JOURNAL OF ADVANCED MILITARY STUDIES

JAMS

Vol. 16, No. 2, 2025

JOURNAL OF ADVANCED MILITARY STUDIES

JAMS

MCUP
MARINE CORPS UNIVERSITY PRESS
2044 Broadway Street | Quantico, VA 22134

Journal of Advanced Military Studies
(Print) ISSN 2770-2596
(Online) ISSN 2770-260X

Established in 2008, MCU Press is an open access publisher that recognizes the importance of an open dialogue between scholars, policy makers, analysts, and military leaders and of crossing civilian-military boundaries to advance knowledge and solve problems. To that end, MCUP launched the *Journal of Advanced Military Studies* (JAMS) to provide a forum for interdisciplinary discussion of national security and international relations issues and how they have an impact on the Department of Defense, the Department of the Navy, and the U.S. Marine Corps directly and indirectly. JAMS is published biannually, with occasional special issues that highlight key topics of interest.

ARTICLE SUBMISSIONS
The editors are looking for academic articles in the areas of international relations, geopolitical issues, national security and policy, and cybersecurity. To submit an article or to learn more about our submission guidelines, please email MCU_Press@usmcu.edu.

BOOK REVIEWS
Send an email with a brief description of your interests to MCU_Press@usmcu.edu.

SUBSCRIPTIONS
Subscriptions to JAMS are free. To join our subscription list or to obtain back issues of the journal, send your mailing address to MCU_Press@usmcu.edu.

ADDRESS CHANGE
Send address updates to MCU_Press@usmcu.edu to maintain uninterrupted delivery.

INDEXING
The journal is indexed by ProjectMUSE, Scopus, ScienceOpen, EBSCO, ProQuest, Elsevier, OCLC ArticleFirst, Defense Technical Information Center, Journal Seek, IBZ Online, British Library System, Lancaster Index to Defense and International Security Literature, and AU Library Index to Military Periodicals.

FREELY AVAILABLE AT
WWW.USMCU.EDU/MCUPRESS

Contents

Vol. 16, No. 2

From the Editor

It is with great honor that I provide the introduction for this issue focusing on emerging disruptive technology for the *Journal of Advanced Military Studies* (JAMS). Artificial intelligence (AI), advanced human-machine team configurations, profound technological developments, and the never-ending security demands for all societies in this fast-paced world have placed humanity at the edge of a steep incline. Our species is moments away from multiple historic, likely game-changing developments that will require massive changes in how our military profession understands, prepares, and executes missions to deter conflict, win decisively when required, and encourage peaceful coexistence.

During the next decade or less, we will likely witness a firm expansion of humanity into the solar system, becoming a multiplanetary species with cosmic aspirations that carry with them new and unfamiliar security requirements. In the same period, we may finally spawn artificial intelligence that rivals or exceeds our own in ways that have extraordinary military consequences, with parallel robotics and drone developments giving AI the means to interact in the human world with their unique cognitive abilities. Decision-making methodologies, doctrines, practices, and even the language and underlying principles that comprise the current understanding of how to strategize and achieve tactical success must be tempered not with traditional or familiar tools, but with these emerging and unprecedented ones that will undoubtedly cause a paradigm shift in how we conduct war.

This issue of JAMS attempts to illuminate these new pathways with provocative and well-researched offerings. Major John Bolen boldly proposes drone employment en masse using swarm configurations, while Ameema Khalid considers the space domain and the clear need for new space policies, laws, and security preparations through a technological, deterministic lens. Lieutenant Commander Jonathan Alexander explores how human operators may become "enmeshed" into human-machine teams that carry new moral issues and risks. Paul A. Eisenmann critiques Western democracies in this emerging world of technological ambiguity, where authoritarian regimes may have the upper hand in waging cyber wars. These authors examine conflict and decision making with

clear appreciation of the disruptive nature of this rapidly changing technological environment before us.

Yet, we might not toss the human baby out with the AI bathwater. Defense of institutional norms, principles, and beliefs in this rapidly changing period is a valid and necessary area for debate. Major Vincenzo Gallitelli critiques the rise of AI by defending the institutionally favored conventions of Carl von Clausewitz, offering ways for humans to harness AI without becoming replaced. Major Gavin Holtz works in parallel, proposing interagency concepts that integrate new AI abilities with established military frameworks such as John R. Boyd's OODA (observe, orient, decide, act) loop. Ehsan Ejazi and Mahsa Ahmadyan offer analysis on how AI might be used to efficiently sustain existing geopolitical orders that use proxy wars to prevent nuclear or total war escalations. These authors provide signposts for future pathways where disruptive technology might be harnessed to further buttress existing institutional norms and best practices.

Lastly, this issue features some unorthodox and forward-looking positions on how far we might be technologically disrupted from our comfort zone. Lieutenant Colonel Jani Liikola and Commander Petteri Blomvall challenge the institution in a provocative fashion, offering readers new insights into how AI multiagent systems might transform nearly everything in the defense paradigm. A.S.M. Ahsan Uddin offers readers an overview of fantastic technology and theory such as antimatter missiles, kinetic bombardment from space, and antigravity propulsion that could in the coming decades move from the improbable to the feasible.

These authors collectively have peered out into the uncertainty and fog between our present state and a near future where these profound technological developments manifest in one form or another. We may be standing before some momentous transformation where new and dangerous pitfalls lurk. Readers should find their offerings in this issue of JAMS illuminating in a variety of ways to pierce the techno-veil.

Ben Zweibelson, PhD
Strategic Innovation Group Director,
U.S. Space Command

Achtung—Swarm!
A Proposal for Swarm Maneuver Groups

Major John Bolen, USA

Abstract: The unmanned combat vehicle, or combat drone, is making its presence felt on battlefields around the world. Much like the tank and aircraft in World War I, drones have been employed individually or in small groups to conduct reconnaissance and precision strikes. But the Department of War's renewed focus on large-scale combat operations warrants new thought regarding drone employment. This article is not a treatise on the technical aspects of unmanned combat vehicles, but instead a proposal for drone employment en masse as an operational maneuver force. It uses historical examples of operational maneuver, recent drone operations, and imagination to generate a new concept for combat drone employment: the swarm maneuver group. The high mobility and mass of the proposed swarm maneuver group offers the Joint Force a new means of conducting persistent deep operations to disintegrate adversary antiaccess/area-denial (A2/AD) systems and enable Joint operational access to theaters. The aim of this article is to generate creative thought, debate, and purposeful action regarding the offensive employment of unmanned combat vehicles in large-scale combat operations.

Keywords: swarm maneuver group, unmanned systems, military innovation, antiaccess/area-denial, A2/AD, Joint Force, swarm tactics, combat drone doctrine

Introduction

The United States faces the prospect of a multifront war against several rogue adversaries and a peer, which is arguably the most existential threat the United States has faced in its history, the People's Republic of

Maj John Bolen is currently a student at the U.S. Army Command and General Staff College in Leavenworth, KS. He holds a bachelor's degree in military history from Virginia Miliary Institute and a masters in military history from Norwich University.

Journal of Advanced Military Studies vol. 16, no. 2
Fall 2025
www.usmcu.edu/mcupress
https://doi.org/10.21140/mcuj.20251602001

China. As highlighted in the Joint Operational Access Concept (JOAC), these adversaries have robust antiaccess, area-denial (A2/AD) systems combining the tyranny of distance with the lethality of long-range reconnaissance-strike complexes. They seek fait accompli victories, believing they can achieve political objectives with armed incursions before the United States and its allies can mass a credible military response. Simultaneously, shortfalls in recruiting and retention efforts and large numbers of citizens unfit for service constrain the size of the U.S. military. While the United States has the best servicemembers in the world and many exquisite capabilities, the Services are spread thin and have constrained mobilization potential.

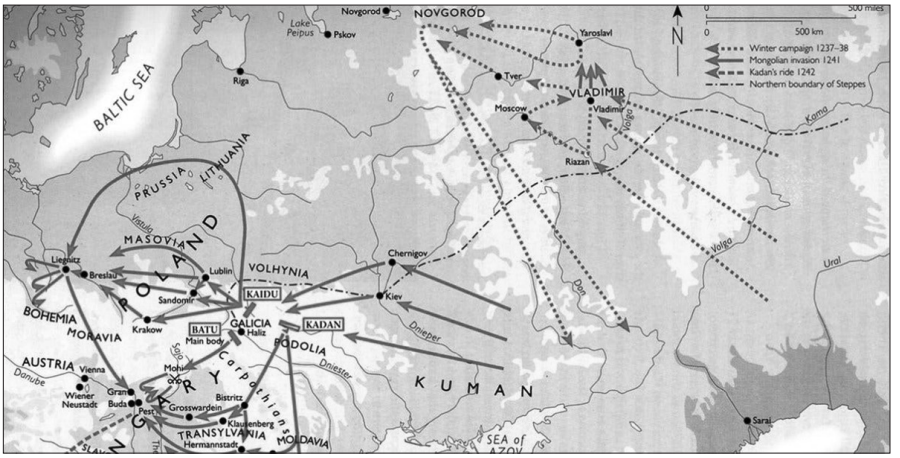
During the interwar years, figures such as J. F. C. Fuller, Georgii Samoilovich Isserson, Heinz Guderian, and William L. "Billy" Mitchell grappled with a similar dilemma: How can the offense, constrained by peacetime budgets and force sizes, overcome the immense depth and firepower of the modern defense at the outset of the war? Two new combat platforms, tanks and aircraft, had achieved tactical successes in World War I but in limited and auxiliary roles. Armor served as infantry support, and aircraft in reconnaissance and air-to-air combat.

In the 1920s and 1930s, these visionaries and others developed doctrine for the offensive employment of armor and airpower en masse to achieve not just tactical breakthroughs but operational-level ruptures of entire defensive systems. They used history, combat experience, training, and imagination to develop new theories of warfare, often before tanks and aircraft of sufficient quality existed to validate their proposals. It was not until the 1939–40 German invasions of Poland and France that their hypotheses were substantiated. Tanks, aircraft, operational design, and offensive-minded leadership outmaneuvered and defeated the epitome of defensive depth and firepower, the Maginot Line.

A new offensive means, the unmanned combat vehicle (UCV), is making its presence felt on battlefields across the world. Just like tanks and airplanes in World War I, they are spread throughout the force in driblets, conducting aerial reconnaissance and isolated strikes. But as the German general Heinz Guderian said, "You hit somebody with your fist and not with your fingers spread." The United States requires a highly mobile force with sufficient mass to conduct, as stated in the *Joint Concept for Entry Operations*: "opportunistic and unpredictable maneuver in and across multiple domains, establishing local superiority at multiple entry points to gain entry and achieve objectives."[1]

This article proposes a new method of using UCVs to meet many of the requirements outlined in the JOAC—the swarm maneuver group. This is not a treatise on the technical aspects of UCVs but instead a theory of their organization and employment en masse as a deep maneuver force synthesized from historical examples, recent tactical actions, and imagination. The aim is to

Map 1. Map of the Mongol invasion of Eastern Europe



Note the use of multiple, converging columns.
Source: Derek Davidson, "Today in European history: the Battle of Mohi (1241)," Foreign Exchanges, 11 April 2019.

generate creative thought, debate, and purposeful action regarding the offensive employment of UCVs to disintegrate adversary A2/AD and decision making and enable Joint entry operations.

Mongols, Napoléon, Vicksburg, and Operational Maneuver Groups: Historical Precedence for Operational Maneuver

During 1240–41, the Mongols invaded Eastern Europe with the intent of subjugating Hungary. A simultaneous operation in Poland led by the Mongol commander Subutai supported the Hungary operation by preventing the opposing forces from concentrating combat power. The Mongols divided their army into four columns, each of which had two to three *tumens* (divisions) of 10,000 horsemen. Column commanders had the freedom to plan their own route and tactical actions, so long as they adhered to the operational timeline and theater strategy.[2]

Mongol commanders bypassed enemy strongpoints and only attempted to storm fortresses once. If resistance was strong, they moved on. By raiding vulnerable yet critical parts of their enemy's civil-military system—agriculture, small towns, etc.—they consolidated gains while avoiding enemy strengths. When the opportunity to defeat their enemy in detail emerged, as at the Battles of Mohi and Liegnitz (April 1241), the Mongols used speed, deception, swarming tactics, and envelopments to defeat the slower European forces.[3]

Six centuries later, during the American Civil War, commanders on both sides employed large, mobile groups of horse cavalry in raiding operations. In

late 1862, Union major general Ulysses S. Grant initiated his first campaign to capture the Confederate river fortress of Vicksburg, attempting an overland march east of the Mississippi River. Lieutenant General John C. Pemberton, the Confederate commander, launched two deep cavalry raids on Grant's supply lines while keeping his main forces in Vicksburg. The first Confederate raid, led by Nathan Bedford Forrest, destroyed rail junctions in the vicinity of Jackson, Mississippi, roughly 200 kilometers (km) behind Grant's forces, severing Union wire communications and supply lines.[4] Nearly simultaneously, General Earl Van Dorn led 3,500 Confederate cavalry in three columns in a raid on Grant's main supply depot at Holly Springs. Van Dorn's forces quickly overcame the defenders and destroyed the Union depot.[5] Grant's attempt to use support area forces to neutralize the Confederate raiders failed and, with the loss of his lines of supply and communication, he was forced to temporarily regroup at Memphis, Tennessee.

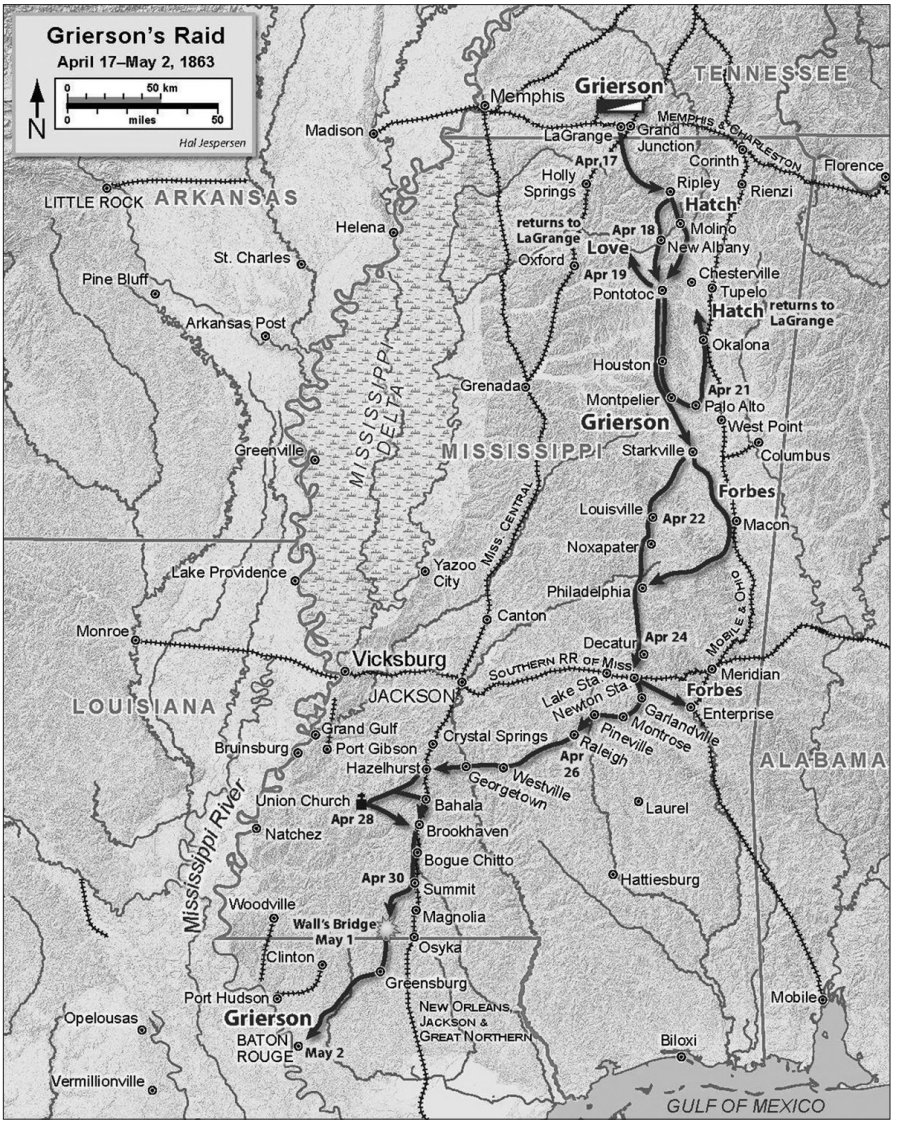
In April 1863, Grant launched a second Vicksburg Campaign, this time seeking to cross the Mississippi River south of the fortress. On 17 April, he dispatched a brigade of 1,700 cavalry and six small guns under Colonel Benjamin H. Grierson with the dual purposes of distracting Pemberton from Grant's movement and fixing Confederate forces, primarily their cavalry, away from the Union crossing site. Grierson avoided Confederate strengths and attacked weaknesses. He routinely detached subordinate elements to move on separate axes and made numerous feints to confuse the Confederates as to his real objective. He also employed an advanced reconnaissance force wearing Confederate uniforms to provide early warning of enemy forces.[6]

For 16 days, Grierson covered 970 km of enemy territory and destroyed more than 80 km of Confederate railways and telegraph wire.[7] More importantly, he fixed a division of Confederate combat power in a secondary sector while Grant crossed the Mississippi. His actions highlight the outsized operational effects that highly mobile maneuver forces can have on opposing armies as well as their commanders' minds.

During the 1945 Soviet invasion of Japanese-held Manchuria, the Red Army employed forward detachments of combined-arms mechanized divisions, corps, and armies to execute deep penetrations of Japanese positions and seize objectives that supported follow-on-force advances. These forward detachments operated jointly with Soviet air, airborne, and amphibious groups to penetrate up to 800 km into Manchuria and disintegrate Japanese command and control (C2) and transportation systems.[8] During the Cold War, Soviet military theorists used the forward detachment model to conceptualize the operational maneuver group. An operational maneuver group is:

> a highly mobile, combined arms formation intended to operate ahead of the main body of Warsaw Pact frontal forces. It would be commit-

Map 2. Grierson's raid in support of Grant's Vicksburg Campaign



Source: Mike Phifer, "Grierson's Raid in Support of Grant's Vicksburg Campaign," Warfare History Network, accessed 24 September 2025.

ted, through a gap created in enemy defenses by first echelon forces, to conduct a "deep operation" in the enemy rear.[9]

Operational maneuver groups would disrupt North Atlantic Treaty Organization's (NATO) C2, neutralize airfields, seize mobility corridors, and threaten enemy capitals in order to enable the success of follow-on-forces. Their employment would, ideally, force an early decision in conflict while avoiding NATO's

high-readiness frontline units and succeeding before NATO could mobilize additional forces or employ nuclear weapons.

