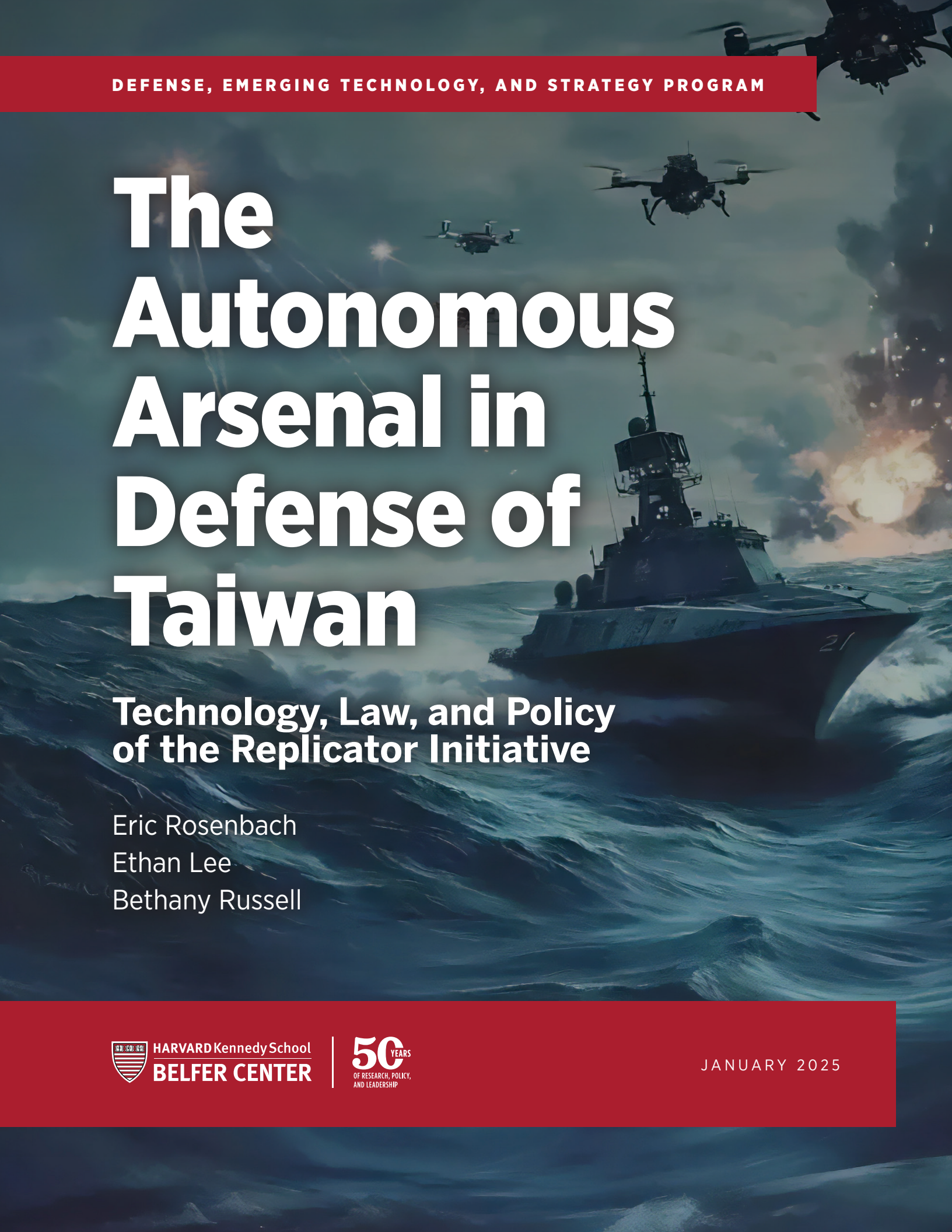


DEFENSE, EMERGING TECHNOLOGY, AND STRATEGY PROGRAM

The Autonomous Arsenal in Defense of Taiwan

Technology, Law, and Policy of the Replicator Initiative

Eric Rosenbach
Ethan Lee
Bethany Russell

HARVARD Kennedy School
BELFER CENTER

50 YEARS
OF RESEARCH, POLICY, AND LEADERSHIP

JANUARY 2025

Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org

DEFENSE, EMERGING TECHNOLOGY, AND STRATEGY PROGRAM

The Autonomous Arsenal in Defense of Taiwan

Technology, Law, and Policy of the Replicator Initiative

Eric Rosenbach
Ethan Lee
Bethany Russell

HARVARD Kennedy School
BELFER CENTER

50 YEARS
OF RESEARCH, POLICY, AND LEADERSHIP

JANUARY 2025

About the Defense, Emerging Technology, and Strategy Program

The Defense, Emerging Technology, and Strategy Program examines defense policy and the role of emerging technologies in shaping international security. For more, visit belfercenter.org/programs/defense-emerging-technology-and-strategy.

About the Authors

Eric Rosenbach is a Senior Lecturer at the Harvard Kennedy School and is the Director of the Defense, Emerging Technology, and Strategy Program at the Belfer Center for Science and International Affairs. He previously co-led the Belfer Center with former Secretary of Defense Ash Carter. Rosenbach currently serves on the Secretary of State's International Security Advisory Board and on the Secretary of Defense's Defense Business Board.

Rosenbach teaches graduate courses in policy development, strategy execution, and emerging technology. He also teaches two online courses for HarvardX on managing cyber risk and public sector strategy execution.

Rosenbach previously held several senior-level appointee jobs in government. As the Chief of Staff to the Secretary of Defense from 2015-2017, Rosenbach served as Secretary Ash Carter's closest strategic advisor on key policy initiatives, such as the war to defeat ISIS, the "rebalance" to Asia, and the effort to check Russian aggression. Rosenbach also led the Department's efforts to improve innovation by forging and managing key initiatives such as the Defense Digital Service and the Defense Innovation Unit.

Before serving as Chief of Staff, Rosenbach was the Senate-confirmed Assistant Secretary of Defense for Global Security and Homeland Defense. His diverse portfolio as Assistant Secretary included cyber, space, countering the proliferation of weapons of mass destruction, antiterrorism, continuity of government, and defense support to civil authorities. Earlier, Rosenbach served as Deputy Assistant Secretary for Cyber Policy.

Rosenbach previously served as national security advisor for then-Senator Chuck Hagel and as a professional staff member on the Senate Select Committee on Intelligence, where he led oversight of Intelligence Community counterterrorism programs. A former Army intelligence officer and commander of a telecommunications intelligence unit, Rosenbach led a team that worked closely with the NSA to provide strategic intelligence in direct support of commanders in Bosnia and Kosovo.

Rosenbach has published widely and authored several books, including *Confronting Cyber Risk: An Embedded Endurance Strategy.* The LA *Times* called his book *Find, Fix, Finish: Inside the Counterterrorism Campaigns that Killed bin Laden and Devastated Al Qaeda*, co-authored with Aki Peritz, "an important volume in the secret history of a nasty war."

As a Fulbright fellow, he conducted research on privatization programs in Eastern Europe. He holds a Juris Doctor from Georgetown, a Master of Public Policy from the Harvard Kennedy School, and a Bachelor of Arts from Davidson College.

Ethan Lee is a Research Assistant to Eric Rosenbach in the Defense, Emerging Technology, and Strategy Program at the Belfer Center for Science and International Affairs.

Previously, he was an Assistant Editor and David M. Rubenstein Editorial Fellow at *Foreign Affairs*. Ethan holds a Bachelor of Arts in Political Science with honors in International Security Studies from Stanford University. His work has appeared in the *Georgetown Journal of International Law, Survival,* and *Things That Go Boom*.

Bethany Russell is a joint Masters in Public Policy and Business Administration candidate at Harvard Kennedy School and Harvard Business School. Prior to attending Harvard, Bethany served for six years as an Army Intelligence officer. She deployed once to Iraq with special operations forces and worked with the First Multi-Domain Task Force analyzing adversary anti-access/area denial in the Indo-Pacific.

Bethany graduated from the U.S. Military Academy with a Bachelor of Science in International Relations and Chinese and from Schwarzman College, Tsinghua University with a Master of Management Science in Global Affairs. Her research interests include the Indo-Pacific, U.S. foreign policy, and economic security.

Table of Contents

AI Generated/Midjourney

Executive Summary

China's military expansion and threats to forcibly reunify with Taiwan undermine U.S. interests in the Indo-Pacific. Fully autonomous weapon systems, designed to be attritable and complete missions without human control in denied electromagnetic environments where communications are impossible, are necessary to support the U.S. military defense of Taiwan.

To accelerate innovation and the fielding of fully and semi-autonomous weapon systems, the U.S. Deputy Secretary of Defense, Dr. Kathleen Hicks, launched the Replicator Initiative in August 2023. This effort, which aims to deploy thousands of "all-domain attritable autonomous systems" and other advanced capabilities, is currently helping the United States strengthen its military deterrent against China. The Department of Defense is making important progress in addressing autonomous weapon systems' unavoidable and interrelated risks spanning strategy, technology, and law. Continued leadership from the Deputy Secretary of Defense, Vice Chairman of the Joint Chiefs, Defense Innovation Unit, and Indo-Pacific Command is crucial to mitigate these risks and preserve the current momentum for the development of advanced autonomous systems.

Key Assessments:

- **The fully autonomous weapon systems necessary for the defense of Taiwan are at least five years away from operational maturity and fielding.** The research, development, and operational testing of advanced AI models and hardware needed for autonomous weapon systems have advanced significantly over the past several years. But, similar to the commercial development of autonomous vehicles, technology optimists often underestimate the technological and operational challenges of fielding fully autonomous weapon systems.

- **The United States is unlikely to utilize fully autonomous weapon systems against China's most likely strategy: a blockade of Taiwan.** Given the risk of escalation and the inherent lack of transparency in advanced AI models, senior policymakers will likely limit the use of autonomous weapon systems in a blockade scenario to missions such as intelligence collection or the deployment of advanced smart mines.

- **Recent advances in counter-drone technologies will likely limit the efficacy of attritable semi-autonomous weapons and increase the urgency of developing fully autonomous weapons.** Since late summer of 2024, the overall efficacy of autonomous platforms on the battlefield in Ukraine has diminished because of increasingly effective counter-UAV capabilities, including electronic warfare and GPS spoofing. Similarly, China's network of defensive capabilities, including anti-aircraft guns, directed energy, and jamming systems, would limit the efficacy of U.S. autonomous weapon systems in a conflict.

- **Replicator will fuel the U.S.-China security dilemma in the context of autonomous weapon systems.** The U.S. fielding of autonomous weapon systems will likely stoke the production and fielding of autonomous platforms and defensive systems, or precipitate an arms race in autonomous weapons systems. This dynamic could ultimately favor Beijing due to its industrial capacity, industrial capacity and strength in commercial drone manufacturing, lower production costs, and consistent disregard for international law.

- **Senior military leaders must continue to develop and exercise realistic, sophisticated concepts of operations for autonomous weapon systems that are fully integrated into any formal military plans for the defense of Taiwan.** These plans will both drive operational innovation and bolster the requirements process necessary for the sustainable fielding of autonomous weapon systems. Without detailed concepts of operations, the production and fielding of autonomous weapon systems may stall.

- **The Department of Defense should prioritize accuracy and traceability over explainability due to the "black box" trade-off.** Ideally, AI models for autonomous weapon systems would provide explanations for their decisions, but the advanced deep learning algorithms necessary for fully autonomous weapon systems are too complex to offer semantic explanations understandable to humans. Given these constraints, traceability and accuracy must take priority over explainability to ensure that autonomous weapon systems are effective in combat and comply with the law of armed conflict.

- **Limited real-world data will require the Department of Defense to manage the risk of using synthetic data for the development of fully autonomous weapon systems' advanced AI models.** The Department of Defense must continue to identify and gather the data necessary to develop underlying AI models for autonomous weapon systems. However, limited real-world

intelligence data from PLA exercises is not sufficient to train autonomous weapon systems for large-scale conflicts in the defense of Taiwan. Generative Adversarial Network models are useful for creating comprehensive synthetic environments to train autonomous weapon systems, refine the underlying AI model and its ability to identify targets, detect anomalies during missions, and navigate complex terrain.

- **Fielding fully autonomous weapon systems will require advancements in battery and edge computing technologies.** Due to the challenges of exchanging information with cloud computing resources in denied electronic environments, autonomous weapon systems must utilize parallel computing on the edge. The advanced AI models used in autonomous weapon systems will also come with other limitations and drawbacks, such as high energy use, compelling developers to make trade-offs between speed, efficiency, and performance.

- **The Department of Defense's interpretation of international law will be embedded in the AI algorithms for fully autonomous weapon systems, effectively serving as a codification of the United States' approach to the laws of war.** Fully autonomous weapon systems operating in denied electronic environments will need to independently interpret and apply the law of armed conflict, maritime legal regimes, and rules of engagement. The training process for autonomous weapon systems' AI models in these scenarios would represent the codification of the U.S. interpretation of the law. To ensure that fully autonomous weapon systems operating without direct human oversight can reasonably interpret the law of armed conflict, the Department of Defense should assemble a team of experienced targeting specialists, military lawyers, scientists, and engineers to comprehensively incorporate legal training into AI model development.

- **The Department of Defense's publicly released policy sets a high international standard for transparency on the development and deployment of autonomous weapon systems.** In contrast to the secrecy characterizing other countries' policies on autonomous weapon systems, the Department of Defense has created explicit guidelines for their responsible development and use. This established a critical foundation for accountability and better positions the United States as a leader in international discussions on autonomy in warfare.

Introduction

"Now is the time to scale, with systems that are harder to plan for, harder to hit, and harder to beat than those of potential competitors. And we'll do so while remaining steadfast to our responsible and ethical approach to AI and autonomous systems... We must ensure the PRC [People's Republic of China] leadership wakes up every day, considers the risks of aggression, and concludes, 'today is not the day'—and not just today, but every day, now and for the foreseeable future."

— Kathleen Hicks, September 2023.[1]

Strategies of Disruption

The United States and China are locked in an economic and security competition. Since the mid-1990s, Beijing has invested the equivalent of hundreds of billions of U.S. dollars to expand the capabilities of the People's Liberation Army (PLA).[2] It has expanded the People's Liberation Army Navy (PLAN) into the world's largest by ship count, built the largest aviation force in Asia, and established an extensive network of overlapping air defense and long-range artillery systems.[3] Beijing is also increasing Chinese military strength through investments in artificial intelligence and quantum computing, which will likely improve the PLA's ability to track and strike adversaries.[4] These new military capabilities are not just for show; the PLA has intensified its military activities around Taiwan since August 2022, rehearsing blockades and long-range strikes, conducting regular violations of Taiwan's Air Defense Identification Zone, sailing vessels near Taiwan's waters, and allegedly launching cyberattacks against Taiwan's digital infrastructure.[5]

While the United States still holds an overall advantage in military technology and capabilities, China does not need to execute its actions perfectly or simultaneously to undermine key elements of U.S. strategy and level the playing field.[6] Wargames suggest that in a conflict over Taiwan today,

Washington could lose dozens of ships—including its forward-deployed aircraft carriers in the region—and run out of long-range munitions within the first week.[7] A "fair fight" often means barely coming out ahead, a dangerous prospect given China's proximity to key U.S. allies and Washington's competing interests in Europe and the Middle East.[8]

To counter the PLA's growing threat against Taiwan, the U.S. Department of Defense (DoD) has increased its investment in traditional military capabilities such as guided missile destroyers and advanced manned aircraft.[9] Given the time and capital necessary to build these platforms, however, the DoD is also aggressively pushing the acquisition and deployment of large numbers of autonomous weapon systems.[10] This report defines fully autonomous weapon systems as a nascent class of military systems that, once activated, can independently conduct missions without human intervention. The DoD's most notable investment in autonomy has advanced through the Replicator Initiative, announced in 2023 by Dr. Kathleen Hicks, the Deputy Secretary of Defense. Along with many other capabilities, Replicator aims to deploy thousands of low-cost and attritable autonomous platforms across different warfighting domains and military branches.

The Defense Innovation Unit and Replicator

The Defense Innovation Unit (DIU) is a key stakeholder in Replicator. More broadly, it collaborates with other components of the DoD to accelerate U.S. forces' fielding of new commercial technology in areas such as AI, cyberspace, energy, and space.[11]

Established in 2015 by then-Secretary of Defense Ash Carter as the Defense Innovation Unit Experimental, DIU connects the DoD with the private sector to bring new commercial technologies for military use.[12] DIU is headquartered in Silicon Valley and has expanded its presence by opening offices in Austin, Boston, Chicago, and Arlington.[13] In 2023, Secretary of Defense Lloyd Austin realigned DIU to have it report directly to the Office of the Secretary of Defense.[14]

The DoD's Innovation Steering Group and the Defense Innovation Working Group oversee Replicator, with DIU providing principal staff support to the Steering Group and chairing the Working Group. To date, Replicator has engaged over 500 commercial firms and awarded contracts to more than 30 hardware and software companies, 75% of which are not traditional defense contractors.[15]

Addressing the Challenge

Autonomous weapon systems cannot fully replace the firepower and capabilities of more traditional military assets. However, they present one promising option for addressing key challenges posed by the PLA in a Taiwan contingency.[16] U.S. autonomous weapon systems across various warfighting domains could act as a force multiplier, serving as a cost-efficient and more expendable alternative to manned systems.[17] Their smaller footprint and lower manning requirements likely make it easier for American commanders to employ them closer to mainland China, and they hold the promise of processing information and making decisions at speeds beyond human capacity. They could also compel China to make difficult trade-offs; Beijing would need to decide how to allocate resources against a wider spread of U.S. platforms, including highly lethal swarms of dispersed autonomous

weapon systems.[18] Beyond their advantages in warfighting, the DoD seeks to use Replicator's fast-tracked deployment as a way of accelerating innovation in the U.S. defense industrial base, expediting the development, production, and acquisition of emerging technologies for future military needs.[19]

Lessons from the war in Ukraine are also driving the DoD's push to develop autonomous weapon systems. Since Russia's 2022 invasion of Ukraine, Kyiv has developed a wide array of unmanned systems (UxS)—more specifically, unmanned aerial vehicles (UAVs), unmanned surface vehicles (USVs), and unmanned underwater vehicles (UUVs)—against Russian tanks, artillery, and warships.[20] Drone warfare is nothing new, but Ukrainian and Russian forces have employed expendable drones at an unprecedented scale, enhancing their battlefield reconnaissance and providing a more cost-effective way to strike targets. Both parties have also developed and deployed counter-UxS technologies to detect and neutralize enemy drones. This includes the use of electronic warfare systems to jam, disrupt, or spoof drone communications and the deployment of kinetic systems to physically intercept and destroy unmanned threats. This has driven new adaptations on the frontlines; Ukrainian forces, for example, have reverted to using wired-guided controls for UAVs due to communications-denied electronic environments.[21] The integration of AI in UxS is still nascent, but as technology continues to evolve, advancements in AI could enable faster, more efficient, and cost-effective approaches to warfare.

