third Quarter Recommendations, National Security Commission on Artificial Intelligence at 106 (2021).

[91] Department of Defense Software Modernization Strategy, U.S. Department of Defense at 1-2 (2022).

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

[93] 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).

Software can also facilitate a shift from a small number of very exquisite satellites to a large number of significantly less expensive and less capable systems, but whose integration through software can produce the same information as the existing, expensive satellites. Such a constellation of low-cost, space-based assets could also play a critical role in defending against missile attacks, particularly hypersonic missiles that challenge existing paradigms of in-flight tracking.

To ensure software advantage, the DoD should consider taking a number of steps. First, DoD should complete a new information *architecture* that will allow DoD to be far more flexible, scale on demand, and adapt dynamically to changing conditions. As recommended by the National Security Commission on AI,[94] this would include access to cloud computing and storage;[95] 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.[96] Second, DoD should create career fields for military *personnel* for software developers, data scientists, and AI engineers, with both management and specialist tracks. Third, the Department should empower its tactical units to *experiment* with, develop, and deploy robust, reliable, and resilient software for the capabilities that they operate. This will allow the U.S. military 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. Fourth, DoD should *accelerate* the Authorization to Operate (ATO) process. 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.[97] 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.[98] 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. Fifth and final, DoD should

[94] Final Report, National Security Commission on Artificial Intelligence at 59-69 (2021);
[95] Department of Defense Software Modernization Strategy, U.S. Department of Defense at ii (2022).
[96] 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).
[97] Software Acquisition and Practices (SWAP) Main Report, U.S. Department of Defense (2019).
[98] SCSP interviews with service members and defense technologists.

measure and track software implementation with metrics focused on performance speed, cyber security, and useful capability delivered to end users.[99]

Ensure Resilience in Our Ability to Sense, Communicate, Attack, and Supply. In a conflict with China, system destruction warfare would indicate that one of the PLA's opening moves will 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 ability to logistically sustain its operations. Blind, deaf, and unable to communicate, deploy, or resupply, U.S. forces will be paralyzed.

To avoid this paralysis, the U.S. military needs to build resilience, including through redundancies, across every link and node of its operations – from sensors to attack platforms, in information architecture and networks, across command and control, and for logistics. This includes both terrestrial and space-based systems and networks. Cyber hardening is a critical component of this resilience at both the strategic and operational levels. Yet another critical component will need to be the acquisition and fielding of very large numbers of low-cost and attritable platforms that would support intelligence collection, communication, expeditionary logistics, and attack – especially during the opening days of a campaign.

Undermine Adversary's Censorship System. Authoritarian regimes are brittle, relying more on information control than buy-in to maintain domestic stability. 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. This would be especially important during a Chinese attempt to capture Taiwan by force. By helping ordinary Chinese citizens during times of war to thwart automatic censors and by placing the burden on regime human censors, the United States can help expand the public discourse beyond the regime's control.

Undermine Adversary Command Systems. The United States should also consider how it can subvert the effectiveness of adversary command, control, and communication (C3) systems. If the United States were to disrupt or cripple the PLA's C3 systems, it would cause disarray among the ranks of the PLA and desync its operations, preventing it from massing effects against U.S. forces. Preparing such offensively-oriented operations, however, should be accompanied by defensive preparations. The U.S. military needs to be prepared, preferably with AI-enabled capabilities, to detect and defend against operations that flood our society with misinformation or undermine U.S. C3 systems.

[99] Software Acquisition and Practices (SWAP) Study, Defense Innovation Board at 29-34 (2019).

Evolve Deliberate War Planning. Traditionally, DoD's deliberate war planning is based on the existing inventory of capabilities and forces. Planning guidance documents have generally instructed Combatant Commanders to construct war plans, and associated time-phased force deployments data (TPFDD), based on the capabilities available to them, in the first instance, and additional capabilities that could be allocated to them in the event of conflict from the total inventory of the Department of Defense.[100]

This approach to deliberate war planning, however, may no longer be suited for the anticipated changes in the character of warfare during this decade. First, the current method of planning does not factor in the state of the defense industrial base and its ability, or lack thereof, to surge production of munitions or platforms,[101] in the event that any of the planning assumptions prove incorrect. This could result in serious strategic risk, particularly in the event of high-intensity operations that rapidly consume existing inventory of munitions and assets, or in the event of a protracted conflict. In other words, the current method of war planning runs the risk of producing a situation in which the U.S. military reaches the end of munition stockpiles or inventory of assets before reaching the end of conflict. Second, the resource straight-jacketing embedded in the current planning methods limits the development of innovative concepts and reduces the ability of Combatant Commanders to influence the development of new capabilities. Put another way, Combatant Commanders are not encouraged to develop branch plans that identify new disruptive technologies and develop corresponding concepts of operations that could lower the risk to force and mission.