Recent Developments in Unmanned Combat Vehicles

Mavericks of armored and aerial warfare during the interwar years pulled from contemporary conflicts and training exercises to develop their theories and doctrine. They also accounted for technical improvements in tanks and aircraft, the five most critical of which were described by Soviet brigade commander Georgii Isserson as increased speed, improved firepower, greater range, higher mobility, and mass production. Isserson particularly emphasized mobility, stating, "Everything that increases mobility enriches offensive potential. Defensive potential can be increased only by increasing firepower."[10] A treatise on the many technical developments of UCVs exceeds the breadth of this article and belongs to experts in the field but suffice it to say the five critical factors described above apply to UCVs today. The following section instead focuses on the performance of UCVs in recent conflicts, wargames, and training exercises as a means of examining their future potential.

Abqaiq-Khurais Attack

On 14 September 2019, Iran attacked Saudi oil refineries at Abqaiq and Khurais with a barrage of 18 loitering munitions and several cruise missiles.[11] These drones and missiles likely traveled 300–500 km and reached their targets despite the presence of Saudi antiaircraft guns and a Patriot missile defense system.[12] This small tactical action had strategic effects on the global petroleum supply chain and highlights the potential of future UCV attacks on national logistics infrastructure. The attack also demonstrated the benefits of combining loitering munitions with more expensive and capable missiles.

Second Nagorno-Karabakh War

During 44 days in 2020, Azerbaijan inflicted a significant military defeat on Armenia in the Second Nagorno-Karabakh War. It was the first war to feature mass-employment of unmanned systems executing reconnaissance strike complexes. Azerbaijan initiated the war with a rapid suppression of enemy air defense operation, destroying 50 percent of Armenia's air defense and 40 percent of its artillery in the first 15 minutes of the war.[13] Using remotely piloted biplanes to trigger Armenian radars and air defenses to engage, Azerbaijan loitering munitions and armed UAVs subsequently destroyed the exposed air defense systems. Azerbaijan combined these attacks with electronic warfare disruption of Armenian radar and artillery suppression of defensive positions, enabling UAV freedom of maneuver.[14]

Azerbaijani commanders established reconnaissance strike zones (RSZ),

a three-dimensional permissive fire control measure allowing human-out-of-the-loop (HOOTL) engagements by UCVs. HOOTL refers to "a weapon system that, once activated, can select and engage targets without further intervention by a human operator."[15] Satellites, reconnaissance UAVs, and small teams of clandestine Azerbaijani forces conducted target identification in RSZs for both UAVs and conventional fires.[16] Azerbaijan first destroyed key Armenian defensive network components (air defense, electronic warfare, C2, and fires), then attrited ground maneuver forces and interdicted supply lines.[17]

Simultaneously, a three-corps ground offensive exploited an Armenian defense fixed throughout its depth by RSZs. Two Azerbaijani corps fixed the Armenians along the northern portion of the front allowing Azerbaijan's main effort, the II Corps and a special forces element, to penetrate Armenians defenses in the south and capture the critical city of Shusha. Also of note, thick fog grounded UCVs for two days during the conflict, displaying the limitations of these systems.[18]

Russo-Ukrainian War

The ongoing Russo-Ukrainian War is emerging as a testing ground for UCVs akin to what the Spanish Civil War was for the *Wehrmacht*'s armored and air forces before World War II. On 29 October 2022, the Armed Forces of Ukraine (AFU) launched a multidomain swarm attack on the Russian Black Sea Fleet docked at Sevastopol, Crimea. In total, 16 unmanned systems—9 UAVs and 7 unmanned surface vehicles (USVs)—traveled 160 km across the Black Sea to the Russian port.[19] Reports on the success of the attack vary, but it likely damaged the Russian fleet's flagship and a minesweeper while losing all 16 drones.[20] While not operationally significant, this marked the first time a swarm of UAVs and USVs executed a joint strike on an enemy port and demonstrates the potential for future littoral swarm employment en masse.

UCV experimentation and proliferation continued during the relative operational stalemate of 2023–25. First, Ukraine expanded its deep-strike campaign against Russian infrastructure with drone attacks hundreds of kilometers deep in Russian territory.[21] Second, in December 2024, the Battle of Lyptsi became the first all-robotic air-land offensive in history. Although only a small tactical engagement with minimal consequence in the war, Lyptsi may one day be remembered similarly to the first insignificant uses of tanks on World War I's Western Front.[22]

Taiwan Wargames

Rand highlighted the potential for large numbers of low-cost, reusable UAVs in support of the defense of Taiwan in their publication, *Operating Low-Cost, Reus-*

able Unmanned Aerial Vehicles in Contested Environments. The UAVs in the wargame were a mix of XQ-58 Valkyries (8.9 hours loiter time, 9,362 km range) and a smaller "kitten" variant (5.6 hours loiter time, 6,182 km range), one-tenth the size of the Valkyrie. The defenders tasked the UAV group with maintaining intelligence, surveillance, and reconnaissance over the strait to enable the accurate delivery of Harpoon antiship missiles against People's Republic of China (PRC) vessels. To accomplish this, the UAVs established a 10,000-square-kilometer formation of 500 UAVs flying over the Taiwan Strait at 30,000 feet. They communicated and shared intelligence using a mesh communications network and a chain of relays.[23] The UAVs enabled the defenders to destroy more than 70 percent of the PRC fleet.[24] The wargamers mitigated the effects of enemy jamming by employing the UAVs at high altitudes, though the article admitted lower-altitude and overland employment would increase the success of enemy jammers.[25]

OFFensive Swarm-Enabled Tactics

Since 2017, the Defense Advanced Research Projects Agency (DARPA) OFFensive Swarm-Enabled Tactics (OFFSET) program has conducted coding, simulations, and field experiments focused on offensive drone swarm employment. Per DARPA's website, the stated objective of the program is to develop ground and air drone swarms that enable infantry units to seize eight square city blocks in four to six hours. The drone swarms, up to 250 UCVs in size, execute tactical enabling operations such as reconnaissance and surveillance and cordon and combine both UAVs and unmanned ground vehicles (UGV). The program completed its sixth urban field experiment in late 2021 and participated in the U.S. Army's Project Convergence 2022.[26]

The Swarm Maneuver Group

The swarm maneuver group is a highly mobile, combined arms, unmanned formation intended to enable the Joint Force to achieve cross-domain synergy. Swarm maneuver groups employ AI-enabled swarm tactics, converging mass, and multidomain capabilities to conduct deep maneuver to disintegrate adversary systems and decision making at both the tactical and operational levels. Swarm maneuver groups do not achieve decisive results on their own; they enable predominately manned forces to gain operational access and close with and destroy adversaries from a position of advantage.

Swarm tactics are coordinated and harmonious attacks on an objective from multiple directions. Swarm tactics require economy of force: attack with enough combat power to overwhelm the defender's ability to respond, but not so much as to produce target overkill. For example, an entire swarm maneuver

group regiment may be required to neutralize an aircraft carrier, while a single UCV may destroy a fuel truck.

Converging mass is the rapid assembly of dispersed forces at decisive points and moments, followed by the immediate disaggregation of forces once the desired effect is achieved. When not massed, swarm maneuver groups move in multiple, dispersed (horizontally and vertically) columns and routinely make feints and direction changes to confuse adversaries as to their intended objectives. Columns are mutually supporting, close enough to allow converging mass as opportunities present themselves.

Organization

This article presents two potential small maneuver group types: continental and littoral. Continental small maneuver groups operate in the air domain and consist entirely of UAVs. UGVs are not incorporated in the below design to maximize mobility and speed. Littoral small maneuver groups are specially designed to operate in coastal areas and consist of UAVs, USVs, and unmanned subsurface vehicles (USSVs). While the graphical depictions of small maneuver groups in this article are organized and symmetric for sake of clarity, in actual operations small maneuver groups will maneuver fluidly to complicate adversary targeting.

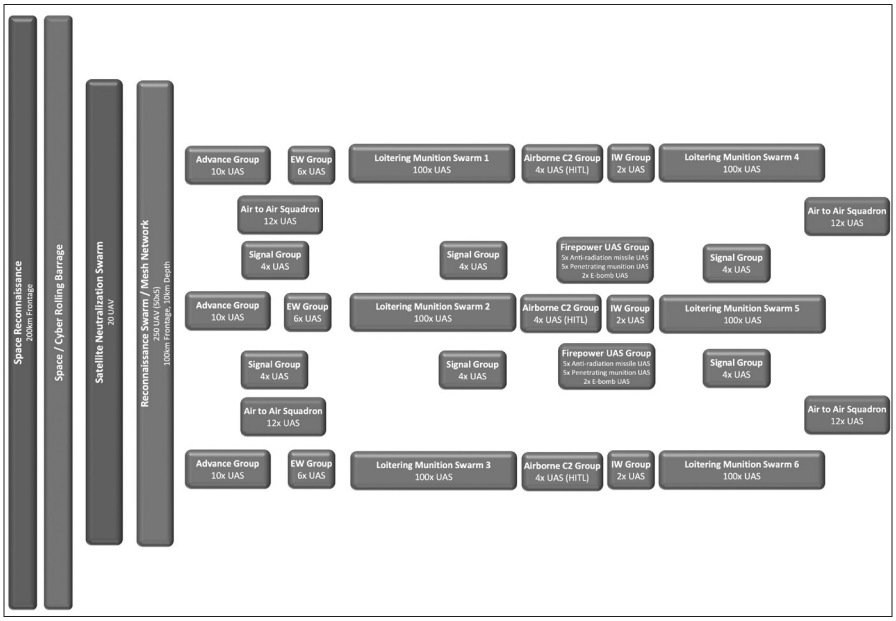
Small maneuver groups are employed in three sizes: regimental (supports maneuver division or Joint equivalent), division (supports maneuver corps or Joint equivalent), and corps (supports army or theater army or Joint equivalent). The continental small maneuver group regiment contains 1,012 total UAVs organized into nine subgroups and can conduct combined arms operations on up to three lines of operation. The littoral small maneuver group regiment has 728 UCVs organized into nine subgroups, and it is designed to combine aerial, surface, and subsurface swarms on a single line of operation. A small maneuver group division consists of three regiments, and a small maneuver group corps consists of three divisions.

The subgroups are broken down into two categories: swarm groups and enabling groups. Swarm groups are the small maneuver group's main firepower: mass-produced UCVs employed in kamikaze swarm tactics or aerial and subsurface minefields to deny enemy maneuver. Enabling groups are more exquisite UCVs that use combined arms effects to allow the swarm groups to accomplish their assigned task. The subgroups are as follows:

- **Satellite neutralization group (SNG)**: UAVs that maneuver in low Earth orbit with conventional or nuclear propulsion. One SNG supports up to one small maneuver group corps.
    - **Task**: Neutralize enemy low-Earth orbit satellites through elec-

tronic attack or affixing to satellites and propelling them back to Earth.
    - **Purpose**: Deny adversary space-based intelligence, surveillance, and reconnaissance, C2, and precision-navigation and timing.
- **Reconnaissance swarm**: Mesh network UAVs modeled on the above Rand wargame.
    - **Task**: Wide-area intelligence, surveillance, and reconnaissance queued by Joint reconnaissance.
    - **Purpose**: Queue swarm columns onto enemy forces or objectives. Enable accurate Joint fires.
- **Advance group**: UCVs with enhanced intelligence, surveillance, and reconnaissance capabilities. Ideally disguised to appear as enemy systems or nature.
    - **Task**: Aerial reconnaissance.
    - **Purpose**: Provide early warning to a small maneuver group.
- **Swarm group**: Groups of 100 relatively cheap, expendable kamikaze-style UCVs.
    - **Task**: Employ swarm tactics to destroy, neutralize, suppress, or disrupt enemy forces.
    - **Purpose**: Nested with Joint task force purpose.
- **Firepower group**: Standoff engagement UCVs armed with penetrating munitions, antiradiation missiles, and electromagnetic pulse bombs.
    - **Task**: Support and attack by fire. Precision strikes.
    - **Purpose**: Enable swarm group maneuver.
- **C2 group**: Remotely piloted UCVs capable of controlling or retasking small maneuver groups.
    - **Task**: Provide human-in-the-loop C2.
    - **Purpose**: Enable human C2 of small maneuver groups.
- **Signal group**: UCVs designed to enhance connectivity in degraded areas.
    - **Task**: Data sharing and communication between swarm groups and to Joint task force headquarters.
    - **Purpose**: Enable small maneuver group C2.
- **Electronic warfare group**: UAVs capable of electromagnetic jamming, deception, and reconnaissance.
    - **Task**: Suppression and deception of enemy radars and precision munitions. Electromagnetic reconnaissance.
    - **Purpose**: Disrupt adversary air defenses. Allow small maneuver group freedom of maneuver.
- **Information warfare group**: Signals intelligence UAVs capable of broadcasting via digital networks.

Figure 1. Horizontal plane view of a continental small maneuver group regiment



Source: courtesy of the author, adapted by MCUP.

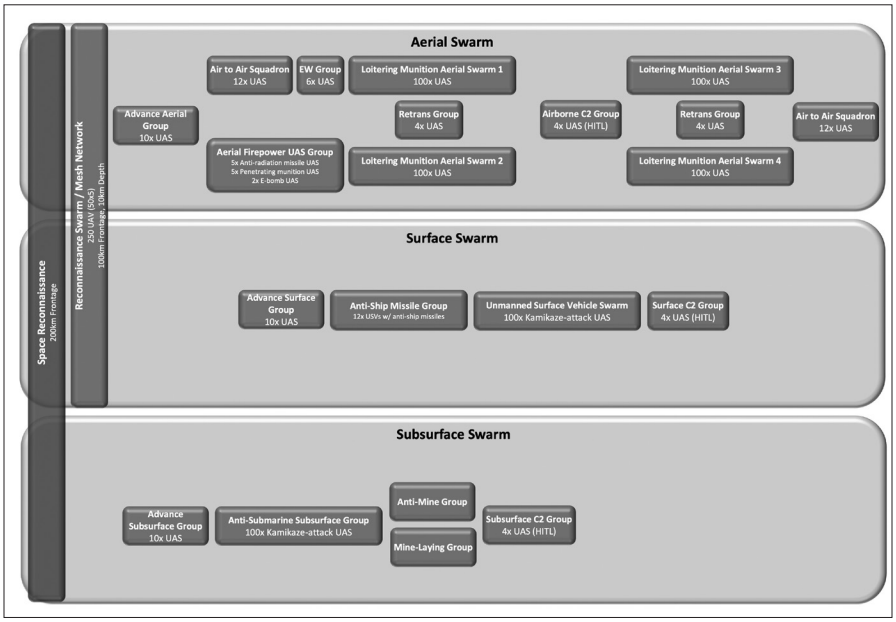
- ° **Task**: Deliver pro-U.S. information and messaging to digital devices.
- ° **Purpose**: Incite civil resistance against adversaries.

- **Air-to-air group**: Unmanned or remotely piloted fighter aircraft, likely models that are currently or soon to be retired.
  - ° **Task**: Combat air patrol.
  - ° **Purpose**: Defeat enemy aviation.
- **Antimine group**: USSVs designed to defeat enemy subsurface obstacles.
  - ° **Task**: Reduce subsurface obstacles.
  - ° **Purpose**: Enable subsurface swarm freedom of maneuver.

Various small maneuver group organizations should be tested in wargames and virtual environments such as the Warfighter Simulation program. If validated, further wargaming should refine the capabilities and design of the small maneuver group. Small scale field experiments should follow, then integration with the Joint Force in free play excises such as the National Training Center at Fort Irwin and Marine Air Ground Combat Center at Twentynine Palms.

Small maneuver groups must be forward postured to enable combatant commanders to employ them on day one of a crisis or conflict. The UCVs should be stored in distributed and concealed locations or on mobile platforms and hardened against both kinetic and electronic attack. Small maneuver

Figure 2. Vertical plane view of a continental small maneuver group regiment



Source: courtesy of the author, adapted by MCUP.

groups should be given HOOTL permission to scramble if adversary first strike operations are detected.

Small Maneuver Group Employment

Due to their high mobility, small maneuver groups are ideal maneuver forces to conduct indirect approaches in support of main body forces on more direct lines of operation. Harmonization between the two forces is critical. For example, a small maneuver group should begin a raid or saturation attack on an adversary while friendly main body forces enter the adversary's primary engagement area. A great historical example of unity of purpose is Grierson's raid enabling Grant's crossing of the Mississippi.

The second tenant is early and rapid offensive employment. Everyone has a plan until they get punched in the mouth. Small maneuver groups are forward stationed to be able to counterattack aggressors on day one of a conflict to prevent a fait accompli. Small maneuver groups should be programmed to execute operations in accordance with established operation plans on human approval or engagement criteria being met. In more deliberate operations, small maneuver groups typically operate forward of manned Joint Force formations.

The third tenant is cross-domain synergy and weaponeering. Small maneuver groups do not achieve strategic success on their own; they enable cross-domain synergy in the Joint Force. In the diagram below, forward stationed

U.S. forces, allies, and partners fix and disrupt adversaries in the contact layer. Joint all-domain fires, masking, protection, and deception enable small maneuver group penetration or infiltration of A2/AD. Satellite neutralization groups, space and cyber rolling barrages, trojan horse attacks, and long-range Joint fires enable small maneuver group freedom of maneuver in enemy rear areas. Small maneuver group raids and saturation attacks, combined with Air Force strategic bombing and air interdiction, disintegrate A2/AD from within. These attacks, combined with psychological and information operations, disrupt adversary decision making and exploit vulnerabilities in authoritarian regimes. These cumulative effects inflict system paralysis on adversaries, enabling the operational access or forcible entry of high readiness follow-on-forces such as airborne units, carrier strike groups, and amphibious ready groups.

Figure 3 is an example Joint task force penetration of the PRC's A2/AD system in the Western Pacific, overlayed on Isserson's deep operation concept.[27] Note SMG saturation attacks, raids, and Joint forcible entry operations disintegrate the PRC's A2/AD systems and enable Joint task force freedom of maneuver.

Small maneuver groups allow Joint task force weaponeering: exquisite Joint fires focus on the highest-value and most protected enemy targets while small maneuver groups mass on more vulnerable yet critical points, such as C2 and logistics. During Operation Desert Storm, there were more than 40,000 ground targets prosecuted during a 43-day campaign by an Air Force larger than today's. Against the PRC, there would likely be 100,000 or more such targets.[28] Instead of gradual attrition of a high value target list, small maneuver groups provide the mass to attack several decisive points simultaneously.