The DoD has intentionally kept details about Replicator vague; for instance, it maintains secrecy around the autonomous weapon systems selected through the Initiative and the ways that they will be employed. This opacity is important to protect strategic advantage, safeguard sensitive technologies, and encourage commercial vendors to innovate beyond traditional developmental constraints. Though DoD has maintained secrecy in its approach, publicly available information indicates it has made significant progress thus far by accelerating the acquisition process for new military platforms, advancing the underlying technology necessary to successfully field autonomous weapon systems, and developing the production capabilities necessary to deploy them at scale. As a result, Replicator is an important milestone in U.S. defense innovation, enabling the rapid deployment of cutting-edge platforms necessary to counter the PLA and helping undermine Beijing's confidence in its ability to favorably alter the status quo by force.

Public Timeline of the Replicator Initiative

(August 2023 - November 2024)

August 28, 2023: Deputy Secretary of Defense Kathleen Hicks announced the Replicator Initiative at the Emerging Technologies for Defense Conference and Exhibition.[22]

May 6, 2024: The DoD publicly unveiled the first tranche of Replicator capabilities, focusing on acquiring attritable UxS platforms for the U.S. military.[23]

September 27, 2024: Secretary of Defense Lloyd Austin announced Replicator 2, aimed at countering U.S. adversaries' small UxS.[24]

November 13, 2024: The DoD unveiled Replicator 1.2. This new tranche publicly introduced additional air and maritime systems and integrated software for autonomy.[25]

November 20, 2024: DIU announced the selection of software vendors to support Replicator; more specifically, improving command and control for UxS and enabling autonomous platforms to collaborate with each other.[26]

December 5, 2024: Building on Replicator 2, the DoD announced that Secretary of Defense Lloyd Austin approved a classified strategy for the U.S. military to counter UxS.[27]

Yet there is still considerable work remaining in order for the United States to effectively field fully autonomous weapon systems—complete adoption will likely take five or more years for the DoD to field a fully mature operational capability. To rapidly and responsibly employ fully autonomous weapon systems, the DoD must focus on three sets of critical challenges. The first is technological. Current technological constraints such as power and AI model development have prevented the DoD from fielding fully autonomous weapon systems as of yet—those with the range and levels of autonomy necessary to effectively contribute to Taiwan's defense are likely five or more years away. To train advanced AI models

for fully autonomous weapon systems, the DoD needs extensive real-world data collection and realistic synthetic datasets. Scientists and engineers need to use advanced machine learning techniques to develop fully autonomous weapon systems with advanced capabilities, such as determining when and how to perform specific tasks, interpreting intent, prioritizing new data to collect, and identifying causal factors in a battlespace. In addition, advanced AI models require significant energy, and fully autonomous weapon systems need to rely on edge computing architectures to operate effectively. These demands will impose constraints on autonomous weapon systems' capabilities, thereby forcing the DoD to make trade-offs between their speed and performance.

The second and third sets of challenges relate to the law of armed conflict and the policies governing the use of autonomous weapon systems. As autonomous weapon systems operate in increasingly austere environments, particularly in denied electronic environments where direct human control is not possible, their AI models will need to independently apply international law and the rules of engagement. To ensure that fully autonomous weapon systems make lawful decisions on the battlefield, their underlying AI models must incorporate legal training from experienced military lawyers, engineers, and targeting specialists. Because the deep learning AI models needed for autonomous weapon systems are too complex to provide semantic explanations that humans can understand, developers must prioritize accuracy over explainability to ensure that they are as effective as possible in combat and comply with the law of armed conflict.

U.S. leaders also need to manage the development and deployment of autonomous weapon systems through Replicator in the context of the U.S.-China security dilemma. Beijing could perceive the U.S. buildup of attritable autonomous weapon systems as provocative and respond by intensifying its current military buildup, including its development of systems built specifically to counter autonomous weapon systems. This cycle risks accelerating the proliferation of UxS and measures meant to counter autonomous weapon systems, fueling a U.S.-China arms race in the quantity and quality of each country's arsenal of autonomous weapon systems, and heightening tensions that could inadvertently trigger the conflict Washington seeks to prevent. The U.S. must focus on rapidly and responsibly fielding autonomous weapon systems to mitigate the destabilizing effects of this dynamic, ensuring these systems strengthen deterrence without provoking unnecessary escalation.

To ensure that autonomous weapon systems are a reliable operational capability, U.S. Indo-Pacific Command must develop clear concepts of operations that outline how, where, and against what these systems will be deployed. These concepts of operations should consider where autonomous weapon systems will be positioned prior to conflict or how they might enter the theater once conflict has begun. Without detailed concepts of operations that fully integrate into any existing plans for the defense of Taiwan, autonomous weapon systems may prove ineffective and underutilized, lacking the confidence of U.S. commanders and policymakers. The requirements outlined in these plans are essential to drive the innovation and acquisition process over the next several years. Moreover, the operational effectiveness of autonomous weapon systems must be realistically assessed against their limitations, including their vulnerability to electronic warfare and the constraints of autonomy in contested environments.

Following this introduction, Section Two of the report analyzes two potential cases that could lead to a U.S.-China conflict: a naval blockade and subsequent conflict over control of Taiwan's surrounding waters, and a full-scale PLA invasion of Taiwan. Section Three examines the nature of the underlying technologies powering autonomous weapon systems, and Section Four explores related legal and policy considerations.

Scenarios

"War, however, is not the action of a living force upon a lifeless mass... but always the collision of two living forces."

— Carl von Clausewitz, *On War.*[28]

Overview and Assumptions

This report frames its analysis of autonomous weapon systems in the context of two potential Taiwan contingencies: a blockade in the waters around the island and a full-scale PLA invasion. These scenarios are not intended as exact predictions of the campaigns that Beijing is most likely to pursue. Instead, they aim to contextualize the threat environment and highlight challenges that autonomous weapon systems could help address.

This report bases its analysis on a few critical assumptions. Chief among them is the belief, often expressed by U.S. officials, that the PLA seeks the capability to invade Taiwan by 2027.[29] The adoption of this assumption does not suggest that 2027 is the most probable date for China to invade Taiwan; while a blockade or invasion by China is more likely after 2027, using this year as a reference point underscores the pressing need for Replicator to help confront the most immediate and severe threat. This framing provides a benchmark for U.S. commanders and policymakers to take the necessary steps, preparing autonomous weapon systems ahead of any potential aggressive action by China.

The second key assumption is that the United States, informed by intelligence on Chinese President Xi Jinping's intentions and PLA planning, would have sufficient warning of actions against Taiwan. This intelligence should clarify whether Beijing intends to impose a naval blockade or launch a full-scale invasion.[30] If these indicators do not materialize or Washington has less time to react than anticipated, the DoD would likely be limited in its ability to deploy U.S. assets like autonomous weapon systems in the region.

Blockade or Quarantine

China could apply coercive pressure against Taiwan and test U.S. and international resolve by initiating a maritime quarantine or blockade with the PLAN. In this scenario, Beijing would strive to remain below the threshold of a kinetic conflict. Instead, it would rely on its Maritime Militia, Maritime Safety Administration (MSA), and China Coast Guard (CCG) to exert economic and transportation pressure against Taiwan. China's goal would be to encroach into Taiwan's space, erode its sovereignty, impose economic hardship, and compel unification without ever crossing a clear red line.[31]

To support this pressure, the PLA would mobilize its Navy and deploy Surface Action Groups—comprised of destroyers, support vessels, and frigates—west of Taiwan into the East China Sea and Philippine Sea. It could augment these forces with one or both of its aircraft carriers. Rather than provide kinetic assistance, these Groups would serve as strategic signals to deter foreign intervention or international support for Taiwan, as well as provide intelligence against approaching adversaries. Positioning destroyers east of Taiwan would also enable a rapid PLA response if Beijing chooses to escalate.[32]

The main force that Beijing would utilize in this scenario would be China's maritime law enforcement, particularly the CCG and MSA. Beijing would likely announce "enhanced customs inspections rules" on shipping to Taiwan, rather than labeling the operation a blockade.[33] To enforce these rules, Beijing would position vessels from the CCG and MSA within Taiwan's territorial waters and near major ports, particularly Taipei, Taichung, and Kaohsiung.[34] The PLA and CCG have already rehearsed this positioning in its "Joint Sword 2024B" exercises in October 2024, involving 153 aircraft and 43 ships.[35] In a quarantine or a blockade, China's law enforcement personnel would then board commercial carriers, inspecting cargo, questioning personnel, and controlling what ships—if any—were allowed to transit to and from Taiwan. Should Beijing wish to escalate, it could order the CCG and MSA to indefinitely impound ships at ports in mainland China under the pretext of customs inspections. At the same time, Beijing would likely deploy large numbers of Maritime Militia ships into the Strait and around the island. The Maritime Militia would restrict the freedom of navigation for Taiwanese ships and complicate Taiwan's maritime domain awareness by making it harder to distinguish between quarantining military vessels and fishing vessels that increase "grey zone" pressurization.[36]

Hypothetical Employment Scenario of Two Publicly Announced Replicator Platforms: the Altius and C-100

Two key platforms publicly unveiled as part of Replicator 1.2 are Anduril's Altius-600 and Performance Drone Works' C-100.[37] The Altius-600 is a fixed-wing UAV designed for surveillance, reconnaissance, counterintelligence, communications, and cyber warfare missions. It can launch from fixed-wing aircraft, helicopters, ground vehicles, or ships. The Altius-600M variant can function as a loitering munition, capable of identifying and striking targets such as armored vehicles or fortified positions.[38] The C-100 is a quadcopter UAV capable of carrying a payload of up to five kilograms—for instance, sensors, supplies, electronic warfare systems, and munitions. It can fly for more than an hour and has a range exceeding 10 kilometers.[39]

These platforms could be used to support Taiwanese forces defending Taiwan-controlled islands near the Chinese mainland. For instance, if Beijing decided to escalate beyond a maritime blockade with an offensive operation falling short of launching a complete invasion of Taiwan, it might authorize units from the PLAN Marine Corps and PLA Special Operations Forces to conduct an assault to seize Taiwan-controlled Kinmen Island, located less than four kilometers from China at its nearest point. To impose costs on Beijing without directly escalating to an overt shooting war between U.S. military personnel and PLA forces, the United States and Taiwan could both deploy Altius-600s and C-100s from ground vehicles prepositioned nearby or USVs and UAVs in the Strait.[40]

Altius-600s and C-100s could then travel to Kinmen, an environment where traditional aerial platforms—such as MQ-9B SeaGuardians or AH-64 Apaches—would not be survivable. They could collect intelligence or use electronic warfare kits to jam PLA communications, thereby disrupting the coordination of attacking PLA forces. Taiwanese

commanders directing the defense of Kinmen could also utilize the C-100's lift capability to deliver critical supplies, such as medical equipment, to troops fighting in forward positions. To deliver lethal effects, Altius-600Ms could receive orders from Taiwanese commanders to conduct precision standoff strikes, while C-100s could drop 13-kilogram fragmentation explosives on enemy positions and be restocked with munitions and fresh battery packs by Taiwanese forces.

This plan would be far more complex in practice—many attritable autonomous weapon systems would fall victim to PLA electronic warfare and air defense systems before fully completing their missions. At the same time, uncertainty on future battlefields will likely increase as degraded communications, adversarial countermeasures, and the deployment of autonomous weapon systems by multiple belligerents intensify the fog of war. Kinmen would almost certainly fall if the PLA committed enough forces to overwhelm it, but the critical question is how much effort such an operation would demand. The coordinated swarming of these platforms can create multiple dilemmas for the PLA, shaping the battlefield favorably and allowing tripwire forces to resist more effectively.

China's goal with a quarantine or blockade would be to pursue reunification through coercion rather than outright force. By disrupting and limiting the flow of goods into Taiwan, Beijing could pressure private companies to delay or reroute their shipping to the island. Taiwan is more geographically and economically vulnerable compared to China, and thus likely possesses a limited ability to sustain itself under such conditions.[41] Even if China allows the majority of traffic to flow through Taiwan's ports, Beijing's imposition of a blockade or quarantine could demonstrate that Taiwan does not control maritime areas it claims as its sovereign space. Compliance by shipping companies would reinforce Beijing's narrative that it controls Taiwan. A lack of U.S. intervention to disperse Chinese maritime law enforcement would further bolster these claims.[42]

In addition, a blockade or quarantine would provide Beijing with scalable options. China could choose to board every ship, a few ships, or only ships from select countries. It might attempt to quarantine Taiwan's entire coastline or merely target major ports. Ships could face detentions ranging from hours to days, and Beijing might limit ships potentially carrying weapons but allow those carrying food. China could block the entirety of the Strait or continue to permit commercial shipping. Beijing could also order the PLA Aviation Force to fly continuous sorties above the island to extend the blockade, disrupting air travel and transport. The PLA would likely conduct electronic warfare and cyberattacks against the Taiwanese government and American forces throughout the blockade, and it could scale the breadth, length, and severity of these communications disruptions.[43]

Should a quarantine or blockade fail to achieve Beijing's goals, China could threaten Taiwan by undertaking additional military actions such as cyberattacks against critical infrastructure or live-fire training exercises near the island. If all actions short of full-scale war are wholly unsuccessful, Beijing could then have the option of transitioning to an invasion of the island.[44] The United States would likely have less time to detect this shift under crisis circumstances; after all, the PLAN assets that would defend the invasion would already be underway and positioned east of Taiwan to support the blockade.

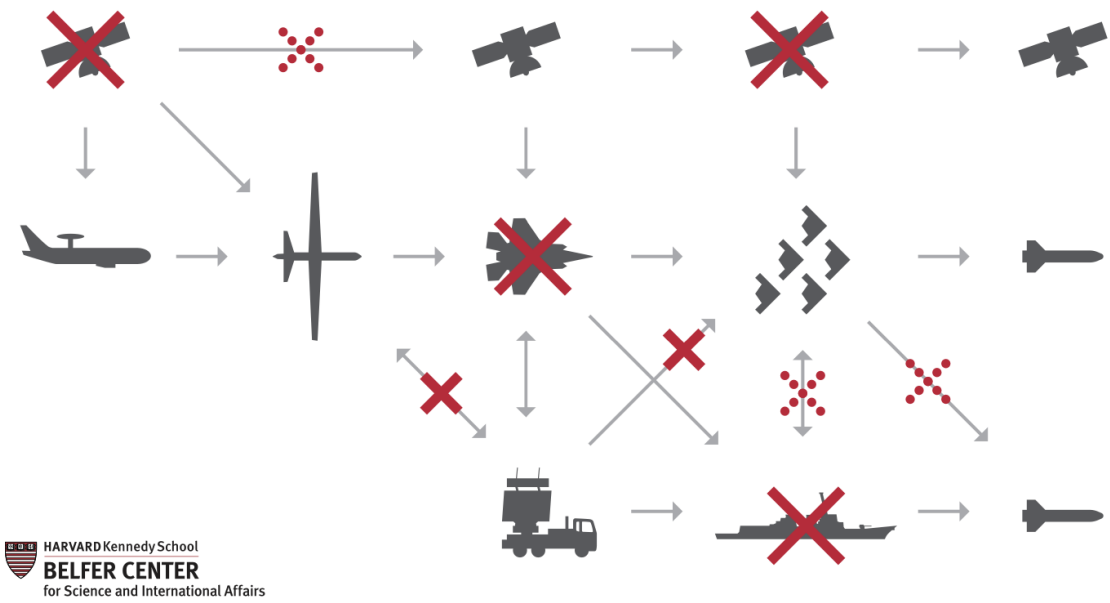
At the brink of such a crisis, the President is unlikely to authorize the use of fully autonomous weapon systems, as they offer no clear operational or strategic advantages in a blockade scenario. Potential U.S. responses to a Chinese blockade could include surveillance, escorting maritime shipping into Taiwanese ports, and counter-blockades; as is reasonably foreseeable, fully autonomous weapon systems do not offer novel, concrete advantages over manned or remotely piloted U.S. assets in these contingencies. It would also likely be challenging to program fully autonomous weapon systems' actions to achieve military objectives in a manner that is neither overly escalatory nor excessively passive. If both belligerents aim to pressure the other to back down while avoiding full-scale war, U.S. policymakers and commanders would be unlikely to trust fully autonomous weapon systems to decide when to use armed force. Instead, they will likely opt to determine themselves whether a red line has been crossed and decide on the appropriate response.[45] In addition, it is difficult for the United States to credibly demonstrate that American commanders have specifically instructed U.S. fully autonomous weapon systems to act as a tripwire under certain conditions, such as engaging

Chinese vessels that enter into Taiwanese territorial waters.[46] If Beijing believes that Washington is bluffing and that U.S. commanders have not pre-delegated such authority to the AI models behind fully autonomous weapon systems, Chinese forces may begin to test the limits of that commitment incrementally.