Therefore, the Defense Department should seriously consider evolving its deliberate war planning guidance documents and methodology, by considering the health and resilience of the defense industrial base and the full potential of the national security innovation network. The Department could do this by modifying the current DOD Instruction 3000.15 "Plan Review and Approval Process" and by incorporating the proposed changes in its Guidance for the Employment of Force (GEF). In the first instance, the modification could direct the Under Secretary of Defense for Acquisition and Sustainment to produce a supporting analysis for each operational plan that provides a clear assessment of the defense industrial base that most directly supports the assumed requirements of that plan and the potential of the base to support unplanned requirements. The updated Instruction and GEF would also direct Combatant Commanders to submit branch plans for each of the high priority contingencies that accompany rather than replace operational plans and include innovative technologies and operational concepts. These updated approaches will likely result in plans that combine rigorous risk

[100] DoD Instruction 3000.15, Plan Review and Approval Process, U.S. Department of Defense at 11 (2020).
[101] For more details on the challenges related to the U.S. techno-industrial base and near-term recommendations, see Mid-Decade Challenges to National Competitiveness, Special Competitive Studies Project at 57-81 (2022).

assessments with more effective operational solutions. This could also help DoD identify and prioritize the development and fielding of new, innovative capabilities.

Help Allies and Partners Develop and Maintain Interoperability and Interchangeability with U.S. Forces. As the United States continues to modernize its military forces, including investments in emerging technologies, there is a risk that a gap in capabilities between the United States and its allies could become a serious impediment to combined operations. Some of this gap is due to under-investments in defense by allies. Some of it has to do with security practices, particularly regarding the transfer of technologies, intelligence sharing, and command and control (C2) operations. But an important part of this gap also comes from the fact the United States has access to a unique innovation ecosystem. The United States must address these challenges if it is to capitalize on one of its most enduring asymmetries against China – its network of alliances and partnerships. In the near term, a promising action could be the establishment of a multilateral intelligence, surveillance, and reconnaissance network to improve coalition awareness in peacetime, and enable a more rapid transition from crisis to conflict during wartime.[102] Another action could be the development of a Joint and Combined All Domain Command and Control (JCADC2) architecture. This would be the multilateral expansion of the current U.S.-only Joint All-Domain Command and Control (JADC2) concept.[103] But the U.S. Government must accept far greater risks in information sharing and transfer of technologies to make this successful.

Implement a New Public-Private Partnering Model Between the U.S. Government, Industry, Academia, Investors, and Civil Society.[104] One of America's greatest defense strengths has been the close collaboration among the government, industry, and academia. That collaboration has, for various reasons, suffered over the past 20 years. At the same time, the CCP has been focusing on comprehensive national military-civilian fusion.[105] China continues its inexorable march toward reducing dependencies on the United States and advancing the development of Chinese technology companies. The United States must make a concerted effort to restore the level of collaboration between the government, industry, and academia, and to accelerate the adoption of commercial technology by the DoD. The defense industry played an essential role in developing capabilities that enabled the United States to prevail in the Cold War and conduct stability and counterterrorism operations in its aftermath and is already playing a critical role in the current geopolitical and technological contest. Just as importantly, collaboration must also extend to private investors and civil society. Civil society plays an important role in helping decide how technology should be employed, both for national security and civilian purposes. Private investors

[102] Becca Wasser, Developing Integrated ISR Networks to Improve Coalition Responsiveness, Presented at SCSP Defense Panel Meeting (July 2022).
[103] Summary of the Joint All-Domain Command & Control (JADC2), U.S. Department of Defense (2022).
[104] For a more detailed discussion of the imperative and models for a new public-private partnership model, see Chapter 1: Harnessing the New Geometry of Innovation in Mid-Decade Challenges to National Competitiveness, Special Competitive Studies Project (2021).
[105] Military-Civil Fusion and the People's Republic of China, U.S. Department of State (2020).