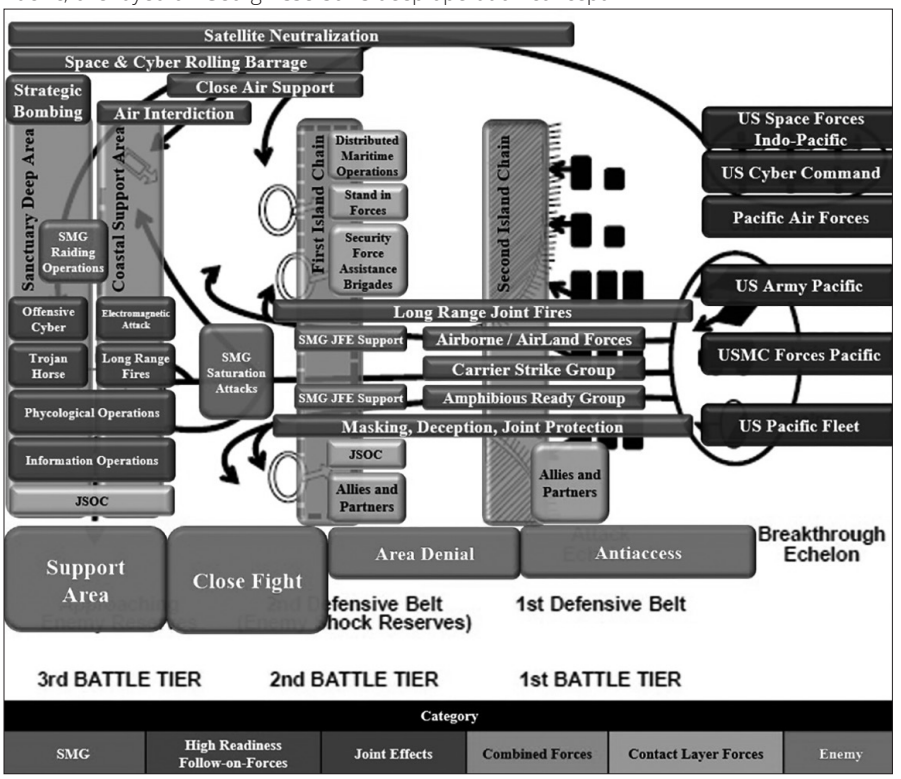
The fourth requirement for a small maneuver group's employment is the establishment of reconnaissance strike zones: RSZs are three-dimensional permissive fire control measures allowing HOOTL engagements by autonomous systems. AI-enabled identification, friend or foe algorithms, and engagement criteria allow UCVs to decide, detect, deliver, and assess at machine speeds, reducing kill chains to seconds. To shorten kill chains, Joint task force fires should not require clearance to fire into RSZs occupied solely by small maneuver groups.

The fifth and final tenants of small maneuver groups are their risk and expendability: small maneuver groups must be primarily or entirely unmanned and viewed as expendable. This enables Joint force commands (JFCs) to execute audacious, high-risk, high-reward operations against adversaries that may result in unacceptable casualties to manned formations.

The three basic methods of small maneuver group employment are:

1. **Raiding**: Raiding operations are modeled on Mongol and U.S. Civil War cavalry raids and Soviet operational maneuver groups (OMGs).

Figure 3. Example of Joint task force penetration of the PRC's A2/AD system in the Western Pacific, overlayed on Georgii Isserson's deep operation concept

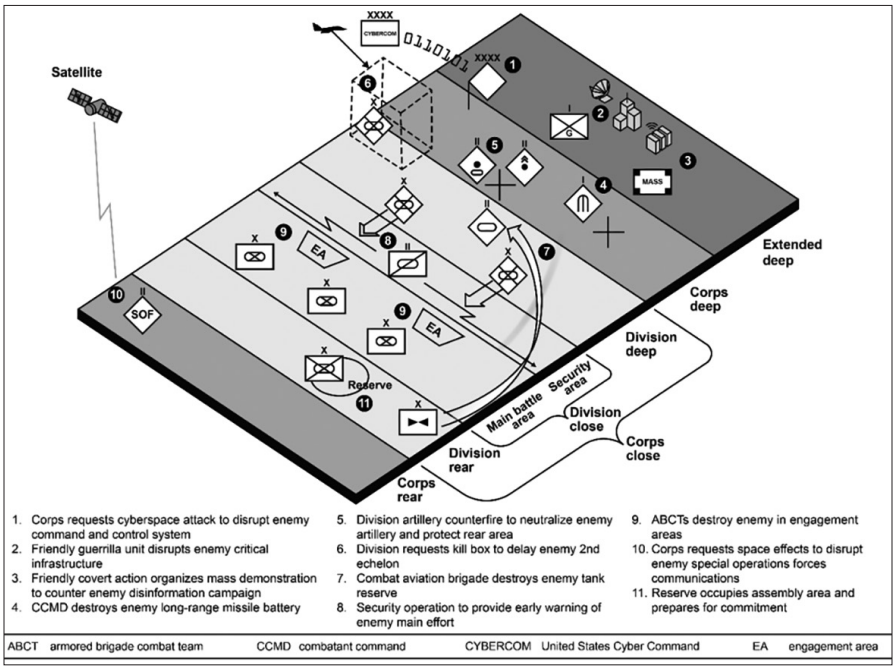


Source: base image from Georgii Isserson, *The Evolution of Operational Art*, trans. Bruce W. Menning (Fort Leavenworth, KS: Combat Studies Institute Press, 2013), 35, adapted by MCUP.

Small maneuver groups avoid enemy strengths and attack weaknesses such as enemy headquarters, C2 nodes, telecommunications infrastructure, depots, logistics infrastructure, electric plants, and other lightly defended but critical components of an enemy's warfighting potential. Raiding operations disintegrate enemy A2/AD and C2, interdict sustainment, demoralize adversaries, and disrupt their decision cycles. Small maneuver groups threaten every inch of an adversary's civil-military system, forcing enemies to divert combat power to support areas or let the small maneuver group run amok in their rear areas. Raiding small maneuver groups persist in the enemy's support zone as long as sustainment capabilities allow.

2. **Saturation attacks**: The Abqaiq-Khurais and Sevastopol attacks provided the inspiration for small maneuver group saturation attacks. In this employment, small maneuver groups mass against strongly defended yet critical adversary system components such as airfields, ports, air defense batteries, missile groupings, and enemy reserves. If

Figure 4. A small maneuver group reconnaissance strike zone overlayed on a notional U.S. Army operational framework for offensive operations



Source: base image from *Operations*, Field Manual 3-0 (Fort Belvoir, VA: U.S. Army Publishing Directorate, October 2022), 6-44, adapted by MCUP.

possible, small maneuver groups use deception and converging mass to achieve surprise prior to beginning saturation attacks. Even if detected and countered, saturation attacks will force defenders to commit massive amounts of surface to air and air to air munitions, creating opportunities for follow-on force exploitation. Small maneuver groups can also be committed against critical enemy main body forces, such as amphibious, airborne, or air assault groupings during enemy joint forcible entry operations. Though small maneuver group attrition will be extremely high in saturation attacks, the damage to critical enemy system components and preservation of follow-on-force combat power and human lives will merit the expense. Attrition operations must enable Joint Force success. As Vietnam taught military planners, kill counts do not always equal victory.

3. **Joint forcible entry**: Airborne, air assault, and amphibious Joint forcible entry are among the most difficult operations to execute. Small maneuver groups can fulfil three roles to enable joint forcible entry operations: advance guard, main body security, and aerial or littoral minefield. In an advance guard role, small maneuver groups conduct a reconnaissance in force of the approach heading and airhead line or

> beachhead, neutralizing enemy air defense, antiship, and counterattack forces that survived preassault fires. In main body security, small maneuver groups act as a three-dimensional shielding force for air and sea transports, interdicting enemy missiles and aircraft with kamikaze-style collision attacks. Once U.S. forces seize a lodgment, small maneuver groups establish an aerial or littoral minefield: a three-dimensional guarding swarm tasked with neutralizing enemy direct and indirect fires against the protected force. The aerial minefield occupies a hollow-cylindrical RSZ between the coordinated fire line and fire support coordination line. After lodgment stabilization and follow-on-force introduction, small maneuver groups can transition to raiding and saturation attacks in support of JFC offensive operations.

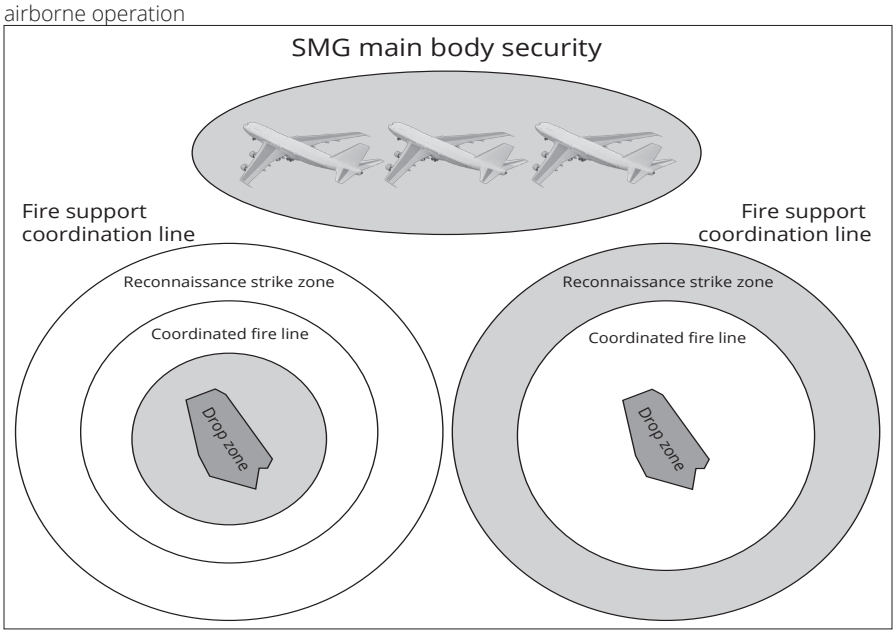
Small maneuver groups enable U.S. interests in competition and crisis. During competition, small maneuver groups offer increased aerial reconnaissance mass to company commanders. For example, in the South China Sea the reconnaissance and advance groups could increase surveillance of PRC gray-zone fishing fleets in Philippine waters. Filming their coercive methods and publishing it for the world to see could increase political pressure on the PRC to obey international law. Electronic warfare groups can jam the fishing fleets navigation systems and communications, and information warfare groups can spread pro-U.S., anti-PRC information to these proxies. Small maneuver groups should partner with Marine Corps stand-in forces, Joint Special Operations Command, and Army security force assistance brigades to train with partners and allies. SMGs must demonstrate their lethality and operational range to adversary decision-makers to inflict doubt on their ability to accomplish fait accompli campaigns. During crisis, small maneuver groups conduct demonstrations to display U.S. resolve to both deter adversaries and assure allies and partners. Small maneuver groups maintain the ability to conduct preemptive strikes on adversaries in conjunction with air forces and long-range fires.

Current Shortfalls and Limitations

As with tanks and aircraft during the early interwar years, UCV capabilities do not yet match the requirements necessary to transform the small maneuver group from theory to reality. While progress is constantly being made, the following capability gaps need to be addressed.

Sustainment: The small maneuver group needs to be capable of deep offensive maneuver and persistent presence in enemy territory. Hydrogen fuel cell batteries and solar power offer potential solutions to extending UAV endurance, as well as in-flight battery swaps currently being experimented with on the civilian market. As small maneuver groups are attrited, replacement UCVs

Figure 5. Visual depiction of a small maneuver group supporting a joint forcible entry—airborne operation



Top: A small maneuver group serves as main body security of transport aircraft. Left: A small maneuver group advance guard neutralizes enemy forces in the vicinity of a planned drop zone and confirms pre-assault fires effects. Right: A small maneuver group establishes an aerial minefield to protect an airborne lodgment.
Source: courtesy of the author, adapted by MCUP.

can be delivered via self-movement or aerial delivery. Forward-postured and disaggregated 3D-printing sites can produce swarm group UCVs in mass and their components as needed. During periods of competition, stockpiles of extra small maneuver group UCVs of all types should be mass produced to facilitate the high attrition likely in conflict.

Command and control: Improvements in AI-enabled swarm tactics, machine learning, data sharing, rapid identification friend or foe (IFF) software, and robust space-based C2 capabilities are all required to make the small maneuver group a reality. Using OFFSET as a baseline, digital and real-world exercises should be used to build data sets and improve algorithms. Joint all-domain command and control (JADC2) is a possible solution to the C2 requirements of small maneuver groups.

Protection: Against hostile kinetic fires, speed, and dispersion are the best protection measures for small maneuver groups. To increase resilience to electronic attack, UAVs must be hardened to resist effects and forward stationed in hardened sites. As an example, Russians implemented primitive measures to reduce the effects of jamming on their Iranian-purchased Shahed-136 loitering munitions in Ukraine.[29] In the event of GPS denial, small maneuver

groups navigate by AI-driven terrain association, celestial navigation, or preprogrammed coordinates. When jammed, UCVs must execute in accordance with AI algorithms or conduct a terminal attack. Small maneuver groups conduct feints, move in unpredictable manners, and disperse to overwhelm adversary sensors and decision making. In short, when employed en masse, the drone will always get through.

Weather effects: Storms, rain, fog, extreme temperatures, and other natural factors will reduce the effectiveness of small maneuver groups. They also provide opportunities for undetected infiltration of enemy territory.

Policy: SMG operations require national-level authorization to conduct HOOTL targeting and engagements in RSZs. IFF systems will need improvements to reduce the risk of collateral damage, especially over areas with significant civilian populations or when operating close to friendly forces.

Conclusion

As Heinz Guderian wrote in *Achtung—Panzer!*, the inspiration of this article, regarding the tank in 1937:

> On many issues there still exist differences of opinion of a sometimes quite fundamental nature. Only time will tell who is right. But it is incontrovertible that as a general rule new weapons call for new ways of fighting, and for the appropriate tactical and organizational forms. You should not pour new wine into old vessels.[30]

This is one attempt at not pouring new wine into old vessels. The methods and proposals in this article are far from perfect, and critiques and alternative opinions are encouraged. The goal of this article is not to be right but to ensure the Joint Force generates new ideas, dialogue, and purposeful action regarding the employment of UCVs in support of the Joint Operational Access Concept and Joint entry operations. If we do not, adversaries will. The only failure in this field will be a failure of imagination.

Endnotes

1. *Joint Concept for Entry Operations* (Washington, DC: Joint Chiefs of Staff, 2014), 10.
2. Chris Bellamy, "Heirs of Genghis Khan: The Influence of the Tartar-Mongols on the Imperial Russian and Soviet Armies," *RUSI Journal* 128, no. 1 (March 1983): 52–55, https://doi.org/10.1080/03071848308522218.
3. Timothy May, *The Mongol Art of War: Chinggis Khan and the Mongol Military System* (Barnsley, UK: Pen and Sword Books, 2007), 121–26.
4. Timothy B. Smith, *The Decision Was Always My Own: Ulysses S. Grant and the Vicksburg Campaign* (Carbondale: Southern Illinois University Press, 2018), 35.
5. Matt Atkinson, "Van Dorn's Raid," Mississippi Encyclopedia, 15 April 2018.
6. Tim Deforest, "Grierson's Raid during the Vicksburg Campaign," HistoryNet, 12 June 2006.

7. Deforest, "Grierson's Raid during the Vicksburg Campaign."
8. Elvis E. Blumenstock, *A Look at Soviet Deep Operations: Is There an Amphibious Operational Maneuver Group in the Marine Corps' Future?* (Quantico, VA: Command and Staff College, Marine Corps University, 1994).
9. Henry S. Shields, "Why the OMG?," *Military Review* 65, no. 11 (November 1985).
10. Georgii Isserson, *The Evolution of Operational Art*, trans. Bruce W. Menning (Fort Leavenworth, KS: Combat Studies Institute Press, 2013), 43–70.
11. "Missiles of Iran," Missile Threat, Center for Strategic and International Studies, 10 August 2021.
12. Natasha Turak, "How Saudi Arabia Failed to Protect Itself from Drone and Missile Attacks," CNBC, 19 September 2019.
13. John Antal, *Seven Seconds to Die: A Military Analysis of the Second Nagorno-Karabakh War and the Future of Warfighting* (Havertown, PA: Casemate, 2022), 22.
14. Uzi Rubin, *The Second Nagorno-Karabakh War: A Milestone in Military Affairs*, Mideast Security and Policy Studies no. 184 (Ramat Gan, Israel: Begin-Sadat Center for Strategic Studies, 2020), 7.
15. *Department of Defense Directive 3000.09, Autonomy in Weapon Systems* (Washington, DC: Department of Defense, 25 January 2023).
16. Nicole Thomas et al., "What the United States Military Can Learn from the Nagorno-Karabakh War," *Small Wars Journal*, 4 April 2021.
17. Antal, *Seven Seconds to Die*, 27.
18. Antal, *Seven Seconds to Die*, 28.
19. John C. K. Daly, "Ukraine Launches Unprecedented Drone Attack on Russian Black Sea Fleet's Sevastopol Headquarters," *Eurasia Daily Monitor* 19, no. 166 (8 November 2022).
20. Luke Harding and Isobel Koshiw, "Russia's Black Sea Flagship Damaged in Crimea Drone Attack, Video Suggests," *Guardian*, 30 October 2022.
21. Mick Ryan, "How Ukraine Has Changed the Character of War," *Futura Doctrina* (blog), 21 February 2025.
22. Mick Ryan, "The Battle of Lyptsi: Robotic Land Combat," *Futura Doctrina* (blog), 22 December 2025.
23. Thomas Hamilton and David A. Ochmanek, *Operating Low-Cost, Reusable Unmanned Aerial Vehicles in Contested Environments: Preliminary Evaluation of Operational Concepts* (Santa Monica, CA: Rand, 2020), 5–7, https://doi.org/10.7249/RR4407.
24. Hamilton and Ochmanek, *Operating Low-Cost, Reusable Unmanned Aerial Vehicles in Contested Environments*, 12.
25. Hamilton and Ochmanek, *Operating Low-Cost, Reusable Unmanned Aerial Vehicles in Contested Environments*, 13.
26. "OFFensive Swarm-Enabled Tactics (OFFSET)," Defense Advanced Research Projects Agency, accessed 13 August 2025.
27. Isserson, *The Evolution of Operational Art*, 35.
28. "Affordable Mass: Precision Guided Munition Requirements for Great Power Conflict," episode 63, 12 February 2022, in *Aerospace Advantage*, podcast.
29. Justin Bronk, Nick Reynolds, and Jack Watling, *The Russian Air War and Ukrainian Requirements for Air Defence* (London: RUSI, 2022).
30. Heinz Guderian, *Achtung—Panzer!: The Development of Tank Warfare*, trans. Christopher Duffy (London: Cassell, 2012), 226, Kindle.

Strategic Vulnerabilities in Space
U.S.-China Militarization and the Risks to Global Strategic Stability

Ameema Khalid

Abstract: This study investigates the militarization of space by the United States and China using the theoretical frameworks of technological determinism and the security dilemma. Data analysis of policy documents, military doctrines, and strategic literature reveals how technological advancements, mutual distrust, and dual-use technologies have transformed space into a contested domain. Findings indicate that the lack of international regulations and transparency exacerbates the risks of miscalculation and conflict. The study suggests actionable measures, including binding treaties, enhanced transparency, and conflict resolution mechanisms to promote peaceful space exploration. This research contributes to the broader discourse on space security by offering insights into managing militarization challenges in a rapidly advancing technological era.
Keywords: strategic stability, space militarization, technological determinism, security dilemma, military doctrines

Introduction

In 1962, President John F. Kennedy famously declared, "We choose to go to the Moon in this decade and do other things, not because they are easy, but because they are hard," embodying the aspirational vision that once unified humanity in space exploration.[1] However, outer space, once a symbol of collective progress, has now become a focal point of geopolitical competition. In 2022, global space-related spending surpassed $100 billion reaching $546 billion, highlighting the growing strategic significance of space.[2] The intensify-

Ameema Khalid is an MPhil scholar of defense and strategic studies from National Defense University, Islamabad, Pakistan, with research focusing on international law and the governance of emerging technologies, with a focus on space security, biotechnology, and AI in military innovation.