While the DoD is unlikely to utilize fully autonomous weapon systems in a blockade scenario, they may choose to employ semi-autonomous weapon systems with oversight from senior policymakers and military leaders. U.S. commanders could use semi-autonomous weapon systems as a force multiplier directly assisting and taking orders from manned assets or human operators. They could conduct intelligence gathering missions, escort tankers and early warning aircraft behind the front lines, or deploy advanced smart mines in defensive positions.

Full-Scale Invasion

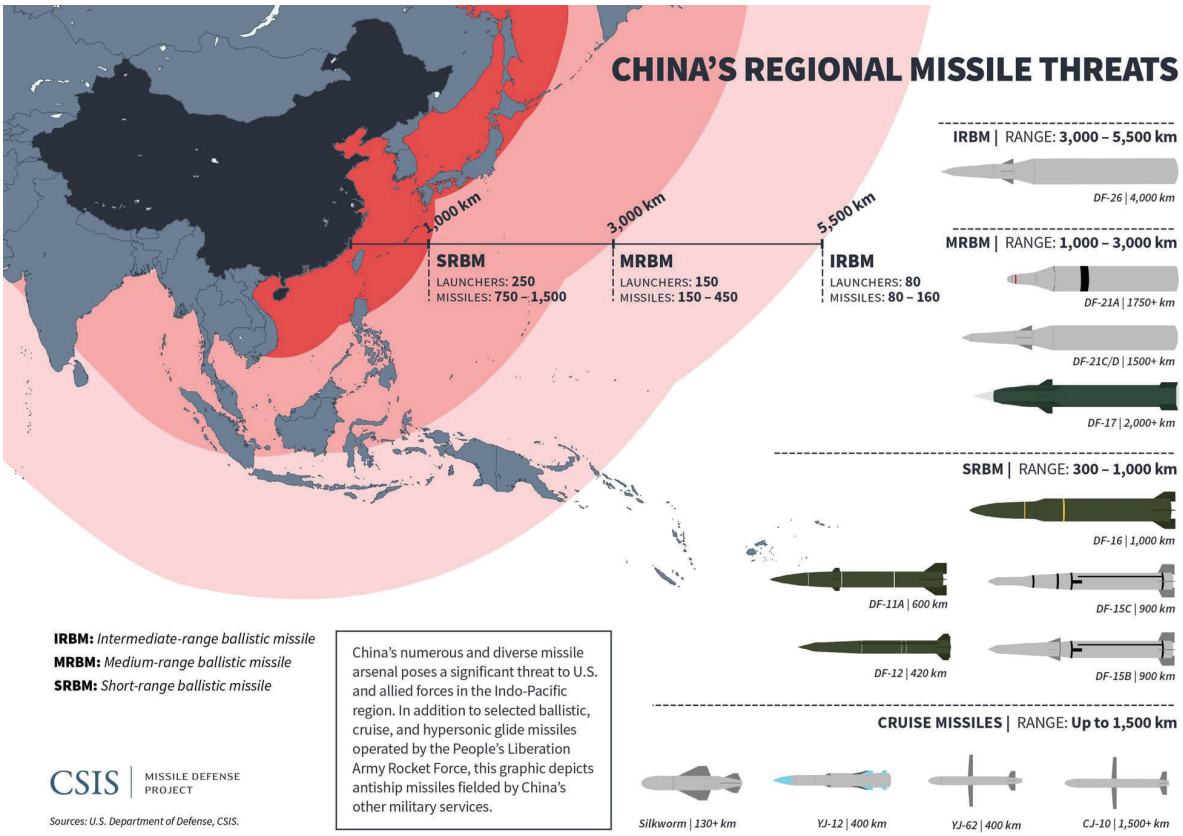
If China decides to launch a full-scale invasion of Taiwan, the PLA would almost certainly begin these efforts by launching cyber and electronic warfare attacks targeting Taiwan and its defending forces.[47] The ability of modern states to coordinate their forces depends on a complex network of communication and navigation systems linking sensors, shooters, and decisionmakers—systems that often operate through predictable and vulnerable nodes.[48] Accordingly, Chinese doctrine directs the PLA to conduct cyberspace and electronic warfare operations. By targeting U.S. command and control networks, the PLA threatens American power projection and limits U.S. and Taiwanese forces' ability to track and engage targets even if they have the necessary munitions to do so.[49] Beijing already has substantial experience conducting cyberattacks against Taiwan's networks.[50] It would likely begin launching cyberattacks against Taiwan's key infrastructure and government sites early in an invasion, sustaining these efforts throughout the conflict to disrupt information flow and prevent Taipei from mounting a strong defense.[51]



Some of the PLA's cyber and electronic attacks would also likely target U.S. assets in space.[52] For instance, the PLA would likely jam U.S. satellite uplinks and downlinks to disrupt communication and navigation satellites critical to both the United States and Taiwan.[53] In addition, Chinese doctrine prioritizes jamming the U.S. global positioning system (GPS) to interfere with American precision-guided munitions and conducting offensive cyberattacks to disrupt U.S. satellite networks.[54] Should Beijing opt for further kinetic escalation in space, it could direct the PLA to use anti-satellite weapons against U.S. assets in orbit, though this would be a highly escalatory step. The PLA demonstrated this capability in January 2007, when it used a missile to destroy a Chinese weather satellite,[55] and it continues to test other anti-satellite weapons, including ground-based lasers.[56]

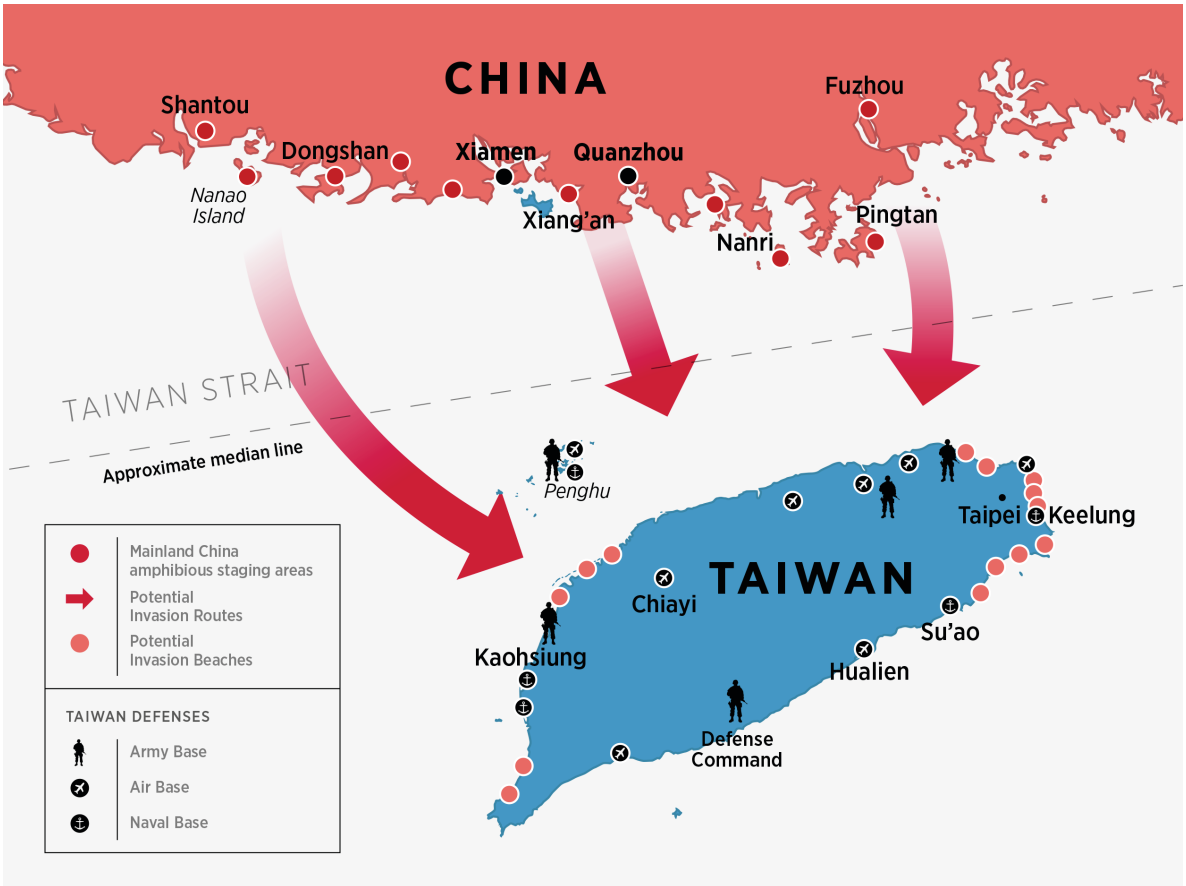
Chinese doctrine repeatedly emphasizes the importance of different PLA services synchronizing strikes across warfighting domains.[57] In conjunction with its attacks in space and cyberspace, Beijing would likely order the PLA to launch a "joint firepower strike campaign" against Taiwan.[58] Coordinated precision artillery strikes would likely target government and military facilities in Taiwan, aiming to cripple allied command and control.[59] To execute these efforts, the PLA Rocket Force already has positioned approximately one thousand mobile short-range ballistic missiles across the Strait, capable of reaching the island in eight minutes.[60] It also has approximately one thousand medium-range ballistic missiles likely intended to strike targets beyond Taiwan, such as U.S. assets stationed near

Guam.[61] This long-range arsenal includes the DF-26, a ballistic missile that can strike moving ships beyond the Second Island Chain, and the DF-17, which carries a hypersonic glide vehicle capable of reaching U.S. forces past the First Island Chain.[62] Although U.S. carrier battle groups have hundreds of interceptor missiles, they can be overwhelmed by large-scale missile barrages and must stay far from the Chinese mainland.[63]



U.S. forces lack sufficient stocks of long-range munitions for a conflict of this scale. American commanders would rely heavily on long-range weapons—such as Tomahawk cruise missiles and Long-Range Anti-Ship Missiles (LRASMs)—to strike PLA assets, but current inventories are limited.[64] The DoD has worked to invest more in long-range munitions and ramp up production; for instance, it directed Lockheed Martin to substantially increase its production rate of LRASMs in 2023.[65] However, LRASMs take two years to produce, cost $3 million each, and are only compatible with two types of U.S. aircraft.[66] This shortcoming in Washington's arsenal of long-range munitions, along with the PLA's vast arsenal of them, has created a "range gap," with China possessing longer-range weapons in greater quantities compared to the United States.

As Beijing subjects Taiwan to a barrage of artillery, it would likely position its PLAN fleet of 153 major naval surface combatants throughout the East and South China Seas.[67] Central to its plans are Renhai Guided Missile Cruisers and Luyang III Guided Missile Destroyers. Beijing has commissioned 25 Luyang III destroyers, each outfitted with 64-cell vertical launch systems capable of firing surface-to-air missiles, cruise missiles, and anti-submarine missiles. Additionally, eight Renhai cruisers are currently in service, each with 112 vertical launch systems cells designed to launch anti-submarine weapons, anti-ship missiles, surface-to-air missiles, and land-attack cruise missiles.[68] These ships would likely form Surface Action Groups near Taiwan and shield invasion forces during amphibious landings.[69] Their extensive firepower would extend China's anti-surface, air defense, and anti-submarine warfare capabilities further into the Pacific, creating new dilemmas for American and Taiwanese forces.[70]



Civilian roll-on/roll-off (RORO) ferries complement the PLAN's conventional warfighting capabilities. Despite China's significant investments in shipbuilding, the PLAN acknowledged in 2015 that it lacked enough amphibious landing ships to transport a PLA Army invasion force across the Strait. To address this gap,

Beijing began mandating that all civilian vessels be constructed to meet "national defense requirements."[71] By 2019, the PLA had access to at least 63 civilian ROROs capable of supporting military operations, giving it the capacity to transport and land more troops than the U.S. Navy.[72] In 2022, the PLA began incorporating ROROs into large-scale military exercises.[73] While it would be unlikely for Beijing to activate all of these dual-use ships for an invasion of Taiwan, they add to China's amphibious capabilities and would provide PLA commanders with a greater number of options to transport soldiers and equipment across the Strait to beachheads.[74]

The PLA has also developed an extensive air defense network to protect its forces and restrict enemy air operations. Ground-based systems in this network can engage targets up to 556 kilometers from the Chinese mainland.[75] The PLAN also contributes to the network—for instance, its destroyers are equipped with surface-to-air missiles capable of engaging targets up to 200 kilometers away.[76] These air defense systems would likely target Taiwanese and American aircraft conducting surveillance and attack operations near Taiwan and China, as well as defend military installations and population centers on the Chinese mainland.[77] Adding to this threat are advancements in the PLA's counter-drone capabilities, including high-power microwaves capable of destroying even small drones near its forces.[78]

All of these capabilities are meant to support the main spearhead of China's invasion strategy: the Joint Island Landing Campaign. The PLA Army has six amphibious combined arms brigades, four of which fall under Eastern Theater Command near Taiwan.[79] Their annual training includes individual and joint large-scale exercises designed to closely replicate the conditions of an amphibious landing on Taiwan.[80] In addition, they are positioned near ports of embarkation to facilitate rapid deployment with all necessary equipment and integrated tank, artillery, and infantry elements.[81] After landing, they would likely prioritize capturing and holding one of the few limited beachheads in Taiwan. If successful, the PLA would then face a challenging and costly campaign across Taiwan's mountainous and urban terrain, with the ultimate goal of seizing Taipei.[82]

The Technology

"The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him."

— Sun Tzu, *The Art of War*.[83]

Levels of Autonomy

As outlined in Section 2, China poses a significant threat to Taiwan given its ability to conduct complex naval operations around the island, coordinate multi-domain strikes on key targets, and transport invasion forces across the Strait using both military and civilian vessels. PLA attacks aimed at inflicting heavy losses on opposing forces and crippling allied surveillance and communication networks are central to Beijing's strategy. In this context, many U.S. defense officials consider autonomous weapon systems and the Replicator Initiative as critical to countering China's military threat. Autonomous weapon systems, if attritable, could help match the PLA's scale while also decreasing risk to U.S. military personnel and reducing the DoD's manpower requirements. As previously noted, the PLA will likely use electronic warfare to disrupt all forms of communication, underscoring the operational requirement for fully autonomous weapon systems that can operate without human guidance. Autonomous weapon systems could also theoretically execute tasks more efficiently and with quicker reaction times compared to remotely piloted or manned platforms. In other words, autonomous weapon systems promise to enhance both the mass and precision of U.S. forces—two critical qualities for degrading China's ability to seize Taiwan by force.[84]

Autonomy in warfare is not a new concept, nor is it specific to Replicator. Weapons designed to act without real-time human guidance have existed for centuries in one form or another, beginning with simple devices such as booby traps and mines triggered by tripwires. By World War II, belligerents developed and employed increasingly sophisticated weapons, such as homing torpedoes that could independently track targets after launch. The Cold War and information age fueled further advancements, such as "fire-and-forget" missiles and fully centralized systems such as the Aegis Combat System, which can detect, track, and engage air and surface threats with minimal human input. But with technology

advancing toward even greater levels of autonomy at the turn of the 21st century, the Office of the Secretary of Defense began evaluating policy guardrails and appropriate limitations for their deployment.[85]

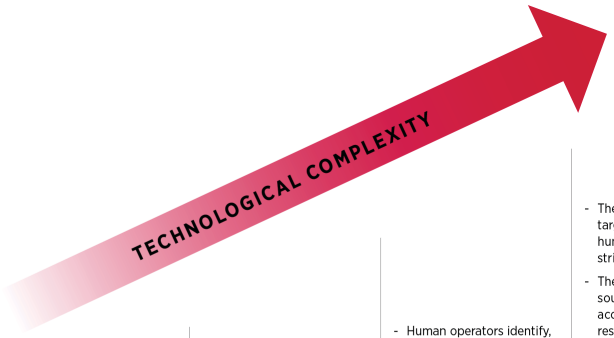
In November 2012, the DoD established its policy on autonomous weapon systems, DoD Directive 3000.09 ("Autonomy in Weapon Systems").[86] It created a department-specific definition of autonomous weapon systems as weapons that "once activated, can select and engage targets without further intervention by a human operator. This includes, but is not limited to, operator-supervised autonomous weapon systems that are designed to allow operators to override operation of the weapon system, but can select and engage targets without further operator input after activation."[87] The policy also defines semi-autonomous weapon systems as those "that, once activated, is intended to only engage individual targets or specific target groups that have been selected by an operator."[88]