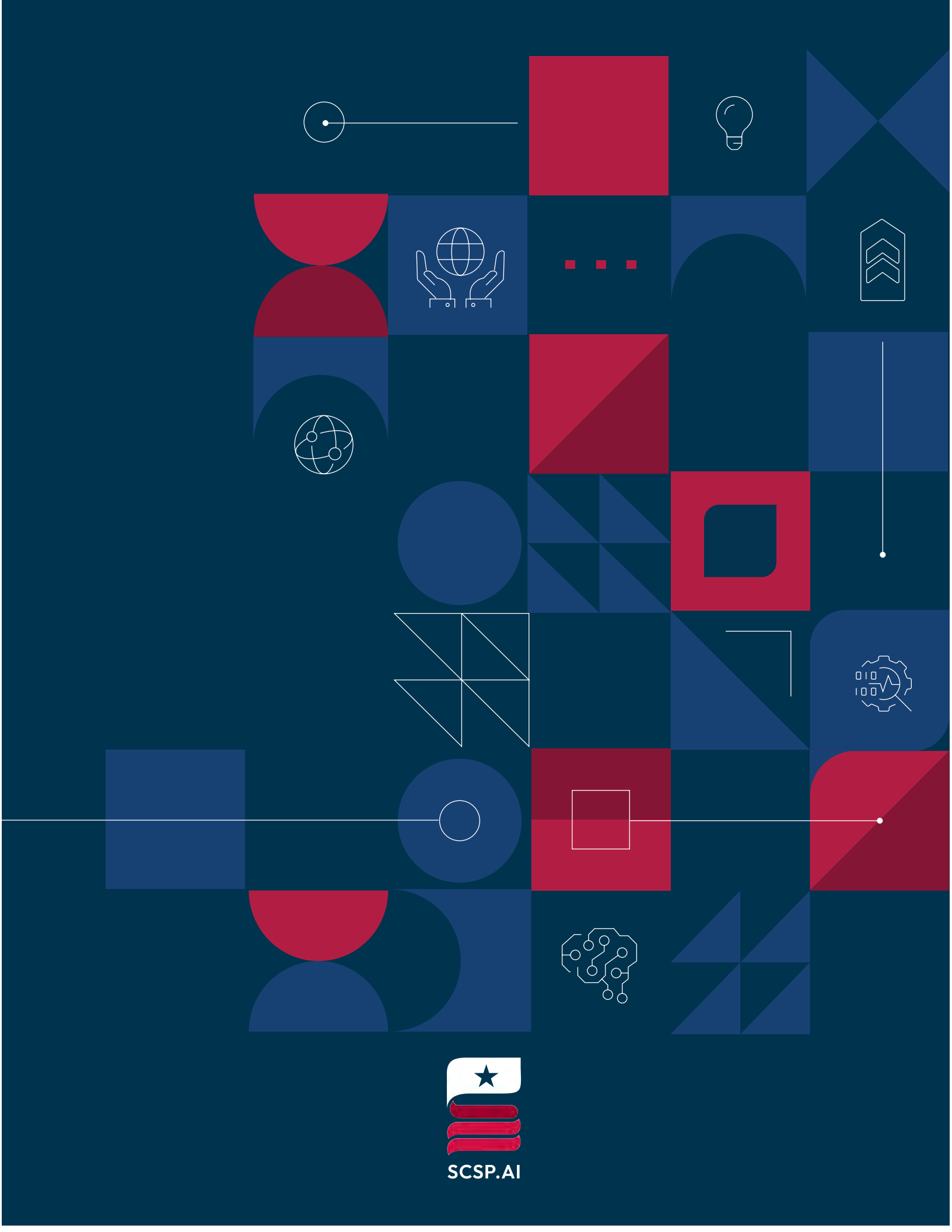
can bring to bear far greater capital towards the development and deployment of technology than the federal government. If the United States is able to unite all five stakeholders to pursue specific goals, America's dynamic capitalist market system and innovative commercial sector are much more likely to prevail over the long term. If not, the United States risks ceding critical ground to China.

Develop 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 should, therefore, develop 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.[106] While the immediate focus of the U.S. military should remain on developing its own autonomous systems, the United States cannot afford to wait for too long to develop the ability to counter and defeat adversarial AI-enabled and autonomous operations.

Operationalizing the Offset-X Strategy

The ten recommendations outlined above embody a competitive strategy to lay the groundwork for achieving and maintaining military-technical superiority over all potential adversaries. They are not intended as, nor should be viewed as, an operational prescription or a war plan. Significant prototyping, experimenting, and wargaming will need to be undertaken to validate the applicability and effectiveness of various innovative technologies for specific operational demands. The precise mix of emerging technologies and capabilities will yet need to be determined to address the changing character of warfare and peace. But as with previous successful offset strategies, the national and DoD pursuit and mastery of emerging technologies and innovation can enable the crafting of new operational concepts that can be tailored to meet specific military challenges. Offset-X strategy aims to build the foundation for future operations that can more easily and quickly offset adversarial capabilities.

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



SCSP.AI