Journal of Advanced Military Studies vol. 16, no. 2
Fall 2025
www.usmcu.edu/mcupress
https://doi.org/10.21140/mcuj.20251602002

ing militarization, particularly between the United States and China, reflects a shift in global dynamics. This rivalry, fueled by dual-use technologies and the recognition of space's critical role in national security, economic prosperity, and technological leadership, presents both new opportunities and risks to global stability.

Space has historically represented humanity's highest aspirations, exemplified by milestones like the *Apollo 11* Moon landing in 1969 and the creation of the International Space Station, which began construction in 1998 and was finished in 2011.[3] The 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (colloquially known as the Outer Space Treaty [OST]) enshrined the principle of using space for peaceful purposes, free from weapons of mass destruction. However, as Scott Sagan noted, "Seemingly harmless inventions have often been repurposed for destructive ends."[4] Advances in dual-use technologies blur the lines between civilian and military applications, driving the current U.S.-China space competition. Strategic priorities are increasingly replacing collaborative aims.

Here, a distinction is necessary between the militarization and weaponization of space. Militarization is the incorporation of space systems into military activity like surveillance, navigation, reconnaissance, and missile warning functions, which is already advanced. Weaponization, conversely, involves the deployment of offensive and defensive weaponry in or through space with the intent to destroy or incapacitate targets. Contrary to general concerns, the complete weaponization of outer space has not yet been achieved.[5] Thus far, as of 2025, there have been initial experiments like China's 2007 direct-ascent antisatellite weapon (ASAT) test, the United States' 2008 intercept of USA-193 in Operation Burnt Frost, India's Mission Shakti in 2019, which successfully tested an ASAT weapon by destroying a satellite, and Russia's destructive test in 2021 against Cosmos-1408. Since then, there have been nondestructive demonstrations such as Russia's 2020 co-orbital test along with other directed-energy and co-orbital experiments.[6] These are only steps in the direction of weaponization and do not constitute a continued presence of weapons in orbit.

This research thus centers on militarization because it reflects the competitive dynamics already transforming strategic stability. Militarization via dual-use technologies, strategic doctrines, and security dilemmas pushes escalation and suspicion well before weaponization occurs. By examining militarization as an independent driver of instability, this article underscores how space competition is undermining strategic stability even without permanently stationing weapons in orbit.

Theoretical frameworks such as technological determinism and the security dilemma offer insights into this competition. *Technological determinism* suggests

Figure 1. U.S. defense support program early warning satellite Liberty, deployed to provide warning of missile launches during the Gulf War

Source: Curtis Peebles, *High Frontier: The US Air Force and the Military Space Program* (Washington, DC: Air Force History and Museums Program, 2020).

that technological advances inherently drive strategic behavior, as seen in developments in satellite and antisatellite technologies, which spark an arms race in space. The *security dilemma* explains how defensive actions by one state are perceived as offensive by another, intensifying distrust and militarization. These dynamics fuel the U.S.-China rivalry, with broader implications for global security.

The militarization of space poses significant challenges to global strategic stability, particularly regarding crisis management, arms race stability, and deterrence. Space-based infrastructure, vital for communication and surveillance, is highly vulnerable, as demonstrated by China's 2007 antisatellite test, which created debris threatening vital systems. Additionally, arms race stability is compromised as nations race to develop superior space capabilities, risking unsustainable escalation.[7] Deterrence is complicated by the ambiguity of space technologies, where dual-use satellites make it difficult to distinguish defensive from offensive actions, increasing the risk of miscalculation.[8]

This research examines the vulnerabilities arising from space militarization, emphasizing the need for enhanced governance, transparency, and international cooperation to mitigate these risks. As space becomes a more critical domain, the challenge is to ensure it does not evolve from peaceful exploration into unchecked exploitation and conflict. While exploration reflects collective scientific progress, exploitation highlights the pursuit of strategic and economic gains that risk augmenting rivalry. Addressing these issues will be crucial to maintain-

ing global strategic stability and securing a sustainable future for outer space.

As humanity ventures further into the final frontier, the stakes have never been higher, with national security, technological leadership, and the stability of global strategic relationships hanging in the balance. The militarization of space not only threatens the fragile equilibrium of global strategic stability but also jeopardizes the potential for space to remain a domain of peaceful exploration and shared progress. By understanding the drivers, risks, and implications of this phenomenon, this research aims to contribute to the development of strategies that ensure a secure and sustainable future for outer space.

U.S.-China Space Militarization: Potential Implications

The escalating rivalry between the United States and China for space militarization has raised significant concerns about its implications for strategic stability. As both nations actively pursue advanced space capabilities, the potential implications on international security are multifaceted. The development and deployment of space-based weapons and ASAT capabilities by the United States and China have amplified the concerns about the risk of an arms race extending beyond Earth's atmosphere. The absence of clear international norms and regulations governing space militarization further complicates the threat to strategic stability, as the potential for misunderstandings, miscalculations, and unintentional escalations looms large. The lack of established protocols for managing potential conflicts in space heightens the risk of destabilizing events that could impact Earth. The interdependence of modern economies and the global nature of modern security challenges places emphasis on a comprehensive and collaborative approach to address the implications of U.S.-China space militarization on strategic stability. There is a dire need to analyze the evolving dynamics of space militarization between the United States and China, exploring the associated risks to strategic stability and proposing viable frameworks for international cooperation. If left unchecked, the increasing militarization of space between the United States and China is likely to disrupt strategic stability.

This research provides a holistic analysis of the escalatory U.S.-China space militarization race and its potential impact on global strategic stability, crisis escalation risks, as well as deterrence issues. It also aims to examine the drivers behind the absence of robust arms control legislatures for space-based weapons and identify policy agendas for cooperative actions that can mitigate these threats to ensure a secure future for space as an equitable realm for peaceful explorations and sustainable global security.

Research on the Militarization of Space

The literature on space militarization presents a range of perspectives, examining strategic stability, historical comparisons, and emerging threats. Histor-

ical parallels, as discussed in Pericles Gasparini Alves's *Prevention of Arms Race in Outer Space: A Guide to the Discussions in the Conference on Disarmament* and Curtis Peebles's *High Frontier: The U.S. Air Force and the Military Space Program*, provide valuable insights into the Cold War's space race between the United States and the Soviet Union.[9] These works argue that the current rivalry between the United States and China in space bears similarities to that era. However, the world today is markedly different, shaped by multipolar dynamics and significant technological advancements. With new spacefaring nations entering the field, the challenge lies in crafting strategies to prevent the further militarization of space.[10]

Bleddyn E. Bowen's *Original Sin: Power, Technology and War in Outer Space* and Dean Cheng's works emphasize the realist perspective, where national security concerns drive space militarization.[11] Realism highlights the strategic advantage of controlling space assets vital for modern military operations. Yet, this viewpoint often overlooks other important factors such as economic interests, domestic politics, and technological progress. Introducing alternative theories, such as liberalism—focused on international cooperation or constructivism (emphasizing the role of norms and perceptions) could enrich the understanding of space governance.[12]

The rapid development of technologies like hypersonic weapons, directed-energy systems, and cyber capabilities poses challenges to existing frameworks such as the Outer Space Treaty.[13] These advancements blur the lines between civilian and military applications. Their military character is evident: hypersonic weapons are being tested as nuclear-capable delivery systems that oppose space-based early warning; directed-energy weapons are designed to blind or disable satellites, a key military enabler; and cyber operations increasingly attack satellite command networks, which was seen in the 2022 hack of an American satellite owned by Viasat, which impacted their KA-SAT network. The hack occurred on the first day of Russia's invasion of Ukraine on 24 February 2022.[14] China's 2021 test of a hypersonic glide vehicle illustrates the manner in which such technologies directly challenge strategic stability, observing that the OST's focus on weapons of mass destruction in space does not extend to the militarization of such new platforms.[15] Works like *The Hypersonic Revolution* by Richard P. Hallion underscore how technological determinism—the idea that new technologies drive progress and competition intensifies these challenges.[16] Ahmad Khan and Sufian Ullah's analysis points out the OST's shortcomings, particularly its lack of enforcement mechanisms to regulate dual-use technologies and ASAT weapon tests.[17] To address these gaps, the development of new treaties with robust verification mechanisms and risk-reduction strategies is critical. Confidence-building measures and transparency protocols are essential to prevent miscalculations that could escalate tensions.[18] While in the

current geopolitical landscape of U.S.-China tensions, Russia's estrangement, and India's growing counterspace capabilities, such negotiations seem unlikely; however, voluntary moratoria on destructive ASAT testing as the United States pledged in 2022, later joined by Japan, Canada, and some other nations and track 2 diplomacy could offer modest yet feasible ways to reduce risks until broader agreements become possible.[19]

Articles like Ulrich Kuhn's "Strategic Stability in the 21st Century: An Introduction" and Parliamentary reports like Claire Mills's *The Militarisation of Space* explore the deterrence dynamics between the United States and China.[20] While deterrence remains central to strategic stability, applying it to space introduces unique challenges. Unlike nuclear deterrence, space deterrence faces issues such as crisis instability and the dual-use nature of technologies. Addressing these concerns calls for innovative governance frameworks.[21] Effective communication channels and confidence-building measures can help avert unintended escalations. Decentralized governance models and multistakeholder approaches, as suggested by James Clay Moltz's article "The Changing Dynamics of 21st Century Space Power," could build trust and reduce risks.[22] Prioritizing international norms over unilateral measures is essential for long-term stability.

Critical Gaps in Legal Frameworks and Treaties

Despite the depth of existing literature, several critical gaps remain unaddressed. The limitations of current treaties, such as the Outer Space Treaty, highlight the urgent need for updated legal frameworks to address dual-use technologies and emerging threats like hypersonic weapons and directed-energy systems. The lack of enforcement mechanisms further exacerbates the challenge of ensuring compliance. Additionally, the unique characteristics of space deterrence, particularly its distinction from nuclear deterrence, remain insufficiently explored. The literature often downplays the risks of crisis instability and unintentional escalation in space, which could trigger conflicts.

Another overlooked aspect is the need for robust verification systems and effective communication channels to build trust and reduce risks. The proliferation of weapons in space, combined with inadequate frameworks to regulate their use, poses a significant threat to strategic stability. Furthermore, the concept of "peaceful use" of outer space remains ambiguously defined, especially concerning dual-use technologies that blur civilian and military applications. Greater clarity and consensus are required to guide international cooperation and governance. Finally, there is a lack of emphasis on interdisciplinary approaches that integrate technological, legal, and policy perspectives to ensure the long-term sustainability of space activities.

This article highlights the need to address the limitations of existing trea-

ties, incorporate diverse theoretical perspectives, and propose actionable solutions to mitigate the risks of space militarization. Further research is needed to develop effective verification systems, clearly define peaceful uses of outer space, and explore interdisciplinary approaches.

Theoretical Framework

This research uses the theories of *technological determinism* and *security dilemma*, which provides a broader understanding of the topic under consideration. Technological determinism provides insights into the objectives of the United States and China in space and analyses the implications of their endeavors on global strategic stability. On the other hand, the security dilemma thoery explores the threat perceptions of the United States and China and elucidates the need and the security concerns of both states in the space domain.

Theoretical Frameworks

Technological Determinism

Technological determinism asserts that technological advancements inherently drive societal and strategic transformations. In the context of U.S.-China space militarization, this theory explains the inevitability of advancements in space technologies fueling competitive dynamics. For instance, China established the Strategic Support Force (SSF) in 2015 to centralize space, cyber, and electronic warfare missions. In 2024, it disbanded the force and reorganized its functions into three separate entities: the Space Force, the Cyber Force, and the Information Support Force. This has triggered reciprocal measures from the United States such as its Space Force in 2019 and development of advanced satellite surveillance systems.[23] While these developments were not a direct response to the SSF, Department of Defense analyses made repeated references to adversaries (mainly China and Russia) counterspace advances as central arguments for establishing an independent Service dedicated to space. These actions reflect the autonomous trajectory of technological progress, where each state's innovations compel the other to respond, perpetuating an escalation spiral. The development of ASAT weapons by both nations further illustrates this deterministic cycle, as each perceives the other's advancements as a threat requiring a countermeasure.

While technological determinism provides valuable insights into the inevitability of technological progress shaping military strategies, it often downplays the role of human agency and governance. The theory assumes an unyielding trajectory of innovation, yet history shows that policy interventions and cooperative frameworks can mitigate escalatory tendencies, as seen in arms control efforts during the Cold War.

Security Dilemma

The security dilemma highlights how defensive measures by one state can be perceived as offensive by another, fostering mutual suspicion. This is evident in China's BeiDou navigation system. Although framed as a civilian project, its origins lie in the 1995–96 Taiwan Strait crisis, when Chinese leaders came to believe that reliance on the American controlled GPS had undermined their missile operations, underscoring escalation based on one state's actions that accelerated the other state's technology development in response:

> According to a retired Chinese general, China's military concluded that an alleged disruption to GPS caused it to lose track of some ballistic missiles it fired into the Taiwan Strait during the 1995–1996 Taiwan Strait Crisis. This was "a great shame for [China's military] . . . an unforgettable humiliation. That's how we made up our mind to develop our own global [satellite] navigation and positioning system, no matter how huge the cost. BeiDou is a must for us. We learned the hard way."[24]

This episode was interpreted in Beijing as humiliation and a stark reminder of strategic vulnerability, reinforcing the determination to build an independent navigation system regardless of costs. While conceived from a defensive logic of autonomy, BeiDou's evident military utility has raised alarm in the United States. Similarly, the U.S. deployment of the X-37B spaceplane—capable of rapid orbital maneuvering—has spurred concerns in China about potential offensive uses. The dual-use nature of these technologies underscores the difficulty of distinguishing between defensive and offensive intentions, thereby escalating tensions and complicating deterrence.

Historical parallels, such as the Cold War space race, reveal how perceptions of technological superiority often spiral into arms races. However, the security dilemma's assumption of rational actors sometimes overlooks ideological or economic motivations that drive state behavior. For instance, China's investment in space infrastructure is not solely defensive but also tied to broader economic ambitions, such as the Belt and Road Initiative's space component.

The Fragile Balance: Strategic Stability Risks in the U.S.-China Space Race

Imagine a stool with three legs—unsteady, yet remarkably sturdy. This fragility accurately represents the intricate balance of power referred to as strategic stability, which serves as the foundation of international relations. It represents a condition in which powerful nations are deterred from employing military force against one another.[25] The preservation of this delicate equilibrium is crucial to avert conflict and uphold peace.

The escalating rivalry between the United States and China in space militarization is undermining the core concepts of strategic stability, causing uncertainty about their effectiveness and giving rise to concerns about the future of global security. As the fight for supremacy in space grows stronger, the possibility of wars, uncontrolled arms races, and weakening deterrent systems becomes a significant concern, leading to a pressing need to consider the consequences for the future of peace on Earth. By discussing the concept of strategic stability and its tiers, this research illustrates implications of the U.S.-China space militarization arms race, crisis stability, and deterrence stability.

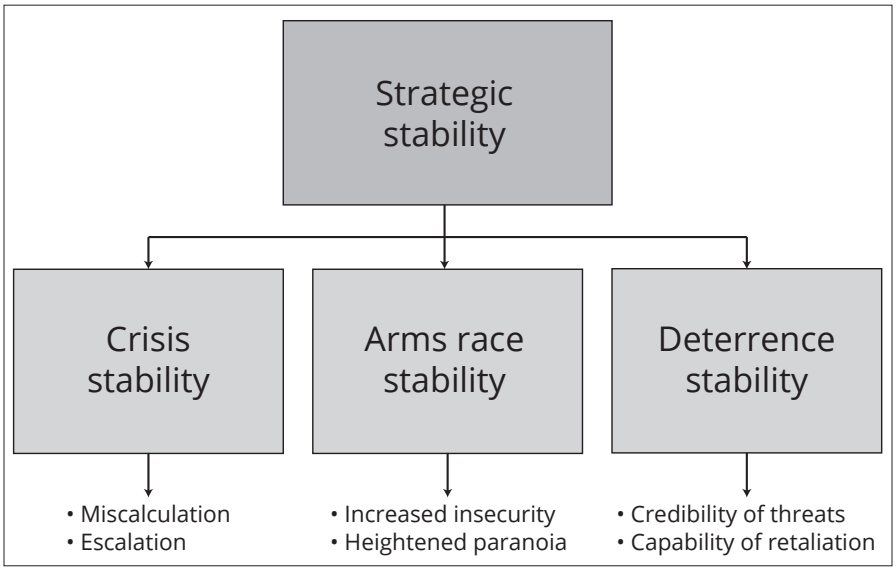
Tiers of Strategic Stability

The concept of strategic stability is based on three core pillars: crisis stability, arms race stability, and deterrence. Crisis stability refers to the capacity of nations to effectively and peacefully address and resolve international crises. This is crucial because even minor crises have the potential to grow into more significant wars. Various elements, including miscalculations, escalation, and unintended accidents can erode crisis stability. *Miscalculation* arises when a nation inaccurately assesses the intentions of another nation. *Escalation* is the process by which a situation intensifies and becomes unmanageable. Unintentional accidents might also give rise to conflict.

Arms race stability denotes a state in which nations do not feel obligated to constantly augment their military capabilities. When nations participate in an arms race, it can develop a sense of insecurity and paranoia, which heightens the likelihood of conflict, whereas deterrence is the capability of a state to discourage an opponent from launching an attack against it. Deterrence relies on the prospect of retaliation. For a deterrent threat to possess credibility, it must be perceived as believable. The other nation must have confidence that the deterring nation will genuinely carry out its threat in the event of an attack. To possess the capability of deterring, a threat must possess a capacity to cause substantial harm to the aggressor.[26]

These pillars interact to establish a conducive environment in which countries experience a sense of security and are less inclined to engage in armed aggression. The process of militarizing space by the United States and China is causing substantial challenges for the three tiers. The likelihood of crises turning into conflicts is being heightened, along with the destabilization of arms race dynamics and the undermining of conventional deterrent approaches. The production and placement of sophisticated space-based weapons and technologies create additional sources of instability in global affairs, presenting substantial obstacles to the preservation of peace and security in outer space.

Figure 2. Tiers of strategic stability



Source: courtesy of author, adapted by MCUP.

Risk of Crisis Instability and Escalation

The increasing development and deployment of offensive counter-space capabilities by both the United States and China raises significant concerns for crisis instability in the space domain. Although these capabilities may seem small, they have the capability to greatly destabilize the fragile balance of power and set off a series of destabilizing actions and reactions between these two prospective rivals. Crisis instability pertains to the susceptibility of the space domain to intensify tensions and conflicts during times of crisis or increased geopolitical rivalries.[27] The inherent threat stems from the fact that even very slight improvements to offensive counter-space capabilities can cause significant discomfort and anxiety among competitor states, resulting in increased tensions and intensifying competition. The unpredictability of crisis instability in space is exacerbated by the ambiguity surrounding the consequences of such situations. Although the precise outcome of a space crisis cannot be foreseen, the risk of crisis instability is significant and is projected to increase as the United States and China further develop offensive counter-space capabilities.