Sea drones are among some of the first autonomous weapon systems that the DoD is deploying under Replicator. Early reporting on platforms pursued by the DoD through the Initiative include Anduril's Dive-LD, a portable USV capable of performing multi-week missions with minimal logistical support.[89] But even before Replicator, the DoD pursued maritime autonomous platforms for years; these include Sea Hunter, a USV tested in 2016 under DARPA's Anti-Submarine Warfare Continuous Trail Unmanned Vessel program, and Orca, a large UUV developed by Boeing and Huntington Ingalls Industries for missions including surveillance, anti-submarine warfare, electronic warfare, and minesweeping.[90] Although not publicly announced as part of Replicator, the DoD could pursue new minelaying platforms or acquire new naval mines as part of the Initiative. Currently, the U.S. Navy fields the Quickstrike family of air-dropped mines and the Submarine-Launched Mobile Mine, both equipped with fusing systems that detonate upon detecting vessel signatures. These mines are being upgraded with new GPS guidance and pop-out wing kits.[91] General Dynamics is also developing the Hammerhead, a modular mine capable of launching a homing torpedo after independently analyzing the signatures of nearby ships to identify whether they are hostile.[92]

In addition to Replicator's maritime systems, the DoD is pursuing a variety of airborne autonomous weapon systems. As an example, Hicks confirmed in May 2024 that the DoD would deploy the Switchblade 600 loitering munition system as part of the Initiative.[93] First produced by AeroVironment in 2011, an American

defense contractor, Switchblades can be pre-programmed against specific targets.[94] After launch, they use an internal navigation system, along with infrared and electro-optical sensors, to identify and engage their target.[95] Steve Gitlin, AeroVironment's Chief Marketing Officer, noted that the Switchblade "could lock in on a target, and the aircraft will basically maintain position on that target autonomously."[96]

Ukrainian forces have employed Switchblade loitering munitions and other kamikaze drones equipped with AI systems in their war against Russia. But these systems cannot operate without human intervention—in Ukraine, their role has been confined to target identification, navigation support, and countering electronic interference.[97] Switchblade requires operators to pre-program targets and allows "wave-off" commands when communications are uninterrupted. Human operators must manually direct kamikaze drones to a target area, after which they can be activated to independently pilot themselves in spite of electronic countermeasures.[98] These systems are thus likely assessed as semi-autonomous under DoD Directive 3000.09, falling at most into the category of level two or level three autonomy, as this report outlines in the table below.[99]



LEVEL 0	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
No Autonomy	**Low Autonomy**	**Partial Autonomy**	**Conditional Autonomy**	**High Autonomy**	**Full Autonomy**
Human-controlled	Human-controlled	Human-in-the-Loop	Human-in-the-Loop	Human-on-the-Loop	Human-out-of-the-Loop
Operates in **comms-available** environments to complete missions.	Operates in **comms-available** environments to complete missions.	Operates in **comms-available** environments to complete missions.	Operates in **comms-available** environments to complete complex missions.	Operates in **comms-degraded** environments to complete complex missions.	Operates in **comms-denied** environments to complete **highly** complex missions.
- All controls are fully manual, with a human directly piloting and managing all system functions without automated assistance.	- Human operators identify, confirm, and strike targets with onboard munitions. - Commanders provide mission guidance to human operators who execute missions. - Human operators navigate with assistance from GPS and visual sensors. - Human operators pilot the mission.	- Human operators identify, confirm, and strike targets with onboard munitions. - The system analyzes multi-source intelligence and accesses edge compute resources to identify targets. - The system receives human guidance for missions, normally within geographic boundaries. - The system navigates primarily with GPS and has a constant communication link with human operators. - Human operators pilot the mission.	- The system confirms targets for approval by human operators prior to strike. - The system analyzes multi-source intelligence and accesses edge compute resources to propose and improve target identification. - The system identifies specific pre-approved military targets within pre-assigned boxes of geographic coordinates. - The system receives human guidance for missions, normally within geographic boundaries. - The system navigates primarily with GPS. - The system pilots missions, but human operators can adjust or terminate the mission.	- The system independently identifies, confirms, and strikes targets with onboard munitions, but human operators can intervene. - The system uses line-of-sight communications to operate in swarms. - The system uses onboard intelligence collected using multi-source sensors, and has limited access to edge compute resources. - The system receives missions within a box of geographic boundaries and with a set of predetermined military targets. - The system navigates primarily with GPS, but has limited capability to use terrain-based navigation. - The system pilots independently, but human operators monitor and can terminate or adjust the mission.	- The system independently identifies, confirms, and strikes targets with onboard munitions. - The system uses line-of-sight communications to operate in swarms. - The system uses onboard intelligence data to plan and execute missions. - The system collects intelligence using multi-source sensors, independently analyzes the operational environment, and accesses edge compute resources to identify targets. - The system navigates using onboard inertial, vision-based, or terrain-based processing. - The system may receive guidance from commanders for missions within a "fenced" box of geographic boundaries. - The system pilots itself with complete independence, and human operators have a limited ability to terminate or adjust the mission when operating in comms-denied environments.

Fully autonomous weapon systems would utilize onboard sensors to identify, navigate to, and engage targets without human intervention. Human operators decide when and how to deploy level five autonomous weapon systems, but the systems do not require any human guidance once they are underway.[100] As previously noted, this enables autonomous weapon systems with level five autonomy to be effective in environments where adversaries are denying communication and navigation networks, which are essential to the operation of manned or lower-autonomy systems.[101] For level five autonomy, a critical criterion is an AI model's grasp of situational development: identifying causal factors in a battlespace and the ways that they could shift and change the battlefield. To achieve this, the AI models behind autonomous weapon systems with level five autonomy must prioritize which new data to collect. They must also be able to consistently interpret the intent of different objects and individuals on the battlefield based on their behavior.

Level five autonomous weapon systems remain under development in the United States and abroad; those with the power, range, and intelligence necessary to defend Taiwan are likely five or more years away. They hold considerable near-term potential, however, for a wide range of offensive and defensive applications in a U.S. conflict against China. While U.S. defense officials have not disclosed the autonomy levels of Replicator platforms, the DoD needs to develop autonomous weapon systems with high levels of autonomy (level four or level five) to counter PLA tactics aimed at disrupting traditional U.S. military assets. In a full-scale conflict over Taiwan, these systems would need to operate in large numbers, function in a denied electronic environment, and adapt to a rapidly changing battlespace.

Technology Requirements for Full Autonomy

The AI models powering autonomous weapon systems with level five autonomy must:

1. Enable navigation, target identification, and an adaptive understanding of military objectives in a contested combat environment;
2. Network with other autonomous weapon systems and UxS to coherently work interoperably in swarms;
3. Reliably execute an operational mission, namely delivering weapons payloads on the battlefield (for instance, attacking targets as a one-way attack drone or as a reusable platform that can deliver multiple munitions);
4. Make reliable, traceable decisions using incomplete information and in spite of an adversary's defenses and countermeasures;
5. Comply with domestic and international law, as well as operational requirements and rules of engagement from U.S. commanders.

To meet the requirements of level five autonomy, machine learning engineers, data scientists, and computer vision specialists can employ several advanced approaches to develop the underlying AI models. This report reviews four of these; the first is convolutional neural networks (CNNs), which are a type of supervised learning frequently utilized to help make predictions based on different data types. CNNs utilize a mathematical operation called convolution to analyze small portions of input data, such as parts of an image, in successive pieces. Information is then automatically simplified and condensed, helping to identify patterns regardless of their location in the data. This process enables AI to detect basic features from data—such as edges or variations of color in an image—and use them to recognize more complex features in detected objects, such as the body of a submarine or naval vessel.[102] For example, companies such as Tesla and Waymo leverage CNNs to process and interpret video data from autonomous vehicle sensors in real time.[103] The U.S. defense industrial ecosystem launched initial experimentation with CNNs in 2019, when the Defense Advanced Research

Project Agency developed an AI algorithm called AlphaDogfight that successfully controlled a fighter aircraft in a simulation against a real human pilot and won in five one-on-one dogfights.[104]

Second are generative adversarial networks (GANs), deep learning models incorporating unsupervised learning and aspects of supervised learning. They have gained significant attention in the U.S. defense community for their ability to generate realistic synthetic data, which makes them particularly valuable for situations where real-world data is insufficient or not available (the importance of high-quality data is discussed later in this section). GANs consist of two contesting systems: a generator and a discriminator. The generator produces synthetic data, and the discriminator tries to identify what is "real" data—as designated by the DoD—against the synthetic data created by the generator.[105] Outcomes from these competitions, whether the discriminator correctly identified the real data or incorrectly identified synthetic data, are fed back to both systems, which iteratively improves both the generator's effectiveness in producing high-quality synthetic data and the discriminator's capacity to distinguish between real and synthetic data. This makes GANs a useful component for creating comprehensive synthetic environments to train autonomous weapon systems; for example, refining the underlying AI model and its ability to identify targets, detect anomalies during missions, and navigate complex terrain.[106] Despite their utility, using GANs and synthetic data entails significant risks and limitations. Any potential flaws in the synthetic data would be amplified, leading to large-scale inaccuracies, and the models would require ongoing human oversight for fine-tuning and evaluation, thereby reducing rapid scalability.

Third are recurrent neural networks (RNNs), a type of supervised deep learning that can identify trends in sequences of data by maintaining a form of memory of previous inputs. This capability makes RNNs particularly effective for tasks where the order, context, and interdependence of data points are critical.[107] Researchers have demonstrated that RNNs have the potential to improve autonomous vehicles' ability to detect and identify man-made objects, even underwater.[108] This could, for instance, enable an underwater autonomous weapon system to track the movements of PLA Navy submarines and aid targeting based on predictions of their future positions. RNNs can also help manage autonomous weapon systems' interactions with nearby platforms and translate sensor data directly into driving instructions.[109]

Fourth are liquid neural networks. These AI models, a type of RNN, differ from traditional models like CNNs and GANs by continuously adjusting their behavior in real time based on incoming data.[110] The term "liquid" reflects the network's flexible structure, with each connection point in the AI model modifying its settings on the fly. This adaptability allows the system to evolve and respond to new patterns or anomalies, enhancing its ability to handle unexpected situations and sequential data.[111] For example, research at MIT supported by the U.S. Air Force demonstrates that liquid neural networks can enable drones to apply learning from how to locate objects in a forest during summer to locating the same objects in winter or urban settings, in conjunction with varied tasks like seeking and following.[112]

Data and Training

Given the potential risks and unintended consequences of deploying autonomous weapon systems with U.S. forces during crises or wartime, policymakers and legal advisors must understand the processes for designing and developing their underlying AI models. This process begins with the collection of multimodal data on terrain and an adversary's military assets—such as vehicles, infrastructure, and personnel—to create large, high-quality datasets. Relevant intelligence collection methods include imagery and electronic intelligence, such as high-resolution satellite images of military facilities in China, synthetic aperture radar scans of concealed PLA assets, acoustic and infrared signatures from PLAN ships in emissions control status, and radar signals from PLA air defense systems.[113]

Much of this real-world data will likely come from PLA exercises simulating potential Chinese actions against Taiwan. For instance, U.S. and allied forces almost certainly collected extensive intelligence on the PLA's full-scale military exercises conducted in May 2024 around Taiwan and its islands near the Chinese mainland.[114] Order-of-battle datasets on PLA military assets will also be important; although some of this information may come from open-source imagery providers, most of it will likely be collected using classified sources. Given the classification of both the training data and the imagery, AI models will also have to be classified at the same level. This classification will affect the model's development—all developers must have the necessary clearances, and the models must be stored on government-approved systems.

The next step is to transform this data; in other words, pre-processing the data by cleaning, organizing, and labeling it. This is essential in training AI models to recognize, for example, the signatures of PLA naval vessels through a process of trial and error. As former DoD Chief Digital and AI Officer Craig Martell emphasized, "If we're going to beat China in AI, we have to find a way to label at scale."[115] Data transformation also includes augmentation—flipping, rotating, cropping, scaling, or adding noise to the data. Through data transformation that creates training datasets reflecting a broader combination of environments and conditions, AI models for autonomous weapon systems will be more generalizable and robust across different contexts.

> "Level five autonomous weapon systems with the power, range, and intelligence necessary to defend Taiwan are likely five or more years away."

Scientists and engineers then use this transformed data to train baseline AI models for autonomous weapon systems, with CNNs supporting sensor fusion and RNNs enhancing the processing of temporal data for tasks such as object detection and predictive analysis, respectively.[116] The creation of many of these AI models can benefit from transfer learning, a technique used to leverage pre-trained AI models originally optimized for one task to form the basis of a model built to address a distinct but similar task. This method applies general patterns from initial training to create a robust foundation to start from, reducing training time and the need for extensive real-world data while also improving accuracy. It is especially useful when data is limited.[117] For example, the software behind U.S. autonomous weapon systems intended for a fight against China could leverage AI models created for environments like Ukraine or Syria. As with other AI techniques, transfer learning can be used alongside methods such as CNN training.

From here, the AI models can refine their decisionmaking through supervised learning, a common method of training that provides the model with label datasets of targets and then receives direct feedback from a targeting expert. For example, a typical model for autonomous weapon systems would start development with a labeled set of several thousand images of PLA military hardware. During training, the model would receive new data, which it would then attempt to confirm as a valid target. At that point, a human targeting expert would confirm whether the model had correctly identified the target, allowing it to adjust and improve. Developers can also use unsupervised learning to bolster the

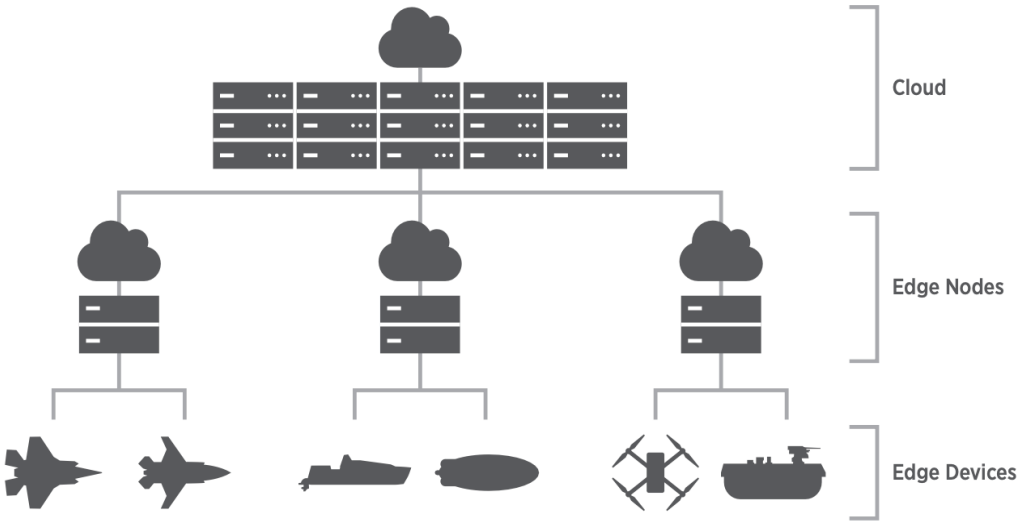
AI models' ability to process sensor data—such as radar or infrared signatures—to distinguish PLA military targets from non-combatants. Unsupervised learning does not use labeled data; the model analyzes vast amounts of unlabeled data to identify unusual groupings or communication patterns of objects that, for example, likely represent a formation of PLA targets. Likewise, these models can be used to help autonomous drone swarms navigate without GPS to targets within a specific geographic box and provide optimal approaches for an attack.[118]

Another important machine learning technique used could be reinforcement learning: the AI model trains by testing actions in its environment and being rewarded or penalized accordingly. Through this process of trial and error, akin to how humans learn from experience, it trains on which actions yield the most favorable outcomes based on its incentives over time, gradually improving its performance per the incentives. For instance, researchers from the Dalian University of Technology in China have proposed using a special kind of reinforcement learning using deep neural networks to make an AI model that can use basic fighter maneuvers to win a dogfight in a simulated environment.[119] Researchers from the U.S. Army Engineer Research and Development Center have used reinforcement learning techniques in mission engineering and combat simulations to train agents that can interpret environments and make informed decisions without direct human intervention.[120]

Once these AI models achieve satisfactory levels of performance, they can be deployed and integrated into autonomous weapon systems. However, as with manned weapon systems, the development and training of autonomous weapon systems will be an ongoing process that never truly ends. To maintain reliability and adaptability, engineers and scientists must continuously integrate, test, and deliver changes for autonomous weapon systems' AI models. This includes testing and monitoring the performance of autonomous weapon systems with new AI models in real-world environments, an important step to detect performance degradation over time and assess whether their training data still reflects the environments in which they operate. The DoD must also ensure that these AI models are scalable to manage large data volumes and high traffic without losing performance or precision. At the same time, it should prioritize developing and testing alternative AI models for autonomous weapon systems as a contingency to preempt foreseeable issues that could arise in primary AI models.