Crisis Instability and the Offense-Defense Conundrum in Space

Thomas C. Schelling illustrates crisis instability through a scenario where armed individuals fear the other will shoot first, prompting preemptive action.[28] This analogy mirrors space militarization, where the United States and China, driven

by strategic distrust, may consider first strikes advantageous to avoid perceived vulnerabilities. The asymmetric benefits of preemption—particularly in neutralizing ASAT capabilities—can incentivize rapid, decisive action, escalating tensions.

Space conflict risks are heightened by reduced human cost and the strategic imperative to maintain dominance. For example, the United States may opt for a preemptive strike to incapacitate China's ASAT systems, viewing this as essential to protect critical assets and strategic dominance. However, such measures risk triggering uncontrollable escalation.[29] Retaliatory cycles could destroy satellites, disrupt global communications, and create long-term space debris, jeopardizing space stability.

Additionally, the U.S.-China rivalry in space is also exacerbated by ambiguity surrounding offensive and defensive maneuvers. Unlike terrestrial warfare with defined boundaries, space operations lack clarity.[30] For instance, destroying a satellite might be framed as defensive, but without sovereignty in orbit under the OST, such acts are more likely interpreted as strategic aggression. This dual-use nature of technologies like lasers and cyber tools further blurs distinctions, complicating intent interpretation.

Such uncertainty fosters crisis instability. Imagine China destroying a U.S. surveillance satellite passing over its territory claiming defense, while the United States perceives it as a hostile act undermining intelligence capabilities. Current norms like the OST guidelines for peaceful use, the United Nations Committee on the Peaceful Uses of Outer Space norms, and more recent political undertakings like the U.S. commitment not to conduct destructive ASAT tests offer some constraint.[31] However, they are voluntary, sporadically followed, and have no strong enforcement, so the threats of miscalculation and escalation remain.[32]

The disparity in interpretation can exacerbate suspicions and intensify animosity among states, hence augmenting the likelihood of conflict escalation. Perception has a critical role in the interpretation of actions in space.[33] Engaging in the destruction of an adversary's satellite, even in a defensive manner, when it is located above your own territory, may be interpreted as an aggressive action. For example, in the event that a U.S. missile defense system successfully neutralizes a Chinese satellite that was inadvertently approaching low-Eart orbit over U.S. territory China may perceive it as an unwarranted act of aggression, despite the U.S. intention to safeguard itself from an unanticipated but potential threat.

Deploying ASAT weapons exacerbates this offense-defense conundrum by lowering conflict thresholds. If either the United States or China employs ASAT systems, mutual vulnerability could spiral into large-scale conflict, driven by reciprocal escalation and mistrust.

Vulnerability of Space Centers of Gravity: A Threat for Crisis Escalation

Space plays a pivotal role in national power, serving as a key battleground in U.S.-China rivalry. This competition for strategic superiority is not merely hypothetical but poses a genuine risk of escalating into conflict. At the heart of this struggle are centers of gravity (COGs), critical resources, capabilities, and advantages that enable states to achieve objectives and exert influence in space.[34] These include satellites, space stations, ground control facilities, launch sites, and communication networks, forming the cornerstone of a nation's space infrastructure.[35]

The race to secure dominance over COGs has profound implications for crisis stability. Significant investments by both nations in space infrastructure mean that any perceived threat to a COG could trigger a "use it or lose it" mindset, prompting preemptive strikes and initiating a perilous cycle of escalation. This competition is further exacerbated by the intrinsic vulnerabilities of space COGs, such as the limited maneuverability of satellites.

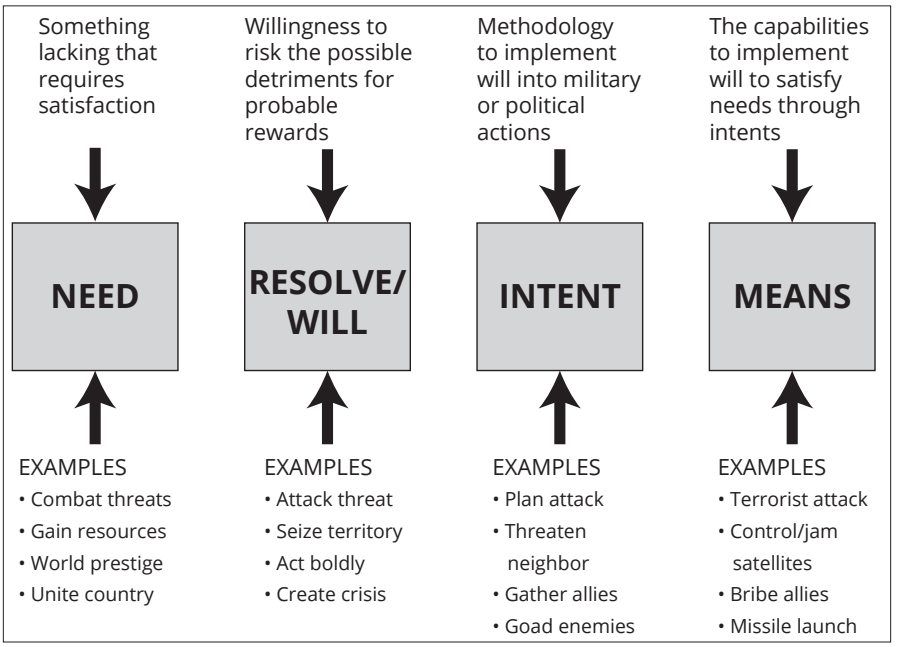
Military strategists in both nations prioritize identifying and exploiting weaknesses in their opponent's COGs. Through wargaming simulations, they evaluate scenarios to devise countermeasures and preemptive strategies. However, preemptive actions based on incomplete intelligence risks miscalculations, misunderstandings, and unintended consequences, potentially escalating into a large-scale space conflict. Such hostilities amplify the risks of destabilization, undermining crisis management and intensifying global tensions.

To mitigate these risks, both nations must prioritize dialogue, transparency, and strategic restraint. Without these measures, the competition for space COGs threatens to destabilize global security and escalate conflicts into uncharted territory.

Resource Competition and Quest for Dominance: A Threat to Global Peace

Both the United States and China recognize the immense strategic importance of space resources as pivotal to achieving geo-economic leadership and asserting global influence. Control over critical space positions and regulatory frameworks grants these nations the ability to shape wealth distribution, assert dominance, and influence the emerging global order.[36] This high-stakes competition increasingly raises the prospect of unilateral sovereign claims or territorial appropriation in space, such as declaring exclusive economic zones or defense identification zones.[37] Although there are some states, like the United States, that have committed to restraint on ASAT testing that is destructive, such steps do not respond to wider sovereignty issues. Unilateral assertions of space ter-

Figure 3. The center of gravity depicting the need, will, and intent of any state or military force to make decisions, strategies, devise a course of action, and shortlist means to accomplish its objectives and vested interests



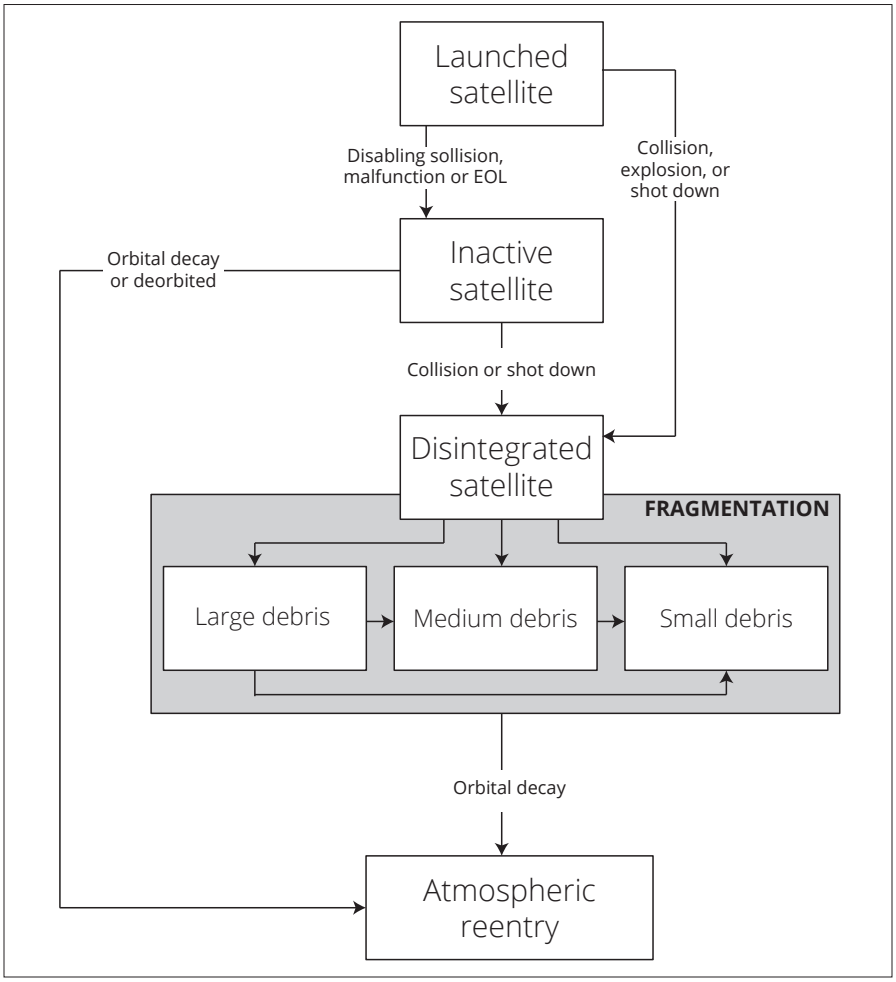
Source: courtesy of author, adapted by MCUP.

ritory or resources would violate Article II of the OST, which forbids national appropriation of outer space, and invite defensive escalation.[38]

In this context, one actor's attempts to assert dominance may trigger coercive countermeasures from the other, aimed at preserving national identity, strategic objectives, and geopolitical status. These measures could range from targeted military interventions to leveraging economic tools, such as disrupting supply chains or neutralizing critical assets. The dual-use nature of space technologies—serving both civilian and military purposes—further compounds the difficulty of distinguishing peaceful endeavors from aggressive maneuvers. Perceived threats, like ASAT capabilities, often blur the line between defense and offense, intensifying mutual distrust.

China's 2007 direct-ascent capability test, designed to destroy satellites and augment missile defense, exemplifies this duality. The precedent for destructive ASAT testing was first set by the United States in 1985 and reaffirmed in 2008 with the intercept of the USA-193 satellite.[39] Chinese adventure, however, marked the first such demonstration in the twenty-first century and set a precedent that stoked concerns about space weaponization.[40] Similarly, in 2008 the U.S. interception of a satellite using missile defense systems demonstrated

Figure 4. Hypothetical illustration of Kesseler Syndrome depicting how space accidents causing debris can lead to inadvertent escalations



Source: Bettina M. Mrusek, "Satellite Maintenance: An Opportunity to Minimize the Kessler Effect," *International Journal of Aviation Aeronautics and Aerospace* 6, no. 2 (2019): https://doi.org/10.15394/ijaaa.2019.1323.

the inherent ambiguity of dual-use technologies, further destabilizing strategic perceptions.[41]

The crux of the challenge lies in deciphering intentions. Misjudging defensive postures as offensive threats, or underestimating provocations, risks spiraling tensions into conflict.[42] The opacity surrounding space activities amplifies the dangers of miscalculation and reactionary cycles. To avert escalation, the United States and China must prioritize transparency and dialogue, fostering mutual understanding to ensure that space remains a realm of stability, cooperation, and shared progress.

The Domino Effect: A Hair-Trigger Threat

Satellites are marvels of engineering, but they are expensive and intricate pieces of machinery. Even a strike with a small bit of space debris can make them entirely useless. As opposed to fighter aircraft, which can be damaged slightly and still operate, satellites do not have redundancy when breached, so they are particularly vulnerable. This vulnerability is best shown by the Kessler Syndrome (see figure 4), a hypothetical situation in which successive accidents produce a debris cloud that obstructs future space activities for decades. [43]

A Russian weather satellite, Parus, and a retired Chinese rocket had a close call but no collision in October 2020.[44] The event indicates how unstable the space environment is and how easily even small miscalculations can have far-reaching consequences in the form of a chain reaction. What if this kind of collision had really happened, sending debris damaging both countries' vital communication satellites? Tensions may quickly rise as a result of the allegations and finger-pointing that would occur, leading both sides to possibly take retaliatory action. This instance demonstrates the domino effect's vulnerability by implying that a single attack might destabilize a balanced deterrent environment. In this case, even an accidental collision on a vital satellite may set off a catastrophic series of counterattacks that would destroy infrastructure and pull both countries into a confrontation that might have worldwide consequences. This vulnerability is being exacerbated by the United States' and China's expanding space arsenals.

Defense systems and antisatellite capabilities are being developed by China's newly formed Aerospace Force in April 2024 (following the 2024 dissolution of the Strategic Space Force) and the U.S. Space Force. These systems can result in errors in perception and unintentional escalation because they are meant for quick responses in the event of a conflict.[45] For example, China is concerned about the U.S. Boeing X-37B spacecraft's potential for offensive maneuverability due to its reusable design and concealed cargo. Yet, Beijing has also pursued similar capabilities, launching its own reusable spaceplane in 2020 and 2022, underscoring the action–reaction dynamic of space competition.[46] Now consider the following scenario: China misinterprets an X-37B routine mission as a lead-up to an attack. This misconception might result in a preemptive strike on a vital U.S. satellite, setting off a domino effect of counterattacks.

Due to the satellites' susceptibility to collisions as well as the possibility of errors in perception and calculation, a volatile atmosphere is created where even a minor incident has the potential to escalate into a major war.[47] Prioritizing dialogue, openness, and confidence-building measures are crucial as both the United States and China develop space capabilities in order to reduce the possibility of unintentional escalation and maintain peace in the space domain.

Technological determinism and the security dilemma suggest that tech-

nological advancements shape military doctrines and the development of capabilities, ultimately shaping the power balance. The pursuit of superiority in space capabilities is a defining factor in the strategic rivalry between these two major powers. The belief that technological progress yields a strategic advantage introduces inherent instabilities, disrupting traditional notions of strategic stability. The pursuit of superior space capabilities challenges the delicate balance necessary to prevent conflict, creating a paradox. The dual nature of space capabilities lies in the fact that the same technologies developed for launch vehicles, satellites, and others can serve both military and civilian purposes, which can also serve both defensive and offensive purposes. This causes a dual-use-dilemma and can escalate tensions, contribute to an arms race, and bring the world near unavoidable conflict.[48]

The U.S.-China space arms race poses escalation risks due to the competitive environment created by advanced capabilities. This competition increases the risk of miscalculation, misinterpretation, or accidental triggering of conflicts in space. The arms race dynamics raise concerns about the fragility of strategic stability. Each state is deploying cutting-edge technologies, believing it enhances security. However, this competition introduces the risk of unintended escalation.[49] The concept of "spillover" in escalation dynamics can be applied to the space domain, extending conflicts beyond their original scope. The fragility of the pursuit of technological supremacy demands sophisticated diplomatic initiatives and mitigation strategies to navigate the complexities of space militarization in an era dominated by technological determinism.

Challenges of Arms Race and Arms Control in Outer Space

The United States' and China's burgeoning space competition offers an unprecedented and worrisome phase of arms race instability that the world has rarely seen. Unlike the Cold War, where rivalry was primarily state-driven and nuclear-focused, today's contest involves dual-use technologies, commercial actors, and contested governance, creating unprecedented risks for escalation. The ramifications of these two countries' competition for supremacy in the last frontier extend beyond national boundaries, posing important queries regarding the future trajectory of space exploration, collaboration, and security. Arms race instability is the term used to describe the situation in which two or more states' pursuit of military superiority causes tensions to escalate, trust to erode, and the likelihood of conflict to increase. In a situation like this, each side aims to outcompete the other militarily, which fuels a spiral of armaments accumulation and elevated tensions.[50] This dynamic is often described as Thucydides' Trap; that is, the structural tension between a dominant power and a rising power. Just as Sparta feared the ascent of Athens, the United States today

faces strategic anxiety over China's rapid rise.[51] The threat is not only in space weapons accumulation but in the way perceptions of vulnerability can push both sides toward confrontation.

The arms race's inherent danger and uncertainty, which includes the possibility of miscalculation, misinterpretation, and unintentional escalation are the root cause of the instability. Technological developments, geopolitical rivalry, strategic competition, and the proliferation of space weapons are some of the variables that might aggravate this instability.[52] In the end, the instability of the weapons race raises the probability of conflict and jeopardizes global security and stability. The instability of the arms race takes on a new dimension in the context of the U.S.-China space race. Both countries are actively working to develop and employ cutting-edge space-based military capabilities. The collective-action dilemma could result from any action taken by one side that sets off a series of escalations and retaliations in the goal of military control in space.[53]

Escalating Arms Race and Destabilization of Mutually Assured Destruction in Space

A perilous feedback loop between the United States and China is intensifying as both nations pursue missile defense systems and ASAT weapons, escalating capabilities and tensions. These technologies, even during development, are perceived as threats, prompting both sides to expand their space arsenals. This cycle risks undermining deterrence by enabling preemptive strikes, further destabilizing the strategic balance.

The concept of mutually assured destruction has now extended into the space domain, introducing unprecedented risks.[54] Unlike the nuclear mutually assured destruction of the Cold War, space rivalry builds a unique kind of instability. Since satellites are extremely susceptible to preemptive attack, there is always a "use-it-or-lose-it" problem: countries might worry about losing vital communications, navigation, and intel networks at the start of a conflict, which might encourage dangerous escalation. Such an attack would not only blind military forces but also severely disrupt civilian life, highlighting the catastrophic consequences of space warfare. Moreover, the use of ASAT weapons rather than mere deployment exacerbates this instability by creating debris fields that could render critical orbital regions unusable for centuries, effectively locking humanity out of vital space resources.

The dual-use nature of missile defense systems further fuels suspicion. They are not considered "dual-use" technologies in a strict sense because they serve a noncivilian function. However, they often possess a dual capability; the same interceptors designed to target ballistic missiles can also be employed against satellites, as demonstrated in the U.S. 2008 Operation Burnt Frost.[55] China

perceives U.S. advancements in missile defense as direct threats to its space infrastructure, driving its own counter-space and ASAT developments and accelerating the arms race.

Both nations seek to protect space assets, but their actions escalate the likelihood of a catastrophic conflict. Without strategic restraint, dialogue, and cooperative frameworks, space-based mutually assured destruction threatens to destabilize global security, extending conflicts far beyond Earth's boundaries and placing humanity's future in space at grave risk.

The Nature of the Space Arms Race

Compared to conventional terrestrial arms races, the arms race fueled by China's and the United States' militarization of space offers a distinct perspective. Space, as opposed to land, sea, or air is a shared environment. Historically, the goal of arms races has frequently been to obtain an advantage in particular areas. But in space, a nation's actions might inadvertently affect other nations. When a satellite is destroyed while in orbit, debris is released into orbit that might harm or destroy other satellites, making peaceful space exploration impossible for every state.

The primary goal of traditional weaponry is immediate devastation. ASATs and other space weapons, however, add a new level of complication. Not only does destroying a satellite render it inoperable but it also leaves a cloud of debris in the orbit. This debris has the potential to collide with other satellites, starting a chain reaction that might escalate the crisis.[56] Furthermore, site inspections and verification of weapon stocks were a common feature in conventional arms races. A certain amount of confidence and verification about arms control are made possible by this transparency. It is far more difficult to monitor and validate space capabilities, though. Dual-use satellites are those that can be used for both military and civilian purposes.

While the Registration Convention (1976) commits states to giving basic details on space objects placed in orbit, it does not mandate revealing their exact purposes or military uses.[57] This permits nations to maintain secrecy about the true capabilities of their space programs, making verification and trust more difficult. Finally, disarmament in a conventional arms race refers to the destruction of weapon stockpiles. But the issue is even more complicated in space. Debris removal from orbit is now a very expensive and difficult task. The large debris objects can be removed at exorbitant cost, but tiny untrackable fragments cannot be cleared currently, making complete debris removal totally impossible. It would take a long time and great effort to mitigate the current debris population, even if nations came to an agreement on an arms control treaty.[58]

Table 1. Differences between conventional and space arms race

Features	Conventional arms race	Space arms race
Battlefield	Land, sea, and air	Outer space
Nature of weapons	Tanks, aircraft, missiles, nuclear weapons	Satellites, antisatellite weapons, directed-energy systems
Verification	Relatively easier (treaties, inspections)	Very difficult (dual-use technologies, covert programs)
Disarmament	Achieved through arms control agreements (e.g., Strategic Arms Reduction Treaty, Intermediate-Range Nuclear Forces Treaty)	Limited success; no binding treaty banning space weapons
Targeted regions	Specific geographic regions (borders, theaters of war)	Entire globe (space-based assets affect all regions)

Source: courtesy of author, adapted by MCUP.

Arms Control Efforts in Space: A Flawed Framework

Outer space is often viewed as a lawless frontier, yet it is governed by a framework of international laws designed to regulate human activities and prevent conflict. The United Nations Charter, international humanitarian law, and the 1967 Outer Space Treaty collectively provide guidelines for how states should behave in space.[59] These include obligations concerning registration, accountability, liability, and contamination prevention. While efforts to prevent space-related conflicts, including the deployment of weapons, have been ongoing, the legal landscape remains underdeveloped and fragmented.

Although the OST is frequently considered a nonarmament treaty, it contains crucial provisions that indirectly support arms control. Drawing from the 1963 Partial Test Ban Treaty, the OST prohibits the placement of nuclear weapons or other weapons of mass destruction in space or on celestial bodies. It mandates that celestial bodies, such as the Moon, be used solely for peaceful purposes. However, the OST does not place extensive restrictions on the use, testing, or deployment of conventional weapons, either in space or directed toward space objects. This legal gap has been a point of concern as states like the United States and China intensify their space-related military capabilities.

Further arms control efforts are seen in the Hague Code of Conduct, which includes transparency measures for space activities, and the Environmental Modification Convention, which prohibits the use of environmental manipulation techniques for military purposes.[60] The Anti-Ballistic Missile Treaty, though historically significant, no longer holds relevance after the United States formally withdrew in 2002, citing the need for unconstrained missile defense development.

A significant issue in space governance is the ambiguity surrounding the

term *peaceful purposes* in the OST. This lack of definition is fueling uncertainty, particularly amid the escalating space competition between the United States and China. The OST's advocacy for space to be used for peaceful purposes without a clear definition creates a gray area, allowing states to engage in dual-use space activities—technologies that can serve both civilian and military objectives.[61] This lack of clarity enables countries to develop space programs with potential military applications while still remaining formally adherent to the OST's peaceful intent, exacerbating geopolitical tensions.

The United States and China, both leading space powers, increasingly engage in activities with dual-use capabilities. China, for instance, has conducted antisatellite tests, such as the 2007 ASAT demonstration, which, although not violating the OST, showcased its ability to deploy space-based weapons. Unlike dual-use technologies like launch vehicles, this ASAT demonstration was explicitly military in design, yet it raised concerns regarding the distinction between compliant dual-use programs and overt weaponization. This event heightened concerns in the United States, which viewed it as a threat to the peaceful use of space. These incidents underscore the mistrust between the two nations, hampering collaboration and fostering a competitive escalation that could lead to an arms race.[62]

Moreover, the absence of a precise definition of peaceful purposes complicates verification efforts. For example, determining whether a satellite designed for Earth observation is solely for civilian use or could have military applications for targeting becomes a subjective judgment. Without clear criteria, verification of compliance with the OST becomes prone to bias and suspicion. Even overt military systems do not breach the OST, which bans weapons of mass destruction in space, leaving compliance intact but skepticism augmented, thus further straining relations between space-faring nations.

This uncertainty contributes to a climate of secrecy in space programs, with both the United States and China reluctant to disclose comprehensive details of their activities. Because OST does not define peaceful purposes explicitly, disclosing any dual-use capability would cause misinterpretation as militarization, thus this uncertainty incentivizes states to limit transparency. This lack of transparency also makes it difficult to monitor potential weaponization and arms development in space. Consequently, both nations are caught in a security dilemma—each perceives the other's space program as a potential threat, driving them to enhance their own military space capabilities in response.[63] This cycle of suspicion and competition could lead to an avoidable arms race.

To mitigate these tensions and promote stability in space exploration, it is crucial to define peaceful purposes more precisely in international space law. However, major powers like the United States, China, and Russia are unlikely to support such efforts as ambiguity benefits them to expand dual-use capabili-

ties while remaining compliant with OST. However, recognizing this challenge does not devalue the need for dialogue over reducing interpretative gaps, a necessary determinant in long-term stability. A clear definition would help foster transparency, build trust, and ensure a cooperative future for space activities, where security concerns are addressed without resorting to weaponization.

U.S.-China Stalemate on Space Arms Control

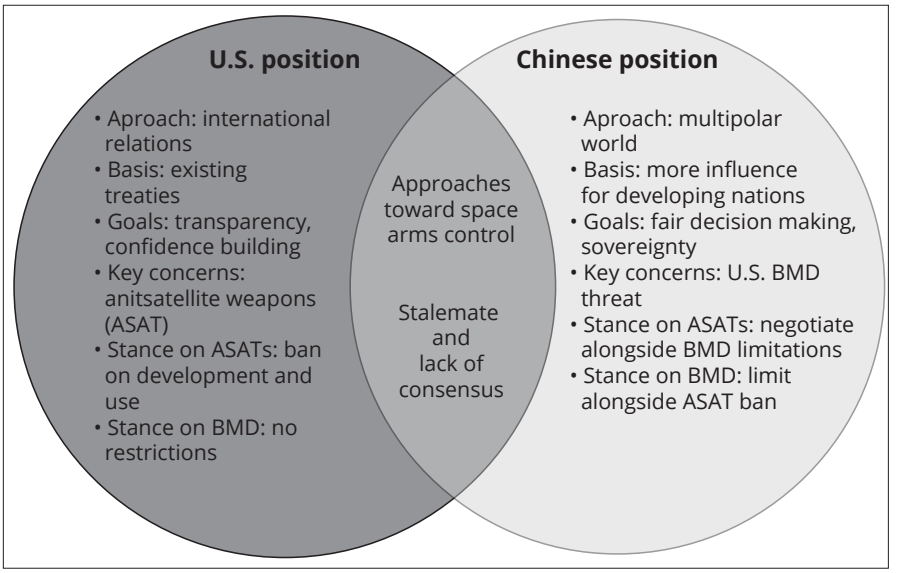
The issue of arms control in space has become contentious because of the contrasting ideas put forth by the United States and China regarding future actions beyond Earth's atmosphere, as the former favors voluntary norms and transparency measures while the latter advocates for legally binding treaties like the proposed Placement of Weapons in Outer Space Treaty (PPWT). The core of this debate stems from basic disparities in approach, with each state advocating for separate concepts and techniques in establishing the rules and norms for effective arms control and managing the arms race in space.[64] The United States advocates for a system of international regulations for controlling weapons in space, which is based on established agreements like the Outer Space Treaty.[65]

This approach highlights the significance of clear interpretations and strict adherence to the principles specified in these treaties. Its aim is to enhance transparency in space activities, thus fostering confidence and minimizing the likelihood of misunderstandings or miscalculations. A key aspect of the U.S. vision is the promotion of international norms that inhibit the creation and utilization of space weaponry. The United States considers space to be a crucial domain for global security and stability. Therefore, it aims to avoid the weaponization of space by employing diplomatic initiatives and engaging in multilateral agreements.

China supports a multipolar system, where developing spacefaring nations have more influence in decision-making processes. They perceive the U.S.-dominated system as favoring established powers to an excessive degree and aim to restore a more equitable allocation of power and influence in the governance of space.[66] This vision underpins China's promotion of the proposed Prevention of the Placement of Weapons in Outer Space Treaty (PPWT) with Russia, which upholds the principle of noninterference in national space programs. For Beijing, the PPWT represents both a counterweight to the United States' dominance and an appeal to equitable multipolar governance.[67] They oppose restrictions on their space endeavors, especially those that are seen as limiting their technological progress or national security concerns. China's stance demonstrates its intention to assert its sovereignty and autonomy in space.

Moreover, the United States perceives China's development of antisatellite capabilities as a threat to peaceful space endeavors, since it may potentially expose its satellites to vulnerability. Washington perceives a definite differen-

Figure 5. United States' and China's contrasting approaches toward space arms control



Source: courtesy of author, adapted by MCUP.

tiation between ASATs and ballistic missile defense (BMD), advocating for a prohibition on the latter while not impeding the former. China, however, perceives the U.S. emphasis on BMD as hypocritical, as it is concerned that it may potentially be used for aggressive intentions. They argue that any prohibition on ASATs should also include restrictions on sophisticated BMD systems to preserve strategic balance and stability.

The ideological conflict between the United States and China leads to a stalemate in discussions aimed at creating a comprehensive treaty that effectively addresses antisatellite weapons and BMDs effectively.[68] Both sides are adamant about not making concessions on crucial matters, as they emphasize that their positions are primarily motivated by concerns regarding national security and strategic objectives. The current deadlock presents substantial obstacles to global endeavors in monitoring and regulating space operations, intensifying conflicts, and accelerating the space arms race. The lack of substantive dialogue and collaboration between the United States and China makes it difficult to achieve consensus on crucial matters concerning space weapons control.

The Verification Dilemma

The escalating U.S.-China competition in space militarization presents strategic gains and drawbacks. While it pushes technological boundaries, it also intensifies verification challenges, complicating arms control efforts and accelerating an unregulated arms race in outer space. Verification in space is in-

herently difficult due to the unique conditions involved. Ensuring compliance with international agreements is complex, as objects in orbit are thousands of kilometers away, making it challenging to observe and analyze them accurately from ground-based sensors. High-powered telescopes provide limited insight, akin to identifying a car's function from a blurry photograph, thus complicating assessments of a satellite's purpose and capabilities.

Further complicating matters, many space technologies have dual-use potential, serving both civilian and military functions. For instance, differentiating a communication satellite from one with reconnaissance capabilities based on orbital parameters alone is challenging, contributing to the verification problem. Effective monitoring would require transparent sharing of information about space programs; however, the United States and China are reluctant to disclose such details. Concerns about compromising their technological edge or exposing vulnerabilities lead both states to withhold critical information, intensifying mutual suspicion.[69]

This secrecy fosters a worst-case-scenario mindset, fueling an unregulated arms race. China views the U.S. Space Force as a shift toward an aggressive space posture, driving China to increase its military space spending. This cyclical action-reaction dynamic sustains a high-stakes rivalry, marked by both nations preparing for potential conflict scenarios. Without a practical, trustable verification system, accurately assessing each state's space capabilities remains challenging, and the lack of transparency exacerbates tensions. Consequently, both nations engage in a high-risk strategic game, making it difficult to achieve stability in outer space.

Deterrence Challenges in Space

Space-based deterrence is seriously threatened by the United States' and China's competitiveness in space militarization. Both countries are working on building antisatellite and directed energy weaponry to be able to target each other's satellites. This leads to a more vulnerable situation: A country's ability to communicate, navigate, and gather intelligence might be severely compromised by an attack on its satellites. Fear of reprisal may not be sufficient to prevent an attack given how dependent both sides are on space infrastructure, particularly if one side thinks it can significantly outmaneuver the other by striking first. The militarization of space risks undermining nuclear deterrence by fostering first-strike incentives, where states may believe space dominance can offset the fear of nuclear reprisals.

Deterrence can be defined as influencing an adversary's cost-benefit calculations to discourage it from doing something it might otherwise choose to do.[70] In practice, deterrence seeks to convince an opponent that taking a prohibited action will result in costs, inability to succeed, or some combi-

nation of the two. One can persuade the opponent to decide against acting on the grounds that the likely consequences would exceed the likely rewards. Coercive persuasion takes the form of deterrence. The goal of deterrence tactics is to affect the actions of a voluntary agent, who has the freedom to refuse to comply with the threats or comply with them.[71] Controlling tactics are those aimed at preventing the other party from making a decision; they are not deterrent techniques.

Nuclear versus Space Deterrence

The United States' and China's space militarization efforts have fundamentally changed the dynamics of successful space deterrence, making the implementation of nuclear deterrent techniques more challenging. It is clear from studying nuclear deterrence that it is not perfect and depends on threats to sway future behavior. If the opponent chooses to disregard the threat, they have no way of knowing how much damage the foe can do or how effective their strikes would be. The opponent makes decisions based on this uncertainty. They assess the possibility of their strike succeeding against the possible costs of ignoring the threat.

Furthermore, two fundamental assumptions that ensure successful nuclear deterrence against one's opponent are credibility and potency.[72] The threat must be genuine and forceful enough to deter an attack. It also needs to be convincing enough to the opponent that it will be carried out. The promise that good behavior will not be punished comes in second. The other player must also be assured that restraint will preserve the status quo, that not attacking will result in no punishment (implicit assurance). Such assurance encourages appropriate behavior. These ideas sound reasonable and promising when applied to land, but they become very difficult when applied to space.

Through the imposition of costs and consequences on potential adversaries, space deterrence aims to dissuade hostile actions against vital space infrastructure. The context in which space-based deterrence functions is essentially different because there are no physical borders, territorial boundaries, or well-defined norms of engagement. Attacks in space might not be as globally devastating as nuclear war.[73] The threat is diminished if an attack on a single satellite is not severe enough to justify escalation to a full-scale counterattack.

Moreover, compared to nuclear war, the possible outcomes of targeting space assets are less certain. An enemy finds it more difficult to feel certain that they will not be penalized for a restricted attack because of this ambiguity. A wider variety of threats are covered by space deterrence, such as directed energy weapons, cyberattacks, electronic warfare, and ASAT weapons. Challenges brought about by these advancements include the possibility of escalating conflicts, the militarization of space, and the spread of destructive powers. The

Table 2. Differences between nuclear and space deterrence

Feature	Nuclear deterrence	Space deterrence
Environment	Earth-bound, terrestrial, and atmospheric domains	Outer space, orbital environment
Threat certainty	High—destructive capacity proven and demonstrated	Lower—uncertainty due to dual-use technologies and limited use cases
Threat credibility and potency	Extremely high—assured destruction	Ambiguous—depends on technological capability and attribution
Scope of threats	Targeting states, cities, military forces	Satellites, communication networks, global infrastructure
Defense	Missile defense limited, mostly deterrence by punishment	Hard to defend against; resilience and redundancy preferred
Limitations	Risk of mutual destruction, high political cost	Attribution problems, escalation risks, debris creation

Source: courtesy of author, adapted by MCUP.

table below shows the distinction between space-based and nuclear deterrence.

Now, this article will explore the threats that U.S–China space militarization poses to space deterrence, explain why this militarization is increasingly losing its efficacy, and discuss the need for new strategies to counter deterrence instability and escalation risks it generates.

Challenges of Punishment and Denial Deterrent Strategies

The United States and China have developed advanced space-based capabilities, including missile defense systems, ASAT technology, and jamming systems, which render traditional deterrence strategies, such as "an eye for an eye," increasingly ineffective. The United States' heavy reliance on space infrastructure for military operations, communications, and intelligence makes it particularly vulnerable, as retaliatory actions against Chinese satellites may not adequately deter attacks. U.S. losses in space would likely be more detrimental for its adversaries' deterrent strategies, further complicating deterrence as Washington might interpret such attacks as escalatory and respond forcefully.[74] In contrast, China's growing but less dependent space capabilities reduce its risk exposure, making threats of retaliation less impactful and escalation more likely.

Proportional retaliation, such as targeting China's ASAT launch facilities, risks rapid escalation. Escalating to airstrikes on urban centers would be disproportionate and could provoke broader conflict.[75] Effective deterrence requires credible threats balanced by proportionality; disproportionate actions, such as bombing cities for satellite losses, lack credibility and undermine strategic sta-

Table 3. Differences between active and passive defenses

Features	Passive defense	Active defense
Definition	Defensive measures that aim to minimize damage and exposure without engaging threats directly	Defensive measures that actively detect, respond to, and neutralize threats
Advantages	- Cost-effective in the long run - Low operational complexity - Reduces exposure to risks	- Real-time threat response - Greater adaptability - Can neutralize or deter attackers
Limitations	- Cannot eliminate threats - Static and predictable - Limited adaptability	- Expensive and resource-intensive - Risk of escalation - Requires skilled personnel
Examples	- Firewalls - Encryption - Intrusion prevention systems - Access controls	- Intrusion detection systems - Honeypots - Threat hunting - Automated response systems

Source: courtesy of author, adapted by MCUP.

bility. This creates a pressing challenge for both nations to establish an equilibrium in their evolving deterrence strategies.

Denial-based deterrence, emphasizing satellite resilience, is also fraught with challenges. Satellites' inherent exposure in space limits passive defenses like shielding, which offers modest protection and often relies on secrecy. Active defenses, such as lasers or directed energy weapons, present technical and economic constraints, including increased launch costs and limited maneuverability due to fuel constraints.[76] Keplerian mechanics and high orbital speeds (around 17,000 mph in low Earth orbit) further restrict satellites' ability to evade calculated attacks.[77] These dynamics make it difficult for deterrence strategies relying solely on maneuverability or active defenses to succeed.

Asymmetric perceptions of risk and reward complicate deterrence. China may calculate that limited strikes on key U.S. satellites could yield strategic advantages with minimal retaliation, challenging the United States to innovate deterrence strategies that address these vulnerabilities while maintaining strategic stability.