Platform and Computing Hardware

In most cases, autonomous vehicles for commercial or military applications rely on wireless communications to access databases and computing power hosted on distant servers. In the context of autonomous weapon systems operating in defense of Taiwan, however, PLA electronic warfare will result in contested, communication-denied areas. To address this challenge, autonomous weapon systems must utilize edge computing; for a fight in the Indo-Pacific against the PLA, AI model processing would need to largely occur locally inside the autonomous weapon system itself rather than relying on cloud-based systems.[121] By eliminating dependence on data transmissions to distant external servers, particularly those that the PLA can readily weaken or disrupt, edge computing can enable AI models for autonomous weapon systems to rapidly process data and make decisions.[122]



HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

AI models operating on edge within autonomous weapon systems platforms require energy-efficient computing to process large volumes of real-time data for tasks such as object detection and avoidance. Most military platforms currently in service, however, lack the resources necessary to handle multiple complex tasks simultaneously for extended periods as is often required in combat. One of the greatest limitations is the significant electric power required for autonomous

weapon systems.[123] As a hypothetical example, consider a 20-kilogram hexacopter designed to drop explosives, powered by a lithium-ion battery with an energy density of 250 watt-hours per kilogram.[124] A 6-kilogram battery pack—making up 30% of the hexacopter's total weight—would provide it with a total energy capacity of 1,500 watt-hours.[125] If the hexacopter consumes power at a rate of 3,000 watts (for flight and running the AI algorithm), flying at an average speed of 50 kilometers per hour, it could theoretically operate for 30 minutes and cover up to 25 kilometers before depleting its battery.[126] These calculations are approximate; real-world performance would depend on various factors, including the autonomous weapon systems' payload, power management system, environmental conditions, and specific mission profile. Researchers are also actively developing new battery technologies with the potential for much higher energy densities than current lithium-ion batteries. In 2023, for instance, scientists at the Chinese Academy of Sciences' Institute of Physics reportedly created a rechargeable pouch-type lithium battery capable of achieving 711 watt-hours per kilogram.[127] But despite new innovations such as this, scaling production of this technology to be cost-effective and suitable for autonomous weapon systems will take many years or decades.

The computational, memory, and energy requirements of advanced AI models running in fully autonomous weapon systems also impose limitations, requiring developers to make trade-offs between the speed and accuracy of underlying AI models. This is because precise AI models often demand more power resources and time, while faster, lower-power AI models may compromise in terms of their levels of accuracy.[128] Techniques like compression, which reduces the number of bits required to store or transmit data, and pruning, which involves removing less significant parts of the AI model to make it more efficient without significantly affecting performance, can help improve the efficiency of AI models. In addition, parallel computing has the potential to help address computational and memory limitations by improving efficiency; by dividing tasks among multiple processors for simultaneous execution, parallel computing can reduce execution time and decrease power consumption per computation, thereby minimizing total energy use.[129] Using these techniques, scientists and engineers must collaborate with military personnel, working together to find an optimal balance between the AI models' speed and accuracy.

Law and Policy

"Until wars are really fought with pawns, inanimate objects and not human beings, warfare cannot be isolated from moral life."

— Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations.*[130]

War and Peace in the Strait

Long-standing debates over the strategy, policy, and legality of U.S. military intervention would be central to White House decisionmaking in a Taiwan contingency. The deployment and use of autonomous weapon systems, however, would also introduce new legal and policy considerations, altering the crisis's overall character. Under what conditions would the recourse to military force be justified? If a state of armed conflict exists, what actions by autonomous weapon systems would be permissible under the international laws on the conduct of warfare? What U.S. domestic laws and policies would govern American forces' employment of autonomous weapon systems in the defense of Taiwan? And in what ways would the governance of autonomous weapon systems differ from that of manned military assets?

Legal analysis for the kinetic use of autonomous weapon systems would begin at the international level, focusing on a U.S. recourse to military force under international law as rooted in binding treaties and customary state practice. Article 2(4) of the United Nations Charter prohibits member states of the organization from using or threatening force "against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations."[131] The Charter recognizes two exceptions to this rule: the right of member states to self-defense—individually or collectively—in response to an armed attack (Article 51), and the use of force as authorized by the United Nations Security Council (Article 42).[132] Although the Charter applies only to United Nations member states and Article 51 permits self-defense only after an armed attack has taken place, customary international law recognizes a fundamental right of legitimate polities to self-defense, including preemptive self-defense in cases of "instant, overwhelming" necessity, with "no choice of

means, and no moment for deliberation."[133] In other words, Washington could plausibly invoke customary international law as justification to use force in defense of Taiwan after an armed attack has begun or to preemptively use force in anticipation of an imminent and unavoidable attack.

As previously highlighted in this report, China's most likely initial military course of action against Taiwan would be the imposition of a swift maritime blockade in the waters around the island, something which Beijing could escalate into a full invasion. Although blockades are an act of war under contemporary international law, Washington likely would refrain from immediately recognizing a blockade by China as the start of an armed conflict to preserve potential pathways for deescalation. The United States could likely find adequate legal justification for using force—including the direct employment of autonomous weapon systems—to try and break China's grip over the island. That noted, if Washington opted for limited military actions in an attempt to compel China to stand down, senior U.S. leaders would likely avoid using autonomous weapon systems because of the risk that even small miscalculations on the use of kinetic force could lead to dramatic conflict escalation.

Rules in War

Assuming the United States has legal grounds to use force in the defense of an invasion of Taiwan, legal analysis of U.S. options would then shift to examining the application of the Law of Armed Conflict (LOAC).[134] This framework, which refers to the international legal regime governing conduct in war and the protection of those not actively engaged in hostilities, directly applies to any potential U.S. employment of autonomous weapon systems—the DoD's interpretation of LOAC will be codified in the AI algorithms for autonomous weapon systems. The U.S.-led Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy, endorsed by 54 states as of March 2024, provides a framework of non-binding principles to ensure that militaries' uses of AI, including autonomous weapon systems, align with LOAC.[135]

Autonomous weapon systems will be better suited to comply with LOAC for a U.S defense against an invasion of Taiwan compared to other combat environments. Unlike counterinsurgency and counterterrorism operations in the Middle East, where combatants often conceal themselves among civilians, PLA forces and

PLAN warships would primarily operate in the waters around Taiwan. Rising tensions would likely prompt shipping companies to reroute away from the region, leaving primarily ships that are actively involved in hostilities.[136] This maritime setting, characterized by a limited number of noncombatants and clearly defined military targets, would simplify the task of autonomous weapon systems identifying and engaging PLA assets.

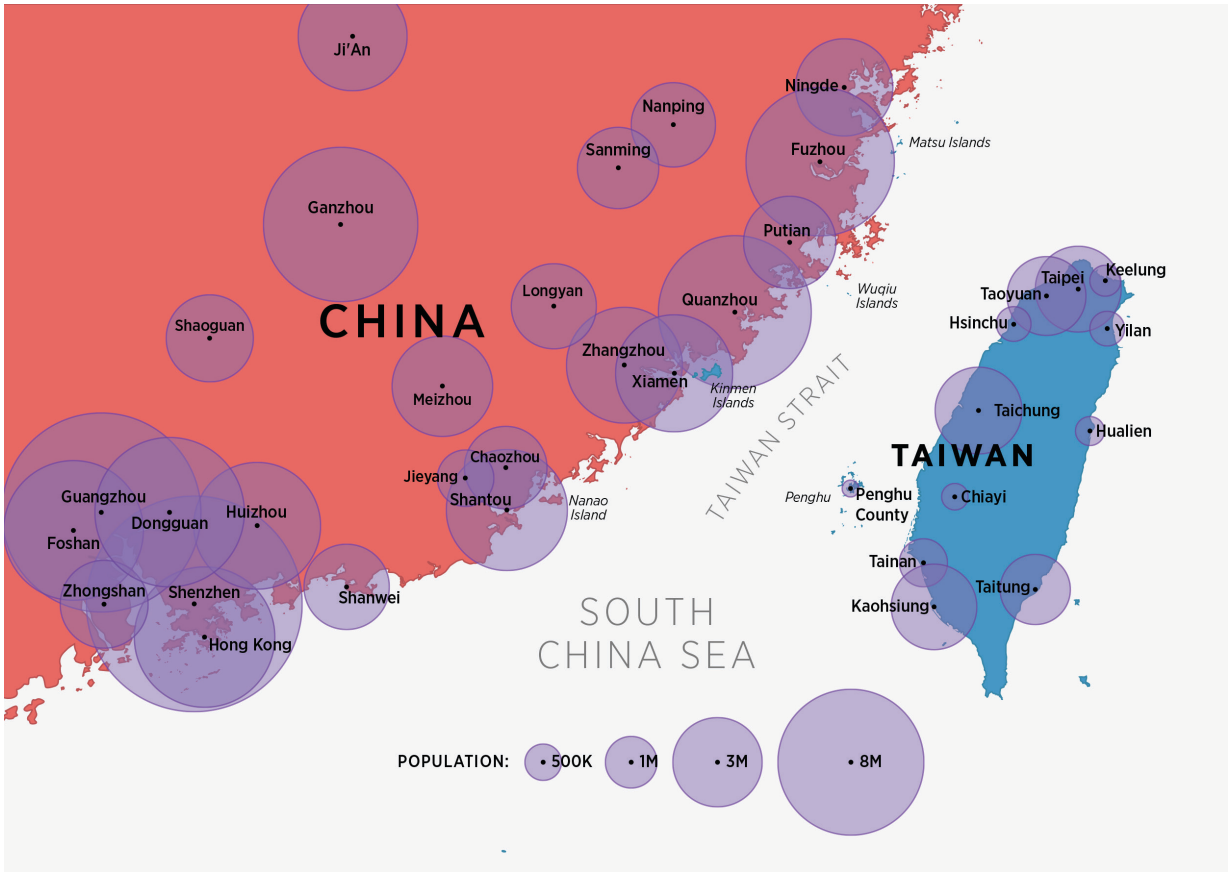
Attacking targets on the Chinese mainland, however, would be considerably more complex from both the operational and the international legal perspective. Due to concern over escalation, the President is unlikely to authorize any preemptive strikes against targets on the Chinese mainland unless an invasion appears inexorable and imminent. If a PLA amphibious invasion of Taiwan is clearly underway, the President would almost certainly authorize such strikes using both traditional military assets and autonomous weapon systems. Even so, using autonomous weapon systems to attack targets in mainland China would raise many more legal concerns due to the presence of noncombatants and civilian infrastructure.

> "The DoD's interpretation of international law would be embedded in the AI algorithms for autonomous weapon systems."

Any evaluation of the employment of autonomous weapon systems necessitates a thorough evaluation of the application of LOAC—this report analyzes four of its core principles.[137] The first is distinction, which requires belligerents to discriminate between civilian objects and legitimate military targets such as enemy combatants, weapons systems, or infrastructure serving a military purpose. To ensure that fully autonomous weapon systems can meet this standard, developers must use supervised learning with carefully labeled real and synthetic data that is then reviewed by LOAC experts. Through this process, the DoD can train AI models for autonomous weapon systems to recognize the differences between military and noncombatant objects, adjusting their actions accordingly. For example, using real and synthetic data, developers can run simulations that have AI models determine whether a ship is a combatant or noncombatant. Algorithms weighed by the developers would then assess strike decisions made in this simulated environment for compliance with the principle of distinction, thereby providing feedback for training the AI models. Through this process, the AI model will evolve to assess distinction using the same criteria applied by human lawyers and operators.

Another key principle relevant to autonomous weapon systems is proportionality—for any military action, unintended harm to noncombatants and civilian objects cannot exceed the anticipated military advantage.[138] The DoD Law of War Manual mandates that proportionality assessments focus directly on an attack's expected civilian casualties; by limiting consideration to effects that are "both expected and not too remote," commanders must weigh collateral damage against immediate tactical gains, preventing justification for civilian casualties based on strategic objectives and long-term consequences.[139] Under many circumstances, the platforms that the Replicator Initiative aims to field could ease these concerns, as their smaller warheads and greater precision likely reduce their kill radius compared to conventional munitions such as Hellfire missiles with 100-pound explosive warheads. Given the need for AI models to make legal interpretations, core aspects guiding assessments of the principle of proportionality will be coded across fully autonomous weapon systems, rather than simply being assessed by human operators on an individual target-by-target basis.[140]

Closely related to proportionality are two additional LOAC principles: necessity and precaution. Under the principle of necessity, military action is permitted only if it is essential to achieve a legitimate military objective under LOAC, i.e., weakening an adversary's military capacity.[141] Under the principle of precaution, belligerents must take all feasible measures to minimize harm to civilians.[142] In applying both of these principles, U.S. commanders must evaluate whether the use of autonomous weapon systems would minimize harm compared to more traditional weapon systems. For instance, if U.S. forces needed to target a PLA command center in an urban area, intelligence might indicate that a swarm of autonomous weapon systems would have a 90% chance of destroying the command center but would incur 100 civilian casualties. Employing a strike package of manned fighters, by contrast, might have a 60% success rate, with half the civilian casualties but also the loss of several U.S. pilots. Would the use of autonomous weapon systems in this scenario align with the principle of precaution? Alternatively, if autonomous weapon systems showed significantly greater precision than manned aircraft, would the principle of precaution compel their use?



As stated earlier, the DoD will need to use synthetic and real-world data for training autonomous weapon systems to be effective in combat and adhere to established norms of acceptable conduct in war. This very likely involves the training of AI models in simulated environments to ensure their actions align with international law, much like a jury determines facts and renders a verdict in court. Lawrence Lessig's assertion that "code is law" is consistent with this notion; just as the software and hardware of cyberspace shape online behavior in ways similar to legal codes, the DoD's interpretation of international law would be embedded in the AI algorithms for fully autonomous weapon systems, effectively serving as a codification of the DoD's approach to the laws of war.[143]

A rare combination of technical, operational, and legal expertise is necessary for the creation and modification of training data on LOAC assessments. Few military lawyers possess the necessary proficiency or regular experience with real-world targeting decisions to ensure reliable assessments. Even fewer understand the precise sequencing and timing needed to strike mobile targets in complex, urban environments. To ensure that fully autonomous weapon systems comply with LOAC, the DOD must continue to assemble experienced operators, military

lawyers, scientists, and engineers. This group must collaborate to evaluate simulated targeting decisions for AI models and label data, ensuring this process informs the development of software from its inception.[144]

When interpreting LOAC principles, military personnel and the AI algorithms behind autonomous weapon systems face the challenge of comparing apples to oranges; with the principle of proportionality, for instance, potential harm to noncombatants cannot be empirically weighed against the unquantifiable concept of military advantage. This reflects the inherent challenges of applying normative standards to the conduct of war. Much of LOAC was deliberately codified as qualitative standards rather than strict rules to avoid the arbitrary and unjust application of fixed ratios alone to assess compliance. Such interpretations, however, are inherently subjective. When interpreting LOAC principles, the AI models for fully autonomous weapon systems will be held to the same standard of reasonableness as humans. Therefore, the critical question is how to ensure AI models for fully autonomous weapon systems can interpret subjective principles with relative consistency despite identical inputs resulting in different outputs—a defining feature of all AI systems. The technical challenge of ensuring consistent LOAC interpretation is more complex than refining relatively straightforward foundational tasks such as target recognition.[145]

U.S. Policy

Given the novelty of autonomous weapon systems and the risk that an AI-powered weapon could inadvertently escalate a crisis between the United States and China, the final decision approval for the operational use of such weapons would almost certainly rest with the President. Thus, it is important to distinguish between the broader legal authority to take military action and the President's strategic decision of whether to employ a novel weapon system.

At the departmental level, DoD Directive 3000.09 establishes the policy framework and requirements for designing, developing, and deploying autonomous weapon systems. This includes guidance for ensuring that autonomous weapon systems comply with international legal regimes such as LOAC and U.S. domestic law. By creating a supplemental review process to introduce autonomy in the U.S. military, the original 2012 version of DoD Directive 3000.09 is distinguished in its transparency. In contrast to the secrecy characterizing other countries' policies on

autonomous weapon systems, it created explicit guidelines for their responsible development and use, establishing a critical foundation for accountability and positioning the United States as a leader in international discussions on autonomy in warfare.

The 2012 version of DoD Directive 3000.09 did not specifically authorize autonomous weapons systems to take lethal action without human oversight. Carter affirmed this stance in 2016, stating that "whenever it comes to the application of force, there will never be true autonomy, because there'll be human beings (in the loop)."[146] The January 2023 version updated an already rigorous approval process, including required adherence to the DoD Principles for Ethical Artificial Intelligence. Prior to the "formal development" of autonomous weapon systems as defined by the DoD, approvals are required from the Under Secretary of Defense for Policy, the Under Secretary of Defense for Research and Engineering, and the Vice Chairman of the Joint Chiefs of Staff.[147] Additional approvals are needed from the Under Secretary of Defense for Policy, Under Secretary of Defense for Acquisition and Sustainment, and Vice Chairman of the Joint Chiefs of Staff "before fielding" autonomous weapon systems as defined by the DoD.[148]

Fielding refers to the distribution and integration of a weapon into the U.S. military's operational inventory, marking its readiness for use beyond testing, exercises, or experiments.[149] Deployment, in contrast, involves the assignment and movement of a fielded weapon to specific operational areas or their use in military missions. After the DoD has approved such a system for fielding, its deployment around Taiwan would likely require additional national-level approvals from the Secretary of Defense and the President due to the sensitivities and strategic implications of using it.