Considering these challenges, a comprehensive space defense strategy is necessary. This approach should explore various defensive solutions, including advancements in space situational awareness (SSA) to enhance detection and tracking of threats in orbit. SSA capabilities are critical in providing early warning and potentially neutralizing threats before they cause damage. A combination of enhanced SSA, innovative defensive measures, and credible and proportional deterrent strategies can help secure space assets and maintain stability.[78] By adopting such a strategy, the United States and China, as leading

space powers, can mitigate risks of escalation and preserve stability and safety in an increasingly contested domain.

OODA Loop Gap in Space

Space warfare occurs with an accelerated pace, as both China and the United States possess the capability to launch unexpected assaults on each other's satellites using kinetic ASAT weapons. Defense in this domain necessitates the efficient execution of the OODA loop—a decision-making framework comprising four critical stages: observe, orient, decide, and act.[79] This framework underscores the importance of swift and informed responses to mitigate threats, yet its application in outer space faces significant challenges.[80]

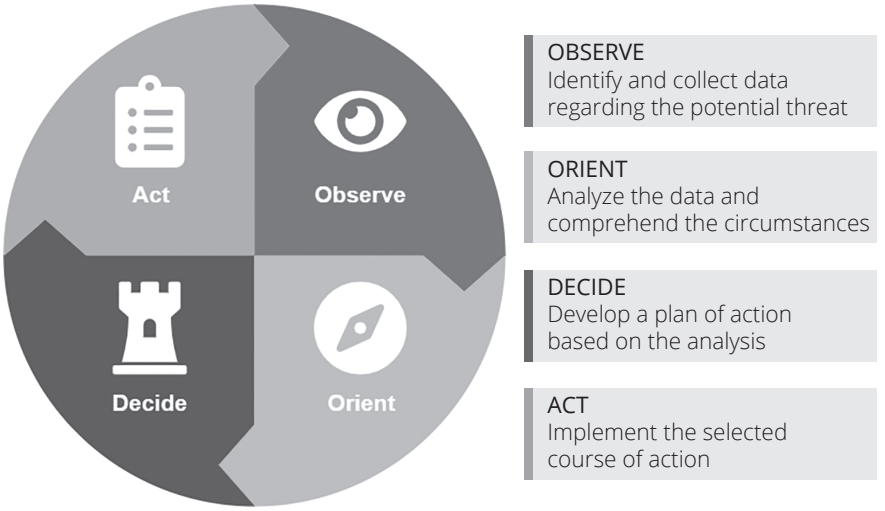
The *observe phase* involves identifying and collecting data on potential threats. In outer space, this is hindered by the difficulty of monitoring diminutive, maneuverable objects like ASAT weapons. Limited sensor coverage, particularly for high-orbit systems such as geosynchronous satellites, creates significant detection gaps. Attackers can exploit these gaps to launch undetected assaults, compromising the ability to respond effectively.[81] The *orient phase*, which requires analyzing the data to understand the nature and severity of threats, is similarly constrained by delays in data processing and limited sensor capabilities. This results in incomplete or outdated situational awareness, further complicating timely decision making.

During the *decide phase*, commanders must formulate actionable plans based on available data. However, the pace of space war and intricacies of the space environment dictates severe time limitations, usually compelling decision makers to make decisions with limited information. Even once a decision is made, the *act phase*—like maneuvering satellites or activating countermeasures—is limited by orbital mechanics, fuel restrictions, and technological lag, making timely inception problematic.

The challenges inherent in the OODA loop highlight the urgent need for advancements in sensor technology, data processing, and real-time decision-making frameworks. Without these enhancements, the vulnerabilities in each phase of the OODA loop leaves space assets exposed to operational failures and augmented susceptibility to hostile interference or accidental collisions. As technological determinism suggests, advancements in offensive space capabilities continue to outpace defensive measures, challenging existing norms and treaties like the Outer Space Treaty. The dynamics underscore the paradox of technological progress, where the pursuit of strategic advantage undermines stability.

Strategic stability—comprising crisis management, arms control, and deterrence—is increasingly strained by U.S.-China competition. The proliferation of counterspace capabilities heightens the risk of crisis escalation through

Figure 6. OODA loop of decision making and course of action



Source: adapted from Col John R. Boyd, *A Discourse on Winning and Losing*, ed. Grant T. Hammond (Maxwell, AFB: Air University Press, 1987).

miscalculations and retaliatory spirals. Unlike traditional arms races, space militarization introduces unique instability, as ASAT weapons and missile defense systems enable preemptive strikes, while attribution challenges further render deterrence ineffective. Furthermore, ambiguities surrounding the definition of peaceful purposes and verification challenges exacerbate the complexity of arms control efforts.

The stakes in this cosmic brinkmanship are immense. A single misstep could result in catastrophic conflict with global ramifications. To avert such outcomes, global cooperation is imperative. Robust arms control agreements, enhanced transparency, and prioritization of peaceful initiatives are essential to preserve strategic stability. Navigating this volatile domain with foresight and intelligence is critical to securing a sustainable and conflict-free future in outer space.

Recommendations for Space Security

The intensifying space militarization by the United States and China poses significant challenges to global strategic stability, necessitating a multifaceted and collaborative approach. Addressing these challenges requires the integration of technological advancements, the formulation of comprehensive strategies, and robust global cooperation. By adopting targeted measures, both nations can promote security, stability, and the sustainable use of outer space, ensuring that its vast potential benefits all.

The following recommendations outline critical policies and strategies to

foster peaceful coexistence in space, mitigate conflict risks, and enhance mutual security. These measures emphasize improving crisis and deterrence stability, advancing arms control mechanisms, and building a balanced framework for long-term collaboration in the space domain.

Enhance Crisis Stability through International Dialogues

- Foster regular communication channels between the United States and China to clarify intent and prevent miscalculations during crises.
- Establish bilateral and multilateral forums to discuss space security concerns, drawing precedents like the Artemis Accords and support with memorandums of understanding and agreements for real-time information exchange during emergencies.
- Encourage the use of regional platforms, such as the Asia-Pacific Regional Space Agency Forum, to address space security in localized contexts.

Promote Transparency and Space Situational Awareness (SSA)

- Develop joint SSA initiatives to improve tracking, cataloging, and monitoring of space objects, thereby reducing the risk of misinterpretation.
- Share satellite launch notifications, orbital data, and operational details to build mutual trust and reduce the likelihood of accidental escalations.
- Expand data-sharing efforts with independent experts and international organizations to enhance oversight and accountability.

Commit to Restraint in the Use of Kinetic ASAT Weapons

- Advocate for a "no-first-use" pledge by the United States and China for kinetic ASAT systems, initially between the United States and China as leading space powers, but with a goal of expanding to other states like Russia and India to prevent space debris and orbital congestion.
- Leverage diplomatic pressure and advanced nonkinetic capabilities to encourage responsible behavior and reduce reliance on destructive ASAT systems.
- Work toward a multilateral framework under United Nations supervision to establish a global ban on ASAT testing and deployment.

Define and Regulate Space Weapons

- Develop internationally accepted definitions for space weapons based on their design and intended use, focusing on their potential to cause harm in space.

Table 4. Proposed space weapons categories to make arms control efforts effective and more practical

Space weapon category	Description	Example	Regulation focus
High-threat weapons	Widespread or lasting harm	Lasers to destroy satellites, nuclear weapons	Stringent regulations or prohibitions
Weapons of moderate threat	Disable or destroy a single satellite	Electronic jammers, lower-power lasers	Restrictions on deployment or testing
Low-threat weapons	Limited effectiveness, minor disruption	Basic ASAT capabilities, short-range jammers	Transparency and notification requirements

Source: courtesy of author, adapted by MCUP.

- Categorize weapons into high-, moderate-, and low-threat levels, with high-threat weapons (e.g., destructive lasers and nuclear arms) subject to strict bans, and low-threat systems requiring transparency measures.
- Introduce protocols to regulate dual-use technologies, ensuring their peaceful application while mitigating security risks.

Strengthen Verification Mechanisms

- Design robust verification frameworks that combine satellite monitoring, open-source intelligence, and independent expert evaluations to ensure compliance with space agreements.
- Address national security concerns by introducing phased transparency agreements, beginning with nonsensitive data sharing and evolving into comprehensive verification practices.
- Explore technological solutions for real-time monitoring, such as advanced SSA systems, to provide early warnings of potential violations.

Foster Multilateral Cooperation on Space Governance

- Engage with global and regional organizations like the UN Committee on Peaceful Uses of Outer Space to address the governance gaps in space, focusing on collaborative efforts for arms control and debris management.
- Develop shared norms and protocols for peaceful space activities, including mechanisms to resolve disputes and ensure accountability like the China and Russia sponsored International Lunar Research Station that promote an alternative governance vision.
- Encourage Joint missions and projects between the United States and China to establish trust and demonstrate commitment to shared goals in space exploration and utilization.

Conclusion

The militarization of space by the United States and China reflects a complex interplay of geopolitical ambitions, technological advancements, and shifting national objectives. Initially spurred by Cold War tensions and perceived Soviet threats, the United States established space dominance, investing heavily in military space technologies. China, driven by military, prestige, and economic factors, has since emerged as a formidable space power, challenging U.S. supremacy. This U.S.-China rivalry now extends beyond exploration, focusing on control over strategic space resources and the military advantages space offers.

Technological determinism and the security dilemma illustrate this competition's impact on strategic stability, as advancements fuel mutual suspicion. Space is perceived as a zero-sum game, where the line between defensive and offensive capabilities is blurred, fostering a cycle of militarization. This escalation threatens the three pillars of stability—crisis management, arms control, and deterrence. The deployment of ASAT weapons and missile defense systems risks crisis escalation and undermines deterrence, as space-based weapons enable potentially destructive, preemptive strikes. The lack of clarity on peaceful purposes and challenges in verifying space activities further complicate arms control efforts. This rivalry thus disrupts the balance of power, increasing the likelihood of miscalculation and unintended conflict, ultimately threatening peace in the space domain.

Last, the hypothesis that the militarization of space by the United States and China is likely to disturb strategic stability is strongly reinforced by the creation of a feedback loop characterized by suspicion and discontent. Technological progress (technological determinism) serves as the catalyst for military space programs, leading one nation to view the other's accomplishments as a potential security threat, resulting in a security dilemma, which can then create a Thucydides' Trap situation, particularly with the United States' focus on maintaining supremacy over China in all domains. This perpetuates a cycle of distrust and heightened allocation of funds toward military endeavors in space.

The stakes could not be higher. A single misstep in this celestial game of brinkmanship could result in a catastrophic conflict with substantial and far-reaching consequences. To avert such a dismal result, a comprehensive, cooperative framework becomes essential to manage the risks of conflict, maintain crisis stability, and ensure responsible use of this vital domain. The suggested approaches—enhanced global dialogues, a no-first-use commitment, a multi-stakeholder space arms control regime, and a phased approach to transparency—form the pillars of a sustainable path forward. By focusing on transparency, space situational awareness, and the creation of internationally agreed definitions and regulations, the United States and China can lead the way in establishing norms that benefit all spacefaring nations.

A multilateral framework, underpinned by open-source intelligence and collaborative information-sharing platforms, could foster mutual understanding, mitigate misperceptions, and reduce the potential for miscalculations in space. Commitment to these measures by the United States, China, and other stakeholders would not only help prevent a costly and dangerous space arms race but also serve as a model for international cooperation. Such a commitment would ensure that space remains a domain of shared prosperity, setting a precedent for stability, security, and collaborative innovation in this new frontier by avoiding the risks of a Thucydides' Trap of continued escalation of the two preeminent space powers.

Endnotes

1. Curtis Peebles, *High Frontier: The US Air Force and the Military Space Program* (Washington, DC: Air Force History and Museums Program, 2020), 2–5.
2. *2023 Annual Report* (Colorado Springs, CO: Space Foundation, 2023).
3. Helena Fortea Colomé, "The Militarization of Outer Space: An Analysis of the Current International Dynamics at Play" (master's thesis, University of Barcelona, September 2020).
4. Quoted in Colomé, "The Militarization of Outer Space."
5. Bleddyn E. Bowen, *War in Space: Strategy, Space Power, Geopolitics* (Scotland: Edinburgh University Press, 2020).
6. Directed-energy ASAT tests imply the deployment of powerful lasers or microwave systems intended to dazzle, blind, or interfere with satellites' sensors and electronics without physical contact. Most of these tests are conducted from ground or airborne platforms. An oft-quoted incident is China's 2006 ground-based laser test mentioned by U.S. defense officials, which aimed to illuminate and potentially blind U.S. imaging satellites. *Co-orbital* ASAT tests entail the deployment of a satellite that moves in proximity to some other space object to examine, disrupt, or even disable the latter. Although such systems are capable of civilian uses (e.g., servicing satellites or removing space junk), they also convey the capability of being offensive counterspace tools. The most evident example is that of Russia's Kosmos-2543 in 2020 performing proximity maneuvers interpreted by U.S. Space Command as a co-orbital ASAT trial. James Clay Moltz, "The Changing Dynamics of Twenty-First-Century Space Power," *Journal of Strategic Security* 12, no. 1 (2019): 15–43, https://doi.org/10.5038/1944-0472.12.1.1729.
7. Moltz, "The Changing Dynamics of Twenty-First-Century Space Power."
8. Ulrich Kuhn, "Strategic Stability in the 21st Century: An Introduction," *Journal for Peace and Nuclear Disarmament* 6, no. 1 (2023): 34–56, https://doi.org/10.1080/25751654.2023.2223804.
9. Pericles Gasparini Alves, *Prevention of an Arms Race in Outer Space: A Guide to the Discussions in the Conference on Disarmament* (New York: United Nations Institute for Disarmament Research, 1991); and Curtis Peebles, *High Frontier: The U.S. Air Force and the Military Space Program* (Washington, DC: Air Force Historical Studies Office, 1997).
10. Michael Brown, Eric Chewning, and Pavneet Singh, *Preparing the United States for the Superpower Marathon with China* (Washington, DC: Brookings, 2020), 12–32.
11. Bleddyn E. Bowen, *Original Sin: Power, Technology and War in Outer Space* (Oxford, UK: Oxford University Press, 2023).
12. Dean Cheng, "Chinese Concepts of Space Security," in *Handbook of Space Security: Policies, Applications and Programs*, ed. Kai-Uwe Schrogl et al. (Berlin: Springer, 2014), 431–51.

13. Fortea, "The Militarization of Outer Space," 3–37.
14. *Case Study: Viasat* (Geneva, Switzerland: CyberPeace Institute, 2022).
15. Shannon Bugos, "China Tested Hypersonic Capability, U.S. Says," Arms Control Association, 1 November 2021; and Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (1966), United Nations Office for Outer Space Affairs, accessed 24 September 2025.
16. Richard P. Hallion, *The Hypersonic Revolution: Case Studies in the History of Hypersonic Technology*, vol. 1, *From Max Valier to Project Prime (1924–1967)* (Washington, DC: Air Force History and Museums Division, 1998).
17. Ahmad Khan and Sufian Ullah, "Challenges to International Space Governance," in *Handbook of Space Security*, 35–48.
18. Bowen, *Original Sin*, 199–257.
19. For more information on track 2 diplomacy, see Jennifer Staats, Johnny Walsh, and Rosarie Tucci, "A Primer on Multi-track Diplomacy: How Does It Work?," U.S. Institute of Peace, 31 July 2019. "Track 2 diplomacy brings together unofficial representatives on both sides, with no government participation. Neither track 1.5 nor track 2 discussions carry the official weight of traditional diplomacy, as they are not government-to-government meetings. What they offer is a private, open environment for individuals to build trust, hold conversations that their official counterparts sometimes cannot or will not, and discuss solutions."
20. Claire Mills, *The Militarisation of Space* (London: House of Commons Library, 2021).
21. Ulrich Kuhn, "Strategic Stability in the 21st Century: An Introduction," *Journal for Peace and Nuclear Disarmament* 6, no. 1 (2023): https://doi.org/10.1080/25751654.2023.2223804.
22. James Clay Moltz, "The Changing Dynamics of 21st Century Space Power," *Journal of Strategic Security* 12, no. 1 (2019): https://doi.org/10.5038/1944-0472.12.1.1729.
23. White House, "Text of Space Policy Directive-4: Establishment of the United States Space Force," presidential memoranda, 19 February 2019. This memorandum set in motion the creation of the U.S. Space Force. See also "History," Space Force, accessed 24 September 2025. "The U.S. Space Force was established Dec[ember] 20, 2019 when the National Defense Authorization Act was signed into law."
24. Kevin McCauley, "Putting Precision in Operations: BeiDou Satellite Navigation System," *China Brief* 14, no. 16 (2014).
25. Kuhn, "Strategic Stability in 21st Century."
26. Gregory D. Koblentz, *Strategic Stability in the Second Nuclear Age*, Council Special Report no. 71 (New York: Council on Foreign Relations, 2014), 6–19.
27. Bruce W. MacDonald et al., *Crisis Stability in Space: China and Other Challenges* (Washington, DC: Foreign Policy Institute, Johns Hopkins University, 2022), 37–69.
28. Thomas C. Schelling, "The Strategy of Conflict Prospects for a Reorientation of Game Theory," *Journal of Conflict Resolution* 2, no. 3 (September 1958), https://doi.org/10.1177/002200275800200301; and John J. Klein, *Understanding Space Strategy: The Art of War in Space* (New York: Routledge, 2019), 69–96.
29. MacDonald et al., *Crisis Stability in Space*, 37–69.
30. Robin Dickey, *The Rise and Fall of Space Sanctuary in U.S. Policy* (Arlington, VA: Center for Space Policy and Strategy, 2020).
31. "Long-term Sustainability of Outer Space Activities," United Nations Office for Outer Space Affairs, accessed 12 April 2024; and "Fact Sheet: Vice President Harris Advances National Security Norms in Space," White House, 18 April 2022.
32. Theresa Hitchens, "Norm Setting and Transparency and Confidence-Building in Space Governance," in *War and Peace in Outer Space*, ed. Cassandra Steer and Matthew Hersch (Oxford, UK: Oxford University Press, 2021), 55–90, https://doi.org/10.1093/oso/9780197548684.003.0003.
33. Paul Meyer, "Restraining an Arms Race in Outer Space," *Survival* 64, no. 2 (2022): 81–94, https://doi.org/10.1080/00396338.2022.2055825.