The need for fully autonomous weapon systems to comply with international and domestic law highlights the challenge of addressing the "Black Box Dilemma" posed by advanced AI systems.[150] Ideally, all AI systems should possess explainability, allowing humans to understand and interpret the decisions of the underlying AI model. Similar to deep learning algorithms in commercial autonomous systems, however, the decisionmaking processes of AI models for fully autonomous weapon systems will be too complex to provide semantic explanations understandable by humans. From a technical perspective, experts recognize the trade-off between accuracy and explainability in advanced AI

models, including those used for fully autonomous weapon systems. In short, a more simplistic AI model might produce explainable results, but lower levels of sophistication would result in less accurate and reliable outcomes.[151] Current U.S. defensive weapon systems—such as the Aegis Combat System and the Patriot surface-to-air missile system—already operate at levels of autonomy that are not explainable; they have the capability to independently identify and engage threats, often without human operators fully understanding their decisionmaking.[152]

Since the AI models powering fully autonomous weapon systems will make decisions about lethal action, engineers should prioritize greater accuracy over explainability to ensure that these systems comply with LOAC to the greatest extent possible.[153] Given the challenge of deep learning models providing semantic explanations for lethal actions, most advanced models now strive for "traceability." A model with strong traceability allows leaders to trace the processes of an AI model—such as the underlying data, algorithms, and final choices—essential for holding leaders accountable for the use of autonomous weapon systems and lethal military actions.[154] With this in mind, DoD Directive 3000.09 thus mandates that autonomous weapon systems, as defined by the DoD, "will go through rigorous hardware and software" validation and testing to ensure that they are "traceable" and "reliable."[155]

At the operational level, DoD Directive 3000.09 requires that military AI systems "allow commanders and operators to exercise appropriate levels of human judgment over the use of force in the envisioned planning and employment processes for the weapon."[156] Although this may initially seem to suggest that decisions to employ autonomous weapon systems against China could be pushed down to the tactical level (as suggested by "commanders" and "operators" exercising judgment), the Secretary of Defense ultimately needs to approve all rules of engagement—including those relevant to autonomous weapon systems—developed by the Commander of Indo-Pacific Command. Therefore, autonomous weapon systems' underlying AI algorithms must be capable of aligning their decisionmaking with directives from commanders, particularly as it relates to LOAC and the rules of engagement. Rules of engagement for autonomous weapon systems will likely operate at two levels; foundational rules codifying LOAC and DoD policy will be deeply embedded in the AI model, while commanders will develop operational rules of engagement when deciding how to employ autonomous weapon systems in specific areas of operations and within specific tactical contexts.

Strategy, Risk, and the Security Dilemma

Three additional conditions are necessary to successfully employ autonomous weapon systems in a Taiwan contingency. First, U.S. military planners must continue to develop mature concepts of operations that integrate autonomous weapon systems into existing war plans. Second, the United States must ramp up its production of autonomous weapon systems. Third, U.S. autonomous weapon systems must be prepositioned in theater to enable rapid deployment when needed.

Beyond policies governing the use of AI-enabled systems in armed conflicts, U.S. officials must also weigh the potential long-term strategic consequences of developing and deploying autonomous weapon systems. The most consequential of these strategic consequences is the potential for autonomous weapon systems to exacerbate the U.S.-China security dilemma, fueling the proliferation of autonomous weapon systems or stoking an arms race that ultimately favors Beijing due to its industrial capacity, lower production costs, and consistent disregard for international law.[157] The large-scale deployment of U.S. autonomous weapon systems could prompt China to mass produce weapons meant to counter autonomous weapon systems, more conventional military hardware, or its own autonomous weapon systems in response, further fueling the security dilemma and increasing the likelihood of conflict. China's ability to field larger quantities of autonomous weapon systems could offset any qualitative advantage achieved by U.S. systems.[158]

The Security Dilemma and U.S.-China Military Competition

The security dilemma is an international relations concept describing how states seeking to enhance their security by undertaking certain actions—such as amassing arms stockpiles or conducting military drills—often provoke rivals to do the same, creating a cycle of mutual hostility that increases the likelihood of conflict.[159] Many theories attempt to explain the behaviors of revisionist powers that drive security dilemmas. One theory argues that power-hungry states fuel the security dilemma in pursuit of nationalist, ideological, or authoritarian motives.[160] Contrasting theories suggest that the security dilemma arises from states seeking protection or buffers against perceived threats due to security-based motives.[161] The balance between offensive and defensive military capabilities can affect the severity of the security dilemma; states are more likely to engage in military competition or conflict when offense is easier than defense, whereas stronger defensive capabilities tend to make states more secure and reduce military competition.[162]

Generally speaking, military innovation is a constant cycle of competition, where no technology, including autonomous weapon systems, provides a permanent advantage. Each advancement spurs the development of countermeasures, shifting the advantage between the offense and defense.[163] Replicator reflects this reality through its focus on improving and expediting the development, production, and acquisition of autonomous weapon systems, along with a wide array of other advanced military technologies necessary to improve overall warfighting capability.

If China's industrial capacity remains strong, Beijing will likely have the capability to produce a larger quantity of autonomous weapon systems compared to the United States, produce systems meant to counter autonomous weapon systems faster than the United States grows its arsenal of autonomous weapon systems, or produce more traditional military platforms than U.S. autonomous weapon systems can help counter. The key questions, then, are whether the United States can sustain its lead in the next evolution of military advancements, whether the United States or China will have better quality autonomous weapon systems, and

whether the PLA's defensive systems can effectively counter autonomous weapon systems. For the latter, the closest parallels to mass deployments of autonomous weapon systems are Iran and Russia's recent UAV attacks against Ukraine and Israel respectively, neither of which were effective in themselves due to strong air defenses.[164] As noted earlier in this report, Secretary of Defense Lloyd Austin recently introduced counter-UxS as a new tranche of Replicator to address the evolving need for defensive systems. Similarly, China's advanced air defense and counter-UAV systems are likely to reduce the effectiveness of U.S. autonomous weapon systems in a conflict. Regardless, Beijing will likely begin integrating PLA-fielded autonomous weapon systems as a central component of any military operation China takes against Taiwan.

In the far future, if autonomous weapon systems or other AI-enabled military systems enable quicker and more effective warfighting compared to traditional manned platforms, a state that employs them aggressively at the onset of a conflict could have a decisive advantage. This offense-dominant dynamic could incentivize belligerents—particularly those with weaker conventional forces not employing autonomous weapon systems—to threaten vertical escalation.[165] However, this pattern of states seeking offset strategies to asymmetrically counter adversaries in response to their military innovation is not new. Rather, it is a normal part of interstate military competition and offset strategies. Autonomous weapon systems will likely not immediately meet the high expectations of technology optimists. It will take time for developers to hone the AI models for autonomous weapon systems and improve their performance, and the current limitations of autonomous weapon systems mean they are unlikely in the near term to alter the U.S.-China military balance.

The gradual advancement of technology in the Ukraine War is a clear illustration of this dynamic. Even if autonomous weapon systems eventually have the capability to successfully degrade a PLA invasion force crossing the Taiwan Strait, the PLA will maintain significant capabilities with its artillery, aviation, and air defenses that autonomous weapon systems cannot defeat alone. As is the case with most new military platforms, autonomous weapon systems will likely catalyze evolutionary changes in the character of conflict, rather than instantly conferring Washington with an untouchable edge in conventional warfighting.

Endnotes

1. "Deputy Secretary of Defense Kathleen Hicks' Remarks: "Unpacking the Replicator Initiative" at the Defense News Conference (As Delivered)," U.S. Department of Defense, September 6, 2023, https://www.defense.gov/News/Speeches/Speech/Article/3517213/deputy-secretary-of-defense-kathleen-hicks-remarks-unpacking-the-replicator-ini/.
2. "SIPRI Military Expenditure Database," Stockholm International Peace Research Institute, https://doi.org/10.55163/CQGC9685.
3. *Military and Security Developments Involving the People's Republic of China*, Office of the Secretary of Defense, October 19, 2023, V-VII, https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.
4. Ryan Fedasiuk, *Chinese Perspectives on AI and Future Military Capabilities*, Center for Security and Emerging Technology, August 2020, 15, https://cset.georgetown.edu/publication/chinese-perspectives-on-ai-and-future-military-capabilities/; Jacob Stokes, *Military Artificial Intelligence, the People's Liberation Army, and U.S.-China Strategic Competition: Testimony before the U.S.-China Economic and Security Review Commission*, Center for a New American Security, February 1, 2024, https://www.cnas.org/publications/reports/u-s-china-competition-and-military-ai.
5. Center for Preventive Action, "Confrontation Over Taiwan," Council on Foreign Relations, updated July 1, 2024, https://www.cfr.org/global-conflict-tracker/conflict/confrontation-over-taiwan.
6. Heather R. Penney, "Scale, Scope, Speed & Survivability: Winning the Kill Chain Competition," *Mitchell Institute Policy Paper* 40, May 2023, 8-10, https://mitchellaerospacepower.org/wp-content/uploads/2023/05/Scale_Scope_Speed_Survivability_-KillChain_-Policy_Paper_40-New.pdf.
7. Mark F. Cancian, Matthew Cancian, and Eric Heginbotham, *The First Battle of the Next War: Wargaming a Chinese Invasion of Taiwan*, Center for Strategic and International Studies, January 9, 2023, 88-137, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/230109_Cancian_FirstBattle_NextWar.pdf?VersionId=WdEUwJYWIySMPIr3ivhFolxC_gZQuSOQ; Stacie L. Pettyjohn, Becca Wasser, and Andrew Metrick, Bad Blood: The TTX for the House Select Committee on Strategic Competition Between the United States and the Chinese Communist Party (CCP), Center for a New American Security, April 26, 2023, https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/Pettyjohn-Wasser-Metrick-Statement-for-the-Record-for-House-Select-Committee-on-China.pdf?mtime=20230427122552&focal=none.
8. J.D. Leipold, "Innovation, technology keys to Army maintaining 'overmatch,'" U.S. Army, September 21, 2015, https://www.army.mil/article/155576/innovation_technology_keys_to_army_maintaining_overmatch.
9. C. Todd Lopez, "Competition With China Drives FY 2024 Budget Request," U.S. Department of Defense, March 28, 2023, https://www.defense.gov/News/News-Stories/Article/Article/3343663/competition-with-china-drives-fy-2024-budget-request/.
10. "Deputy Secretary of Defense Kathleen Hicks Keynote Address: 'The Urgency to Innovate,'" U.S. Department of Defense, August 28, 2023, https://www.defense.gov/News/Speeches/Speech/Article/3507156/deputy-secretary-of-defense-kathleen-hicks-keynote-address-the-urgency-to-innov/.
11. "Defense Innovation Unit (DIU)," Defense Innovation Unit, https://www.diu.mil/about.
12. "DIU Turns 7!," Defense Innovation Unit, August 25, 2022, https://www.diu.mil/latest/diu-turns-7.
13. "Defense Innovation Unit (DIU)," Defense Innovation Unit, https://www.diu.mil/about.
14. "Secretary of Defense Lloyd J. Austin III Announces New Director of the Defense Innovation Unit," U.S. Department of Defense, April 4, 2023, https://www.defense.gov/News/Releases/Release/Article/3351281/secretary-of-defense-lloyd-j-austin-iii-announces-new-director-of-the-defense-i/.
15. "Replicator," Defense Innovation Unit, https://www.diu.mil/replicator; "Deputy Secretary of Defense Kathleen Hicks Announces Additional Replicator All-Domain Attritable Autonomous Capabilities," U.S. Department of Defense, November 13, 2024, https://www.defense.gov/News/Releases/Release/Article/3963289/deputy-secretary-of-defense-kathleen-hicks-announces-additional-replicator-all/.
16. Kelley M. Sayler, *DOD Replicator Initiative: Background and Issues for Congress*, Congressional Research Service, updated November 1, 2024, https://crsreports.congress.gov/product/pdf/IF/IF12611.
17. Stacie Pettyjohn, *Evolution Not Revolution: Drone Warfare in Russia's 2022 Invasion of Ukraine*, Center for a New American Security, 2024, https://www.cnas.org/publications/reports/evolution-not-revolution; Joseph Clark, "Defense Officials Report Progress on Replicator Initiative," U.S. Department of Defense (2023), https://www.defense.gov/News/News-Stories/Article/Article/3604459/defense-officials-report-progress-on-replicator-initiative/.
18. Sayler, *DOD Replicator Initiative*.
19. Sayler, *DOD Replicator Initiative*.

20. Mariano Zafra, Max Hunder, Anurag Rao, and Sudev Kiyada, "How drone combat in Ukraine is changing warfare," *Reuters*, March 26, 2024, https://www.reuters.com/graphics/UKRAINE-CRISIS/DRONES/dwpkeyjwkpm/; H. I. Sutton, "Exclusive: New Ukrainian Underwater Drone Project To Dominate The Black Sea," *Naval News*, January 24, 2024, https://www.navalnews.com/naval-news/2024/01/exclusive-new-ukrainian-underwater-drone-project-to-dominate-the-black-sea/; Tayfun Ozberk, "Ukraine's new underwater drone Marichka breaks cover," *Naval News*, August 23, 2023, https://www.navalnews.com/naval-news/2023/08/ukraines-new-underwater-drone-marichka-breaks-cover/.

21. Kateryna Zakharchenko, "Ukraine's Revolutionary Fiber-Optic Drone: An Electronic Warfare Game-Changer," *Kyiv Post*, December 9, 2024, https://www.kyivpost.com/post/43272.

22. "Deputy Secretary of Defense Kathleen Hicks Keynote Address: 'The Urgency to Innovate' (As Delivered)," U.S. Department of Defense, August 28, 2023, https://www.defense.gov/News/Speeches/Speech/Article/3507156/deputy-secretary-of-defense-kathleen-hicks-keynote-address-the-urgency-to-innov/.

23. "Deputy Secretary of Defense Hicks Announces First Tranche of Replicator Capabilities Focused on All Domain Attritable Autonomous Systems," U.S. Department of Defense, May 6, 2024, https://www.defense.gov/News/Releases/Release/Article/3765644/deputy-secretary-of-defense-hicks-announces-first-tranche-of-replicator-capabil/.

24. Lloyd J. Austin, *Replicator 2 Direction and Execution*, U.S. Department of Defense, September 27, 2024, https://assets.ctfassets.net/3nanhbfkr0pc/1dkJGhMeAgPldz1nnIwabK/abf85531a4281cddab6b0d8c953440e2/REPLICATOR-2-MEMO-SD-SIGNED__1_.pdf.

25. "Deputy Secretary of Defense Kathleen Hicks Announces Additional Replicator All-Domain Attritable Autonomous Capabilities," U.S. Department of Defense, November 13, 2024, https://www.defense.gov/News/Releases/Release/Article/3963289/deputy-secretary-of-defense-kathleen-hicks-announces-additional-replicator-all/.

26. "Defense Innovation Unit Announces Software Vendors to Support Replicator," Defense Innovation Unit, November 20, 2024, https://www.diu.mil/latest/defense-innovation-unit-announces-software-vendors-to-support-replicator.

27. "DoD Announces Strategy for Countering Unmanned Systems," U.S. Department of Defense, December 5, 2024, https://www.defense.gov/News/Releases/Release/Article/3986597/dod-announces-strategy-for-countering-unmanned-systems/.

28. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1984), 77.

29. Jude Blanchette, Briana Boland, and Lily McElwee, "What is Beijing's Timeline for 'Reunification' with Taiwan?" Center for Strategic and International Studies, May 26, 2023, https://interpret.csis.org/what-is-beijings-timeline-for-reunification-with-taiwan/; Brad Dress, "China will be ready for potential Taiwan invasion by 2027, US admiral warns," *The Hill*, March 21, 2024, https://thehill.com/policy/defense/4547637-china-potential-taiwan-invasion-2027-us-admiral-warns/; Noah Robertson, "How DC became obsessed with a potential 2027 Chinese invasion of Taiwan," *Defense News*, May 7, 2024, https://www.defensenews.com/pentagon/2024/05/07/how-dc-became-obsessed-with-a-potential-2027-chinese-invasion-of-taiwan/; Mallory Shelbourne, "Accelerated Chinese Timeline to Seize Taiwan Raises Questions on Pentagon Priorities, Says Gallagher," *USNI News*, October 18, 2022, https://news.usni.org/2022/10/18/accelerated-chinese-timeline-to-seize-taiwan-raises-questions-on-pentagon-priorities.

30. John Culver, "How We Would Know When China Is Preparing to Invade Taiwan," Carnegie Endowment for International Peace, October 3, 2022, https://carnegieendowment.org/posts/2022/10/how-we-would-know-when-china-is-preparing-to-invade-taiwan?lang=en.

31. Isaac Kardon and Jennifer Kavanagh, "How China Will Squeeze, Not Seize, Taiwan," *Foreign Affairs*, May 21, 2024, https://www.foreignaffairs.com/china/how-china-will-squeeze-not-seize-taiwan.

32. Bonny Lin et al., *How China Could Quarantine Taiwan: Mapping Out Two Possible Scenarios*, Center for Strategic and International Studies, June 5, 2024, https://www.csis.org/analysis/how-china-could-quarantine-taiwan-mapping-out-two-possible-scenarios.

33. Lin et al., *How China Could Quarantine Taiwan*, 7.

34. Lin et al., *How China Could Quarantine Taiwan*, 7.

35. Erik Green and Meia Nouwens, "China's Joint-Sword B exercise: a calculated follow-on," International Institute for Strategic Studies, October 23, 2024, https://www.iiss.org/online-analysis/online-analysis/2024/10/chinas-joint-sword-b-exercise-a-calculated-follow-on/.

36. Lin et al., *How China Could Quarantine Taiwan*.

37. "Deputy Secretary of Defense Kathleen Hicks Announces Additional Replicator All-Domain Attritable Autonomous Capabilities," U.S. Department of Defense; Noah Robertson, "Pentagon announces new batch of drones for Replicator program," *Defense News*, November 13, 2024, https://www.defensenews.com/unmanned/2024/11/13/pentagon-announces-new-batch-of-drones-for-replicator-program/.

38. "Altius," Anduril Industries, accessed December 10, 2024, https://www.anduril.com/hardware/altius/; "Area-I/Anduril ALTIUS-600M and 700M," Automated Decision Research, accessed December 10, 2024, https://automatedresearch.org/weapon/area-i-anduril-altius-600m-and-700m/.

39. "Performance Drone Works," Doodle Labs, accessed December 10, 2024, https://doodlelabs.com/case-studies/performance-drone-works/; "C100 Heavy-Lift Quadcopter," Unmanned Systems Technology, accessed December 10, 2024, https://www.unmannedsystemstechnology.com/company/performance-drone-works-pdw/c100-heavy-lift-quadcopter/; Joe Saballa, "US Army Selects Two Firms for Company-Level ISTAR Drone Program," *The Defense Post*, September 12, 2024, https://thedefensepost.com/2024/09/12/us-army-drone-program/.

40. Justin Katz, "Saronic unveils latest, largest unmanned vessel, with eye on mass production," *Breaking Defense*, October 23, 2024, https://breakingdefense.com/2024/10/saronic-unveils-latest-largest-unmanned-vessel-with-eye-on-mass-production/; "Vessels," Saronic, https://www.saronic.com/vessels.

41. Bonny Lin et al., *How China Could Blockade Taiwan*, Center for Strategic and International Studies, August 22, 2024, https://features.csis.org/chinapower/china-blockade-taiwan/.

42. Lin et al., *How China Could Quarantine Taiwan*.

43. Lin et al., *How China Could Quarantine Taiwan*, 7-10; *Military and Security Developments Involving the People's Republic of China*, 140-141.

44. Lin et al., *How China Could Blockade Taiwan.*

45. Bruno Tertrais, "Drawing Red Lines Right," *The Washington Quarterly* 37, no. 3 (2014), 7-24, https://doi.org/10.1080/01163660X.2014.978433.

46. Michael C. Horowitz, "When speed kills: Lethal autonomous weapon systems, deterrence and stability," *Journal of Strategic Studies* 42, no. 6 (2019), 764-788, https://doi.org/10.1080/01402390.2019.1621174.

47. Kristin Burke, *PLA Counterspace Command and Control*, China Aerospace Studies Institute, December 2023, 46, https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/PLASSF/2023-12-11%20Counterspace-%20web%20version.pdf.

48. Penney, "Scale, Scope, Speed & Survivability," 10.

49. *Military and Security Developments Involving the People's Republic of China*, 146; Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare*, RAND Corporation, February 1, 2018, 16-18, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1708/RAND_RR1708.pdf; Penney, "Scale, Scope, Speed & Survivability," 5-12; Ian Williams, "Catching Up: China's Developing Military Power," *Georgetown Journal of International Affairs*, January 6, 2020, https://gjia.georgetown.edu/2020/01/06/chinas-developing-military-power/; Anthony P. Carrillo, "Surface Crews Need More Tools to Navigate without GPS," *Proceedings* 148, no. 7 (July 2022), https://www.usni.org/magazines/proceedings/2022/july/surface-crews-need-more-tools-navigate-without-gps; Robert O. Work and Greg Grant, *Beating the Americans at their Own Game: An Offset Strategy with Chinese Characteristics*, Center for a New American Security, June 6, 2019, 5, https://s3.us-east-1.amazonaws.com/files.cnas.org/hero/documents/CNAS-Report-Work-Offset-final-B.pdf.

50. Sarah Wu and Eduardo Baptista, "From 7-11s to Train Stations, Cyber Attacks Plague Taiwan Over Pelosi Visit," *Reuters*, August 4, 2022, https://www.reuters.com/technology/7-11s-train-stations-cyber-attacks-plague-taiwan-over-pelosi-visit-2022-08-04/

51. Seamus Boyle, "In a Crisis, Could China Coerce Taiwan Through Cyberspace?" *The Diplomat,* February 29, 2024, https://thediplomat.com/2024/02/in-a-crisis-could-china-coerce-taiwan-through-cyberspace/.

52. *Military and Security Developments Involving the People's Republic of China*, VII-12; Mark Stokes, Gabriel Alvarado, Emily Weinstein, and Ian Easton, *China's Space and Counterspace Capabilities and Activities*, U.S.-China Economic and Security Review Commission, March 30, 2020, https://www.uscc.gov/sites/default/files/2020-05/China_Space_and_Counterspace_Activities.pdf, 39.

53. Burke, *PLA Counterspace Command and Control*, 34.

54. Burke, *PLA Counterspace Command and Control*, 34-47.

55. Carin Zissis, "China's Anti-Satellite Test," Council on Foreign Relations, February 22, 2007, https://www.cfr.org/backgrounder/chinas-anti-satellite-test.

56. Patrick Tucker, "China, Russia Building Attack Satellites and Space Lasers: Pentagon Report," *DefenseOne,* February 12, 2019, https://www.defenseone.com/technology/2019/02/china-russia-building-attack-satellites-and-space-lasers-pentagon-report/154819/.

57. *Military and Security Developments Involving the People's Republic of China*, 41.

58. Casey, "Firepower Strike, Blockade, Landing," 118-23.

59. *Military and Security Developments Involving the People's Republic of China*, VII-141.

60. "How Are China's Land-based Conventional Missile Forces Evolving?" *ChinaPower*, September 21, 2020, https://chinapower.csis.org/conventional-missiles/; *Military and Security Developments Involving the People's Republic of China*, 67.

61. *Military and Security Developments Involving the People's Republic of China*, 67; Ian Williams and Masao Dahlgren, "More Than Missiles: China Previews Its New Way of War," Center for Strategic and International Studies, October 1, 2019, https://www.csis.org/analysis/more-missiles-china-previews-its-new-way-war.

62. "DF-26," Center for Strategic and International Studies, updated April 23, 2024, https://missilethreat.csis.org/missile/dong-feng-26-df-26/; Jeffrey N. McCormick, *2024 Hypersonic Threat Assessment*, United States House of Representatives (2024), https://www.congress.gov/118/meeting/house/116949/witnesses/HHRG-118-AS29-Wstate-McCormickJ-20240312.pdf.
63. Lague and Lim, "New missile gap leaves U.S. scrambling to counter China."
64. Seth G. Jones, *Empty Bins in a Wartime Environment: The Challenge to the U.S. Defense Industrial Base*, Center for Strategic and International Studies, January 23, 2023, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-01/230119_Jones_Empty_Bins.pdf?VersionId=y_iEwCaIRVFiVedETHwrcuwDaenf7zez, 20.
65. Chris Gordon, "Lockheed Martin Looks to Boost LRASM Production as US Rushes to Buy Anti-Ship Weapons," *Air & Space Forces Magazine*, April 4, 2023, https://www.airandspaceforces.com/lockheed-martin-double-lrasm-production/.
66. Gordon, "Lockheed Martin Looks to Boost LRASM Production as US Rushes to Buy Anti-Ship Weapons;" Jones, *Empty Bins in a Wartime Environment*, 11.
67. U.S. Naval Institute Staff, "Document: Office of Naval Intelligence's Chinese People's Liberation Army Navy, Coast Guard Ship Identification Guide," USNI News, April 30, 2024, https://news.usni.org/2024/04/30/document-office-of-naval-intelligences-chinese-peoples-liberation-army-navy-coast-guard-ship-identification-guide-2; Richard Thomas, "New US Government chart outlines scope of China's naval power," *Naval Technology*, April 30, 2024, https://www.naval-technology.com/news/new-us-government-chart-outlines-scope-of-chinas-naval-power/?cf-view; Ronald O'Rourke, *China Naval Modernization: Implications for U.S. Navy Capabilities—Background and Issues for Congress*, Congressional Research Service, January 30, 2024, 2-3, https://crsreports.congress.gov/product/pdf/RL/RL33153/277.
68. *Military and Security Developments Involving the People's Republic of China*, 56.
69. Cancian, Cancian, and Heginbotham, *The First Battle of the Next War*, 112.
70. Daniel Caldwell, Joseph Freda, and Lyle J. Goldstein, *China Maritime Report No. 5: China's Dreadnought? The PLA Navy's Type 055 Cruiser and Its Implications for the Future Maritime Security Environment*, China Maritime Studies Institute (February 2020), 17-18, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1004&context=cmsi-maritime-reports.
71. *Military and Security Developments Involving the People's Republic of China*, 142.
72. *Military and Security Developments Involving the People's Republic of China*, 142.
73. *Military and Security Developments Involving the People's Republic of China*, 143.
74. Matthew P. Funaiole, Brian Hart, Jaehyun Han, and Jennifer Jun, "China Accelerates Construction of 'Ro-Ro' Vessels, with Potential Military Implications," *ChinaPower*, October 11, 2023, https://chinapower.csis.org/analysis/china-construct-ro-ro-vessels-military-implications/.
75. *Military and Security Developments Involving the People's Republic of China*, VII.
76. *Military and Security Developments Involving the People's Republic of China*, 144.
77. *Military and Security Developments Involving the People's Republic of China*, 145.
78. Hayley Wong and Amber Wang, "Swarming drones and counter-drone systems dazzle at China's Zhuhai air show," *South China Morning Post*, November 14, 2024, https://www.scmp.com/news/china/military/article/3286520/swarming-drones-and-counter-drone-systems-dazzle-chinas-zhuhai-air-show; Amber Wang, "China drones can counter US 'hellscape' in Taiwan Strait: analysts," *South China Morning Post*, June 12, 2024, https://www.scmp.com/news/china/military/article/3266295/china-drones-can-counter-us-hellscape-taiwan-strait-analysts;
79. *Military and Security Developments Involving the People's Republic of China*, 145.
80. *Military and Security Developments Involving the People's Republic of China*, 145.
81. Casey, "Firepower Strike, Blockade, Landing," 174-177.
82. David Sacks, "Why China Would Struggle to Invade Taiwan," Council on Foreign Relations, June 12, 2024, https://www.cfr.org/article/why-china-would-struggle-invade-taiwan.
83. Sun Tzu, *The Art of War*, trans. Lionel Giles (Project Gutenberg, 1994), 52, https://www.gutenberg.org/ebooks/132.
84. Michael C. Horowitz, "Battles of Precise Mass: Technology Is Remaking War—and America Must Adapt," *Foreign Affairs* 103, no. 6 (November/December 2024), 34-40, https://www.foreignaffairs.com/world/battles-precise-mass-technology-war-horowitz.
85. Robert O. Work, *Principles for the Combat Employment of Weapon Systems with Autonomous Functionalities*, Center for a New American Security, April 28, 2021, https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/Principles-for-Combat-Employment-of-Weapon-Systems_FINAL.pdf.
86. Kelley M. Sayler, *Defense Primer: U.S. Policy on Lethal Autonomous Weapon Systems*, Congressional Research Service, updated February 1, 2024, https://crsreports.congress.gov/product/pdf/IF/IF11150.
87. *DoD Directive 3000.09: Autonomy in Weapon Systems*, U.S. Department of Defense, updated January 25, 2023, 21, https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf.

88. *DoD Directive 3000.09*, 23.

89. Brandi Vincent, "Second Replicator tranche to include Anduril's autonomous underwater drones," *Defense Scoop*, August 14, 2024, https://defensescoop.com/2024/08/14/replicator-tranche-anduril-dive-ld-autonomous-underwater-drones/; "Dive-LD," Anduril, https://www.anduril.com/hardware/dive-ld/.

90. "Autonomous Vessels," Vigor, vigor.net/projects/sea-hunter; Xavier Vavasseur, "First Look at the US Navy's Orca XLUUV with Massive Payload Module," *Naval News*, June 12, 2024, https://www.navalnews.com/naval-news/2024/06/our-first-look-at-the-us-navys-orca-xluuv-fitted-with-payload-module/.

91. "US Navy Mines," United States Navy, updated October 8, 2021, https://www.navy.mil/Resources/Fact-Files/Display-FactFiles/Article/2167942/us-navy-mines/; Joseph Trevithick, "U.S. Is Betting Big On Naval Mine Warfare With These New Sub-Launched and Air-Dropped Types," *The Warzone*, June 28, 2021, https://www.twz.com/25235/the-u-s-is-getting-back-into-naval-mine-warfare-with-new-sub-launched-and-air-dropped-types.

92. Kyle Mizokami, "Ambush! The Navy's New Hammerhead Mine is a Submarine Killer," *Popular Mechanics*, October 23, 2020, https://www.popularmechanics.com/military/weapons/a34451548/navys-new-hammerhead-mine/.

93. "Deputy Secretary of Defense Hicks Announces First Tranche of Replicator Capabilities Focused on All Domain Attritable Autonomous Systems," U.S. Department of Defense, May 6, 2024, https://www.defense.gov/News/Releases/Release/Article/3765644/.

94. Product Catalog, AeroVironment, May 2, 2024, https://www.avinc.com/images/uploads/product_docs/ProductCatalog.pdf.

95. Kelsey D. Atherton, "Everything to know about Switchblades, the attack drones the US gave Ukraine," *Popular Science*, July 31, 2023, https://www.popsci.com/technology/switchblade-drones-explained/.

96. Tyler Rogoway, "We Talk Suicide Drones And The Future Of Unmanned Warfare With AeroVironment's Steve Gitlin," *The Warzone*, July 8, 2020, https://www.twz.com/34414/we-talk-killer-drones-and-the-future-of-unmanned-warfare-with-aerovironments-steve-gitlin.

97. Vasco Cotovio, Clare Sebastian, and Allegra Goodwin, "Ukraine's AI-enabled drones are trying to disrupt Russia's energy industry. So far, it's working," *CNN*, April 2, 2024, https://www.cnn.com/2024/04/01/energy/ukrainian-drones-disrupting-russian-energy-industry-intl-cmd/index.html.

98. William Power et al., "Autonomous Navigation for Drone Swarms in GPS-Denied Environments Using Structured Learning," *Artificial Intelligence Applications and Innovations* 584 (2020), 219-231, https://doi.org/10.1007/978-3-030-49186-4_19; Sydney J. Freedberg Jr., "The revolution that wasn't: How AI drones have fizzled in Ukraine (so far)," *Breaking Defense*, February 20, 2024, https://breakingdefense.com/2024/02/the-revolution-that-wasnt-how-ai-drones-have-fizzled-in-ukraine-so-far/.

99. This report created this new taxonomy for categorizing autonomous weapon systems after interviewing experts and reviewing the following sources: *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*, SAE International, April 30, 2021, https://www.sae.org/standards/content/j3016_202104/; Hui-Min Huang, "Autonomy Levels for Unmanned Systems (ALFUS)," lecture presented at the National Institute of Standards and Technology, Gaithersburg, 2008, https://www.nist.gov/system/files/documents/el/isd/ks/ALFUS-BG.pdf; Millie Radovic, "Tech Talk: The 5 Levels of Drone Autonomy," Drone Industry Insights, March 7, 2019, https://droneii.com/drone-autonomy?srsltid=AfmBOoptdzkcviS3rhoWG_zd7CVL49_HUE0GmSImde-NELlxrXNyV7xy; Paul Scharre and Michael C. Horowitz, *An Introduction to Autonomy in Weapon Systems*, Center for a New American Security, February 2015, https://s3.us-east-1.amazonaws.com/files.cnas.org/hero/documents/Ethical-Autonomy-Working-Paper_021015_v02.pdf; Shayne Longpre, Marcus Storm, and Rishi Shah, "Lethal Autonomous Weapons Systems & Artificial Intelligence: Trends, Challenges, and Policies," *MIT Science Policy Review* 3 (2022), 47-56, https://doi.org/10.38105/spr.360apm5typ.

100. Sayler, *Defense Primer: U.S. Policy on Lethal Autonomous Weapon Systems*.

101. Sayler, *Defense Primer: U.S. Policy on Lethal Autonomous Weapon Systems*.

102. Mohammad Mustafa Taye, "Theoretical Understanding of Convolutional Neural Network: Concepts, Architectures, Applications, Future Directions," *Computation* 11, no. 3 (2023), 52, https://doi.org/10.3390/computation11030052; Laith Alzubaidi et al., "Review of Deep Learning: Concepts, CNN Architectures, Challenges, Applications, Future Directions," *Journal of Big Data* 8, no. 53 (2021), 1-15, https://doi.org/10.1186/s40537-021-00444-8.

103. Nilesh Barla, "Self-Driving Cars With Convolutional Neural Networks (CNN)," neptune.ai, April 22, 2024, https://neptune.ai/blog/self-driving-cars-with-convolutional-neural-networks-cnn; Abhishek Gupta, Alagan Anpalagan, Ling Guan, and Ahmed Shaharyar Khwaja, "Deep Learning for Object Detection and Scene Perception in Self-Driving Cars: Survey, Challenges, and Open Issues," *Array* 10 (July 2021), 100057, https://doi.org/10.1016/j.array.2021.100057. For more on Tesla autopilot crash data, see "Tesla Vehicle Safety Report," Tesla, https://www.tesla.com/VehicleSafetyReport. For AV research from Waymo, see "Research," Waymo, https://waymo.com/research/.

104. Christopher T. Cannon and Stefan Goericke, *Using Convolution Neural Networks to Develop Robust Combat Behaviors Through Reinforcement Learning* (Monterey: Naval Postgraduate School, June 2021), https://apps.dtic.mil/sti/trecms/pdf/AD1150887.pdf.

105. Martin Keen, "What are GANs (Generative Adversarial Networks)?," IBM Technology, November 11, 2021, https://www.youtube.com/watch?v=TpMIssRdhco; Ian Goodfellow et al., "Generative Adversarial Networks," *Communications of the ACM* 63, no. 11 (2020), 139-144, https://doi.org/10.1145/3422622.

106. Leila Haj Meftah, Asma Cherif, and Rafik Braham, "Improving Autonomous Vehicles Maneuverability and Collision Avoidance in Adverse Weather Conditions Using Generative Adversarial Networks," *Array* 12 (2024), https://doi.org/10.1016/j.array.2024.100057; Sergey I. Nikolenko, "Synthetic Data for Deep Learning," *arXiv* 1909.11512, September 25, 2019, https://doi.org/10.48550/arXiv.1909.11512.

107. Sajid A. Marhon, Christopher J. F. Cameron, and Stefan C. Kremer, "Recurrent Neural Networks," in *Handbook on Neural Information Processing*, ed. Monica Bianchini, Marco Maggini, and Lakhmi C. Jain, vol. 49 (Heidelberg: Springer, 2013), 29-65, https://doi.org/10.1007/978-3-642-36657-4_2; Claus Metzner and Patrick Krauss, "Dynamics and Information Import in Recurrent Neural Networks," *Frontiers in Computational Neuroscience* 16 (April 2022), 876315, https://doi.org/10.3389/fncom.2022.876315.

108. S.W. Perry and Ling Guan, "A Recurrent Neural Network for Detecting Objects in Sequences of Sector-Scan Sonar Images," *IEEE Journal of Oceanic Engineering* 29, no. 3 (July 2004), 857–871, https://doi.org/10.1109/JOE.2004.831616; Alankrita Aggarwal, Mamta Mittal, and Gopi Battineni, "Generative Adversarial Network: An Overview of Theory and Applications," *International Journal of Information Management Data Insights* 1, no. 1 (April 2021), 100004, https://doi.org/10.1016/j.jjimei.2020.100004; Preeti Sharma, Manoj Kumar, Hitesh Kumar Sharma, and Soly Mathew Biju, "Generative Adversarial Networks (GANs), Introduction, Taxonomy, Variants, Limitations, and Applications," *Multimedia Tools and Applications* (2024), https://doi.org/10.1007/s11042-024-18767-y; Luis E. Velazquez, "Harnessing Deep Learning for Enhanced Military Simulations: A Comprehensive Approach," MODSIM World 2024, Paper No. 8, https://modsimworld.org/papers/2024/MODSIM_2024_paper_8.pdf.

109. Yonghwan Jeong, "Interactive Lane Keeping System for Autonomous Vehicles Using LSTM-RNN Considering Driving Environments," *Sensors* 22, no. 24 (2022), https://doi.org/10.3390/s22249889; Gabriel Andersson and Santiago Martin Favre, "Analysis and Evaluation of Recurrent Neural Networks in Autonomous Vehicles," KTH Royal Institute of Technology, 2017, https://www.edgeimpulse.com/blog/content/files/smash/get/diva2:1155735/fulltext01.pdf; Yonghwan Jeong, "Interactive Lane Keeping System for Autonomous Vehicles Using LSTM-RNN Considering Driving Environments," *Sensors* 22, no. 24, (2022), 9889, https://www.mdpi.com/1424-8220/22/24/9889.

110. Gaudenz Boesch, "What are Liquid Neural Networks?," viso.ai, May 17, 2024, https://viso.ai/deep-learning/what-are-liquid-neural-networks/.

111. Ramin Hasani et al., "Liquid Time-constant Networks," *arXiv*, June 8, 2020, https://doi.org/10.48550/arXiv.2006.04439; Makram Chahine et al., "Robust Flight Navigation Out of Distribution with Liquid Neural Networks," *Science Robotics* 8, no. 77 (April 2023), https://doi.org/10.1126/scirobotics.adc8892.

112. Rachel Gordon, "Drones Navigate Unseen Environments with Liquid Neural Networks," *MIT News*, April 19, 2023, https://news.mit.edu/2023/drones-navigate-unseen-environments-liquid-neural-networks-0419.

113. Jacob Suppiah et al., "Infrastructure Developments for Training China's Army," *Tearline*, April 8, 2022, https://www.tearline.mil/public_page/pla-joint-training; Lars M. H. Ulander, "VHF-Band SAR for Detection of Concealed Ground Targets," *RTO-MP-SCI-145* (2004), 19-4-19-6, https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/RTO-MP-SCI-145/MP-SCI-145-19.pdf; J. Michael Dahm, *Offensive and Defensive Strike*, Johns Hopkins University Applied Physics Laboratory, March 2021, 45-48 https://www.jhuapl.edu/sites/default/files/2022-12/OffensiveDefensiveStrike.pdf.

114. Bonny Lin and Brian Hart, "Analyzing China's Escalation After Taiwan President William Lai's National Day Speech," *ChinaPower*, October 29, 2024, https://chinapower.csis.org/china-taiwan-joint-sword-2024b-coast-guard/.

115. Colin Demarest, "Pentagon's AI chief says data labeling is key to win race with China," *C4ISRNet*, January 26, 2023, https://www.c4isrnet.com/artificial-intelligence/2023/01/26/pentagons-ai-chief-says-data-labeling-is-key-to-win-race-with-china/.

116. Abhishek Thakur and Sudhansu Kumar Mishra, "An In-Depth Evaluation of Deep Learning-Enabled Adaptive Approaches for Detecting Obstacles Using Sensor-Fused Data in Autonomous Vehicles," *Engineering Applications of Artificial Intelligence* 133 (July 2024), https://doi.org/10.1016/j.engappai.2024.108550; Qiping Chen, Yinfei Xie, Shifeng Guo, Jie Bai, and Qiang Shu, "Sensing System of Environmental Perception Technologies for Driverless Vehicle: A Review of State of the Art and Challenges," *Sensors and Actuators A: Physical* 319 (March 2021), https://doi.org/10.1016/j.sna.2021.112566.

117. Karl Weiss, Taghi M. Khoshgoftaar, and DingDing Wang, "A Survey of Transfer Learning," *Journal of Big Data* 3, no. 9 (2016), 9, https://doi.org/10.1186/s40537-016-0043-6; Asmaul Hosna et al., "Transfer Learning: A Friendly Introduction," *Journal of Big Data* 9, no. 102 (2022), https://doi.org/10.1186/s40537-022-00652-w; Mohammadreza Iman, Hamid Reza Arabnia, and Khaled Rasheed, "A Review of Deep Transfer Learning and Recent Advancements," *Technologies* 11, no. 2 (2023), 40, https://doi.org/10.3390/technologies11020040.

118. Nerya Ashush, Shlomo Greenberg, Erez Manor, and Yehuda Ben-Shimol, "Unsupervised Drones Swarm Characterization Using RF Signals Analysis and Machine Learning Methods," *Sensors* 23, no. 3 (2023), 1589, https://doi.org/10.3390/s23031589.

119. Xinwei Wang et al., "Deep reinforcement learning-based air combat maneuver decision-making: literature review, implementation tutorial and future direction," *Artificial Intelligence Review* 57, no. 1 (2024), https://doi.org/10.1007/s10462-023-10620-2.

120. Althea Henslee et al., "Data-Driven Reinforcement Learning for Mission Engineering and Combat Simulation" in *Proceedings of the IUTAM Symposium on Optimal Guidance and Control for Autonomous Systems 2023*, ed. Dilmurat Azimov (Cham: Springer, 2024), 347-360, https://doi.org/10.1007/978-3-031-39303-7_21.

121. Marc Novakouski and Grace Lewis, "Operating at the Edge," SEI Blog, November 29, 2021, https://insights.sei.cmu.edu/blog/operating-at-the-edge/.

122. Joshua Landman and Praveen Rajagopalan, "Edge Computing—Challenges and Opportunities for Enterprise Cloud Architects," Google Cloud Blog, November 22, 2021, https://cloud.google.com/blog/topics/hybrid-cloud/edge-computing-architectural-challenges-and-pitfalls; Taryn Plumb, "Edge Data Is Critical to AI — Here's How Dell Is Helping Enterprises Unlock Its Value," *VentureBeat*, November 12, 2024, https://venturebeat.com/ai/edge-data-is-critical-to-ai-heres-how-dell-is-helping-enterprises-unlock-its-value/.

123. Soumya Sudhakar, Vivienne Sze, and Sertac Karaman, "Data Centers on Wheels: Emissions From Computing Onboard Autonomous Vehicles," *IEEE Micro* (January/February 2023), 30, https://ieeexplore.ieee.org/document/9965950; U.S. Government Accountability Office, *Artificial Intelligence: Status of Developing and Acquiring Capabilities for Weapon Systems*, GAO-22-104765 (Washington, D.C.: U.S. Government Accountability Office, February 2022), 26, https://www.gao.gov/products/gao-22-104765; Brian Wang, "Nvidia AI and Multi-PetaOps Chips for Class 5 Automated Cars Within 4 Years," *NextBigFuture*, October 27, 2017, https://www.nextbigfuture.com/2017/10/nvidia-ai-and-multi-petaops-chips-for-class-5-automated-cars-within-4-years.html.

124. Stéphane Melançon, "Solid State Batteries Vs. Lithium-Ion: Which One is Better?" Laserax, October 28, 2024, https://www.laserax.com/blog/solid-state-vs-lithium-ion-batteries.

125. Ellis Gibson, "How Much Should a Drone Battery Weigh? Guidelines for Optimal Performance and Flight Time," *PoweringAutos*, December 4, 2024, https://poweringautos.com/how-much-should-a-drone-battery-weigh/.

126. "How to Calculate Quadcopter Power Consumption," RC Drone Good, accessed December 11, 2024, https://www.rcdronegood.com/calculate-quadcopter-power-consumption/.

127. Quan Li et al., "The Road Towards High-Energy-Density Batteries," *The Innovation Energy* 1, no. 1 (2024), 100005, https://doi.org/10.59717/j.xinn-energy.2024.100005.

128. Michael Konopik et al., "The Fundamental Energy Cost of Finite-Time Parallelizable Computing," *Nature Communications* 14, 447 (2023), https://doi.org/10.1038/s41467-023-36020-2; Chris Porter, "Energy Efficiency in High-Performance Computing: Balancing Speed and Sustainability," NVIDIA Developer Blog, November 14, 2023, https://developer.nvidia.com/blog/energy-efficiency-in-high-performance-computing-balancing-speed-and-sustainability/.

129. Mesh Flinders and Ian Smalley, "What Is Parallel Computing?" IBM Think, July 3, 2024, https://www.ibm.com/think/topics/parallel-computing.

130. Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations*, 5th ed. (New York: Basic Books, 2015), 64.

131. U.N. Charter art. 2(4).

132. U.N. Charter art. 51; U.N. Charter art. 42. China will almost certainly have a different international legal interpretation to any U.S. justification to the recourse to force in defense of Taiwan.

133. Matthew Waxman, "The 'Caroline' Affair in the Evolving International Law of Self-Defense," *Lawfare* (2018), https://www.lawfaremedia.org/article/caroline-affair.

134. Office of General Counsel, *Department of Defense Law of War Manual*, U.S. Department of Defense, updated July 2023, https://media.defense.gov/2023/Jul/31/2003271432/-1/-1/0/DOD-LAW-OF-WAR-MANUAL-JUNE-2015-UPDATED-JULY%202023.PDF.

135. "Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy," U.S. Department of State, November 4, 2024, https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy/; "Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy," U.S. Department of State Bureau of Arms Control, Deterrence, and Stability, November 9, 2023, https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy-2/.

136. Matthew P. Funaiole et al., "Crossroads of Commerce: How the Taiwan Strait Propels the Global Economy," *ChinaPower*, October 10, 2024, https://features.csis.org/chinapower/china-taiwan-strait-trade/.

137. Michael Press, "Of Robots and Rules: Autonomous Weapon Systems in the Law of Armed Conflict," *Georgetown Journal of International Law* 48, no. 4 (2017), 1337-1366, https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-4-Of-Robots-and-Rules.pdf.

138. Nik Hynek and Anzhelika Solovyeva*, Militarizing Artificial Intelligence: Theory, Technology, and Regulation* (London: Routledge, 2022), https://doi.org/10.4324/9781003045489; Markus Wagner, "The Dehumanization of International Humanitarian Law: Legal, Ethical, and Political Implications of Autonomous Weapon Systems," *Vanderbilt Journal of Transnational Law* 47 (2014), 1371-1409, https://scholarship.law.vanderbilt.edu/vjtl/vol47/iss5/4.

139. Michael W. Meier, "The Principle of Proportionality in the DoD Law of War Manual," *Just Security*, January 18, 2024, https://www.justsecurity.org/91319/the-principle-of-proportionality-in-the-dod-law-of-war-manual/.

140. This unprecedented level of constancy and uniformity for autonomous weapon systems' AI models would reflect a combination of means-ends interpretations of the *jus ad bellum* principle of proportionality and the *jus in bello* principle of proportionality. For more on the *jus ad bellum* principle of proportionality, see Office of General Counsel, *Department of Defense Law of War Manual*, 86; David Kretzmer, "The Inherent Right to Self-Defence and Proportionality in Jus Ad Bellum," *European Journal of International Law* 24, no. 1 (2013), 238, https://doi.org/10.1093/ejil/chs087.

141. Office of General Counsel, *Department of Defense Law of War Manual*, 52-60.

142. International Committee of the Red Cross, "Rule 22. Principle of Precautions against the Effects of Attacks," International Humanitarian Law Databases, https://ihl-databases.icrc.org/en/customary-ihl/v1/rule22.

143. Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999), https://lessig.org/images/resources/1999-Code.pdf.

144. Special thanks to Ben Zeskind for the excellent thoughts he provided on this issue.

145. Press, "Of Robots and Rules," 1358.

146. Colin Clark, "Killer Robots? 'Never,' Defense Secretary Carter Says," *Breaking Defense*, September 15, 2016, https://breakingdefense.com/2016/09/killer-robots-never-says-defense-secretary-carter/.

147. *DoD Directive 3000.09*, 15.

148. *DoD Directive 3000.09*, 15-17.

149. *DoD Directive 3000.09*, 22.

150. Ashley Deeks, "The Double Black Box: AI Inside the National Security Ecosystem," *Just Security*, August 14, 2024, https://www.justsecurity.org/98555/the-double-black-box-ai-inside-the-national-security-ecosystem/.

151. Pantelis Linardatos, Vasilis Papastefanopoulos, and Sotiris Kotsiantis, "Explainable AI: A Review of Machine Learning Interpretability Methods," *Entropy* 23, no. 1 (2021), 18, https://doi.org/10.3390/e23010018.

152. Kenneth Anderson, Daniel Reisner, and Matthew Waxman, "Adapting the Law of Armed Conflict to Autonomous Weapon Systems," *International Law Studies* 90.3 (2014), 386-411, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1015&context=ils.

153. Scott Sullivan and Iben Ricket, "Targeting in the Black Box," in *CyCon 2024: Over the Horizon*, eds. C. Kwan, L. Lindström, D. Giovannelli, K. Podiņš, and D. Štrucl (Tallinn: NATO CCDCOE Publications, 2024), 207-220, https://ccdcoe.org/uploads/2024/05/CyCon_2024_Sullivan_Ricket-1.pdf.

154. Edward Hunter Christie, Amy Ertan, et al., "Regulating Lethal Autonomous Weapon Systems: Exploring the Challenges of Explainability and Traceability," *AI Ethics* 4 (2024), 229–245, https://doi.org/10.1007/s43681-023-00261-0.

155. *DoD Directive 3000.09*, 3-6; "Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy."

156. *DoD Directive 3000.09*, 15.

157. For distinctions between proliferation, competition, and arms races, see Samuel P. Huntington, "Arms races: prerequisites and results" *Public Policy* 8 (1958), 41-86.

158. Heather Somerville and Brett Forrest, "How American Drones Failed to Turn the Tide in Ukraine," *Wall Street Journal*, April 10, 2024, https://www.wsj.com/world/how-american-drones-failed-to-turn-the-tide-in-ukraine-b0ebbac3; Paul Mozur and Valerie Hopkins, "Ukraine's War of Drones Runs Into an Obstacle: China," *New York Times*, September 30, 2023, https://www.nytimes.com/2023/09/30/technology/ukraine-russia-war-drones-china.html.

159. Charles L. Glaser, "Fear Factor: How to Know When You're in a Security Dilemma," *Foreign Affairs* 103, no. 4 (July/August 2024), 122-128, https://www.foreignaffairs.com/united-states/fear-factor-security-charles-glaser.

160. Jack L. Snyder, *Myths of Empire: Domestic Politics and International Ambition* (Ithaca, NY: Cornell University Press, 1993), 1-65.

161. Charles L. Glaser, *Rational Theory of International Politics: The Logic of Competition and Cooperation* (Princeton: Princeton University Press, 2010); Randall L. Schweller, "Neorealism's Status-Quo Bias: What Security Dilemma?" *Security Studies* 5, no. 3 (1996), 90-121, https://doi.org/10.1080/09636419608429277; Dale C. Copeland, *A World Safe for Commerce: American Foreign Policy from the Revolution to the Rise of China* (Princeton: Princeton University Press, 2024), 27-32.

162. Robert Jervis, "Cooperation Under the Security Dilemma," *World Politics* 30, no. 2 (1978), 167-214, https://doi.org/10.2307/2009958.

163. John Frederick Charles Fuller, *Armament and History: A Study of the Influence of Armament on History from the Dawn of Classical Warfare to the Second World War* (New York: C. Scribner's Sons, 1945).

164. Alistair MacDonald and Jane Lytvynenko, "Inside Ukraine's Battle for the Skies as Russian Bombardments Hit Records," *Wall Street Journal*, December 9, 2024, https://www.wsj.com/world/ukraine-russia-war-skies-winter-35aa1fb5?mod=hp_lead_pos8.

165. Horowitz, "When speed kills," 770-788.

Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org

Printed in the United States of America