34. Paul Szymanski, "Techniques for Great Power Space War," *Strategic Studies Quarterly* 13, no. 4 (Winter 2019): 78–86.
35. Nivedita Raju, "Developments in Space Security," in *SIPRI Yearbook 2022* (Stockholm: SIPRI, 2021).
36. Monika U. Ehrman, "Property, Sovereignty, and Customary Governance in Outer Space Resource Extraction," *Georgia Law Review* no. 57 (2023): 1769–88.
37. Roger Handberg, "Is Space War Imminent?: Exploring the Possibility," *Comparative Strategy* 36, no. 5 (2017): 413–25, https://doi.org/10.1080/01495933.2017.1379832.
38. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (1966), United Nations Office for Outer Space Affairs, accessed 24 September 2025.
39. Alexandra Stickings, "The Normalisation of Anti-Satellite Capabilities," *Air and Space Power Review* 22, no. 2 (2023): 33–44, https://doi.org/10.1080/01495933.2017.1379832.
40. Shirley Kan, *China's Anti-Satellite Weapon Test* (Washington, DC: Congressional Research Service, 2007).
41. Eric Hagt, "The U.S. Satellite Shootdown: China's Response," *Bulletin of the Atomic Scientists*, 5 March 2008.
42. Chris O'Meara, "Anti-Satellite Weapons and Self-Defence: Law and Limitations" (presentation at CyCon 2024: Over the Horizon, 16th International Conference on Cyber Conflict, Tallinn, Estonia, 28–31 May 2024), 250–64.
43. Donald J. Kessler et al., *The Kessler Syndrome: Implications for Future Space Operations* (San Diego, CA: American Astronomical Society, 2010).
44. Michelle Starr, "Experts Watch in Horror as 2 Dead Satellites Are on Track for a Potential Collision," *Science Alert*, 15 October 2020.
45. Vipin Narang and Scott D. Sagan, eds., *The Fragile Balance of Terror: Deterrence in the New Nuclear Age* (Ithaca, NY: Cornell University Press, 2023).
46. Leonard David, "New Image of China's Secret Space Plane Shows Delta-wing Design," Space.com, 24 September 2024.
47. Jishe Fan, "Managing China–U.S. 'Strategic Competition': Potential Risks and Possible Approaches," *China International Strategy Review* no. 3 (2021): 234–47, https://doi.org/10.1007/s42533-021-00091-x.
48. Jeffrey A. Bader, "Avoiding a New Cold War between the U.S. and China," Brookings, 17 August 2020.
49. Minghao Zhao, "Is a New Cold War Inevitable?: Chinese Perspectives on U.S.–China Strategic Competition," *Chinese Journal of International Politics* 12, no. 3 (2019): 371–94, https://doi.org/10.1093/cjip/poz010.
50. Julie Dahlitz, "Arms Control in Outer Space," *World Today* 38, no. 4 (April 2019): 154–60.
51. Graham Allison, *Destined for War: Can America and China Escape Thucydides's Trap?* (Boston, MA: Houghton Mifflin Harcourt, 2017).
52. Bruce W. MacDonald, Carla P. Freeman, and Alison McFarland, *China and Strategic Instability in Space: Pathways to Peace in an Era of US-China Strategic Competition* (Washington, DC: U.S. Institute of Peace, 2023).
53. The *collective-action dilemma* arises when individuals or states would all benefit from cooperating to achieve a common good, but each has an incentive to free ride—enjoying the benefits without contributing to the costs. In this case, both Washington and Beijing depend on satellites for communications, navigation, and intelligence. Limiting jamming or cyberattacks would make space safer for both, yet neither side is willing to give up these counterspace tools first, fearing the other might gain a strategic edge.
54. Alves, *Prevention of an Arms Race in Outer Space*, 36–46.
55. Todd Harrison et al., *Escalation and Deterrence in the Second Space Age* (Washington, DC: Center for Strategic and International Studies, 2017), 10–34.
56. Alton Frye, *Space Arms Control: Trends, Concepts, Prospects* (Santa Monica, CA: Rand Corporation, 1964).

57. Convention on Registration of Objects Launched into Outer Space, United Nations Office for Outer Space Affairs, 15 September 1976.
58. Christophe Bonnal, Jean-Marc Ruault, and Marie-Christine Desjean, "Active Debris Removal: Recent Progress and Current Trends," *Acta Astronautica* 85 (2013): 51–60, https://doi.org/10.1016/j.actaastro.2012.11.009.
59. Gershon Hasin, "From 'Space Law' to 'Space Governance': A Policy-Oriented Perspective on International Law and Outer Space Activities," *Harvard International Law Journal* 64, no. 2 (Spring 2023): 392–407.
60. Jessica West and Lauren Vyse, *Arms Control in Outer Space: Status and Timeline* (Waterloo, ON: Project Ploughshares, 2022), 4–23.
61. Kiran Krishnan Nair, "The Principal of Peaceful Uses of Outer Space: Reviewing the Scope of '*Peaceful*' in the Changing Context," in *Small Satellites and Sustainable Development-Solutions in International Space Law* (Cham, Switzerland: Springer, 2019), 7–26.
62. Nair, "The Principal of Peaceful Uses of Outer Space," 7–26.
63. Nair, "The Principal of Peaceful Uses of Outer Space," 7–26.
64. Jinyuan Su, "Legal Challenges of Arms Control in Outer Space," in *War and Peace in Outer Space: Law, Policy, and Ethics,* ed. Cassandra Steer and Matthew Hersch (New York: Oxford Academic, 2020).
65. *Defense Space Strategy Summary* (Washington, DC: Department of Defense, June 2022).
66. He Qisong, "Space Arms Control or Space Behavior Control?: The Competition between American and Chinese Ideas of an International Space Order," *Pacific Focus* 38, no. 1 (2023): 26–51, https://doi.org/10.1111/pafo.12221.
67. Hans Kundnani, *What Is the Liberal International Order?*, Liberal International Order Project no. 17 (Washington, DC: German Marshall Fund of the United States, 2017).
68. Jinyuan Su, "Legal Challenges of Arms Control in Outer Space."
69. Frye, "Space Arms Control," 1–22.
70. Lawrence Freedman, *Deterrence* (Cambridge, UK: Polity Press, 2004), 11–26.
71. Col Jeffrey W. Pickler, "Modern Deterrence: 21st Century Warfare Requires 21st Century Deterrence," *Security Insights* 1, no. 2 (2022): 21–35.
72. Stephen J. Flanagan et al., *A Framework of Deterrence in Space Operations* (Santa Monica, CA: Rand Corporation, 2023), 10–28, https://doi.org/10.7249/RRA820-1.
73. Mark Galeotti, *The Weaponization of Everything: A Field Guide to the New Way of War* (New Haven, CT: Yale University Press, 2022), 45–56.
74. Fan, "Managing China–U.S. 'Strategic Competition'," 234–47.
75. Karen Ruth Adams, "Attack and Conquer?: International Anarchy and the Offense-Defense Deterrence Balance," *International Security* 28, no. 3 (Winter 2003/2004): 45–83, https://doi.org/10.1162/016228803773100075.
76. Todd Harrison et al., *Space Threat Assessment 2020* (Washington, DC: Center for Strategic and International Studies, 2020), 54–70.
77. Harrison et al., *Space Threat Assessment 2020*.
78. Mackenzie Enholm, "The Security Dilemma and Conflict in Space: Impossible or Inevitable?," *Journal of Strategic Security* 17, no. 4 (2023): 48–68, https://doi.org/10.5038/1944-0472.17.4.2255.
79. Jonathan Lowe, "How Not to Lose First Dog Fight in Space," Ansys, 24 July 2019.
80. Lowe, "How Not to Lose First Dog Fight in Space."
81. Brad Townsend, "Strategic Choice and the Orbital Security Dilemma," *Strategic Studies Quarterly* 14, no. 1 (Spring 2020): 73–92.

Conscientious Centaurs
Lethal Autonomous Weapons Systems, Human-Machine Teaming, and Moral Enmeshment

Lieutenant Commander Jonathan Alexander, USN

Abstract: In modern warfare, lethal autonomous weapons systems (LAWS) introduce artificial intelligence–enabled capabilities that may execute lethal actions without final human judgment. Their development envisions human-machine teams (HMT) that combine machine precision with human situational awareness in what has been termed "centaur warfighting." Although some argue that autonomous weapons will shield personnel from the psychological burdens of combat, others contend that such systems risk morally distancing human operators from lethal outcomes. This article instead examines how humans may become "enmeshed" with machines within HMT sociotechnical structures, producing new forms of moral exposure and potentially contributing to morally injurious experiences at the tactical level.

Keywords: autonomous weapons, human-machine team, HMT, centaur warfighting, moral injury, moral enmeshment, moral luck

Introduction[1]

In the history of war, technology has been discovered, designed, and deployed to increasingly distance combatants from their enemy. In today's modern warfare, the development and likely future deployment of lethal autonomous weapons systems (LAWS) represents a potentially new era, as artificial intelligence (AI)-enabled weapons may make lethal decisions apart from the final

LtCdr Jonathan Alexander is an active-duty U.S. Navy chaplain currently serving at the Naval Chaplaincy School in Newport, RI. Prior to the Navy, he served in the U.S. Army as an infantry officer. He holds a doctor of philosophy in humanities and philosophy of technology from Salve Regina University, and his dissertation research was on lethal autonomous weapons systems and the potential of moral injury. His research interests are in the areas of ethics and emerging technologies, especially as it relates to what it means to be human in an age of advanced technology. https://orcid.org/0009-0008-4301-1961.

Journal of Advanced Military Studies vol. 16, no. 2
Fall 2025
www.usmcu.edu/mcupress
https://doi.org/10.21140/mcuj.20251602003

judgment and input of human warfighters. Paul Scharre argues in *Army of None* that "technology has brought us to a crucial threshold in humanity's relationship with war. In future wars, machines may *make life-and-death engagement decisions on their own*."[2] The state of military affairs is currently in the middle of this "crucial threshold" as illustrated by defense-related news sources regularly publishing stories on the current development of autonomous systems and real-time militarized emerging technologies innovation and experimentation in the Russo-Ukrainian War.[3] Numerous factors contribute to the "relentless drive toward autonomy"—the nation's decreased appetite for physical risk to military personnel; lower costs per unit of unmanned autonomous systems; a militarized emerging technologies arms race with peer and near-peer adversaries; the need for hardened systems in cyber-contested wartime environments; and the ever-increasing speed of algorithmic warfare that may not permit humans to stay meaningfully engaged in the kill chain.[4]

Current LAWS development does not envision armies of lethal autonomous robots flying, marching, and sailing through the battlespace independent of all collaborative human partnership and control. Some of the sensationalized rhetoric around LAWS makes this seem the case, but most of the literature and future operational concepts embrace human-machine teaming (HMT).[5] Within this hybridized sociotechnical system of the HMT, the relationship between the human and machine has been metaphorically and cleverly depicted as "centaur warfighting."[6] The mythological centaur is a creature with a human head and upper body and a horse's lower body. Paul Scharre leverages this image to describe the unique advantages that humans and machines both provide: "The best systems will combine human and machine intelligence to create hybrid cognitive architectures that leverage the advantages of each. Hybrid human-machine cognition can leverage the precision and reliability of automation, without sacrificing the robustness and flexibility of human intelligence."[7] As LAWS are currently developed and likely deployed in the future, a crucial question emerges—in the "centaur" HMT relationship, how might the machine's autonomous lethal actions morally and psychologically impact the human warfighter as the end user at the tactical level of war?

While there has been significant scholarship on the ethical, moral, and legal dimensions of LAWS, to date, there has been sparse research and discussion on the potential moral and psychic effects on those who will employ such weapon systems. The limited literature that does exist predominately suggests that the deployment of LAWS in place of human combatants will either minimize war-related traumas like post-traumatic stress disorder and moral injury or LAWS will morally displace, distance, or desensitize servicemembers from the consequences of the lethal robot's autonomous actions.[8] However, as this article argues, the deployment of LAWS serving as a prophylactic against the hu-

man experience of wartime moral and psychic distress or contributing to moral displacement, distancing, and desensitization may not be the case, as some philosophies of technology and studies on anthropomorphizing in human-robot relationships theorize how the human may become enmeshed and entangled with the machine in the sociotechnical architecture of the HMT. This enmeshment may very well extend to the moral effects and consequences caused by autonomous weapons, especially if laws of war (LOW), namely the *jus in bello* principles of discrimination and proportionality, are violated.[9] With the possibility of enmeshment and entanglement, if a lethal machine violates LOW, this could create a potentially morally injurious experience for the human warfighter. When it comes to the possibility of moral enmeshment in the hybridized relationship between the human and machine, perhaps Scharre's description of HMT as centaur warfighting is more prescient than his clever metaphorical use intends.

The structure of the article is as follows. It begins with brief overviews of both LAWS and moral injury and is followed by a theoretical exploration of how the human combatant in a sociotechnical HMT may become morally enmeshed with the machine and ultimately feel a sense of moral responsibility for the machine's autonomous actions. The term *theoretical exploration* is not used to avoid rigorous scholarship or deflect any burden of proof. In the same way that engineers study potential shortcomings or failures in structures yet to be built, the methodology of this exploration is the application of established philosophical and psychological theorems. The investigation of technological and relational enmeshment occurs via: (1) an analysis of Bruno Latour's philosophy of technology and his idea of the "collective"; (2) research on warfighters relationally anthropomorphizing the robots they team with in combat; and (3) an application of the philosophical concept of moral luck.[10] The article concludes with recommended areas for future research so that militarized HMT can be *conscientious centaurs*.

As emerging technologies are increasingly integrated into the future military context, illustrated by the Department of Defense's (DOD) Replicator Initiative and the North Atlantic Treaty Organization's (NATO) Allied Command Transformation, it is vital for civilian and military leadership—policy makers, defense planners, technologists, and commanders alike—to recognize critical inflection points and reflect on the human dimension of autonomous warfare.[11] This not only incorporates considerations on how to wage war justly (*jus in bello*) but also includes intentional efforts to provide "the moral and psychological armor needed to preserve honor and perhaps even humanity during and after war."[12] This type of multifaceted reflection can foster an even greater freedom for servicemembers to fulfill the mission and fight in good conscience because they will trust that ethical and moral issues have been considered by

their leaders in the design, development, and deployment of the technologies at their disposal. Warfighters and their families deserve nothing less.

Lethal Autonomous Weapon Systems

While space constraints limit a thorough discussion on LAWS and other conceptual issues (e.g., continuums of autonomy and lethality; technical components and concepts; ethical, moral, and legal concerns), a brief overview and definition of LAWS is useful.[13] *Department of Defense Directive (DODD) 3000.09, Autonomy in Weapon Systems* defines LAWS as

> *a weapon system that, once activated, can select and engage targets without further intervention by an 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.[14]

Additionally, it is worth quoting in full the DOD's definition of autonomy, contrasted with automation, in the *2018 Unmanned Systems Integrated Roadmap, 2017–2042*:

> Autonomy is defined as the ability of an entity to independently develop and select among different courses of action to achieve goals based on the entity's knowledge and understanding of the world, itself, and the situation. Autonomous systems are governed by broad rules that allow the system to deviate from the baseline. This is in contrast to automated systems, which are governed by prescriptive rules that allow for no deviations. While early robots generally only exhibited automated capabilities, advances in AI and ML [machine learning] technology allow systems with greater levels of autonomous capabilities to be developed. The future of unmanned systems will stretch across the broad spectrum of autonomy, from remote controlled and automated systems to near fully autonomous, as needed to support the mission.[15]

LAWS are also often described by the place of the human operator "in/on/out of" the observe, orient, decide, act kill chain loop (a.k.a. John R. Boyd's OODA loop).[16] "In" the loop refers to the operator deciding what the robotic system does at every stage from target acquisition to engagement. "In" the loop is sometimes also referred to as semiautonomous weapons that "only engage individual targets or specific target groups that have been selected by a human operator."[17] "On" the loop means that the system will carry out most of its functions without a human operator, but the human may intervene at any time. "Out of" the loop (sometimes called "off the loop") is a fully autonomous

system where the machine carries out each action of OODA. *DODD 3000.09* currently directs humans to stay in or on the loop, but it leaves room for future LAWS development and deployment.

In operational concepts of future HMT, the human warfighter and LAWS may team together on the physical battlefield or be separated in the battlespace but connected via high-definition sensors and screens. As an example of the former, one operational scenario might have an infantry squad employing an autonomous ground robot acting as the "point man," minimizing risk to human combatants in the event of initial contact with the enemy. A physically distanced scenario might look like an operator launching a lethal autonomous drone swarm from another continent yet still witnessing kinetic effects via sensors and screens.

Moral Injury

Moral injury (MI) is the "damage done to one's conscience or moral compass when that person perpetrates, witnesses, or fails to prevent acts that transgress one's own moral beliefs, values, or ethical codes of conduct."[18] Brett T. Litz et al.'s seminal article describes MI as "perpetrating, failing to prevent, bearing witness to, or learning about acts that transgress deeply held moral beliefs and expectations."[19] Jonathan Shay defines MI as "a betrayal of what's right by someone who holds legitimate authority in a high stakes situation."[20] In veteran war reporter David Wood's *What Have We Done: The Moral Injury of Our Longest Wars*, he conducts interviews with combat veterans, mental health clinicians, and military chaplains and develops an insightful experiential explanation of moral injury:

> Moral injury is a jagged disconnect from our understanding of who we are and what we and others ought to do and ought not to do. Experiences that are common in war . . . challenge and often shatter our understanding of the world as a good place where good things should happen to us, the foundational beliefs we learn as infants. The broader loss of trust, loss of faith, loss of innocence, can have enduring psychological, spiritual, social, and behavioral impact.[21]

Signs and symptoms of MI include: (1) inappropriate guilt and shame; (2) social or relational issues (e.g., avoiding intimacy, anger and aggression, reduced trust in other people and cultural contracts); (3) spiritual and existential problems (e.g., loss of spirituality or weakened religious faith, negative attributions toward God or higher power, lack of forgiveness, crisis in meaning); (4) substance abuse and other attempts at self-handicapping; and (5) suicide and other self-harm behaviors.[22]

Moral injury is typically viewed as a phenomenon distinct from post-

traumatic stress disorder (PTSD). When Shay, serving as a psychiatrist for the U.S. Department of Veterans Affairs Boston Outpatient Clinic, began to study Vietnam veterans' combat experiences, he did not see PTSD as an adequate explanation of the psychic trauma experienced by those he counseled. Thus, he coined the term *moral injury*. In his 2014 journal article "Moral Injury" in *Psychoanalytic Psychology*, he reflects:

> The DSM [*Diagnostic and Statistics Manual of Mental Disorders*] diagnosis, Posttraumatic Stress Disorder (PTSD), does not capture either form of moral injury [i.e., Shay's own betrayal-focused or Litz et al.'s perpetrator-focused MI]. PTSD nicely describes the persistence into life after mortal danger of the valid adaptations to the real situation of other people trying to kill you. However, pure PTSD, as officially defined, with no complications, such as substance abuse or danger seeking, is rarely what wrecks veterans' lives, crushes them to suicide, or promotes domestic and/or criminal violence. Moral injury—both flavors—does.[23]

Clinical researchers Sonya B. Norman and Shira Maguen note overlapping symptomology of PTSD and MI—guilt, shame, betrayal, and loss of trust. They also highlight nosological differences, especially PTSD's fear-based reactions, hyperarousal, startle response, memory loss, and flashbacks, and MI's sorrow, regret, shame, and alienation.[24] Research and scholarship related to understanding and treating moral injury, including perspectives from both clinical and humanities disciplines, has proliferated in the past two decades because, as Wood observes, MI is "the signature wound of this generation of [Global War on Terrorism] veterans."[25]

Human Machine Teaming and Moral Enmeshment

War as a Moral Arena

War is a moral arena. Article 15 of Francis Lieber's 1863 *Instructions for the Government of Armies of the United States in the Field* (a.k.a. the Lieber Code or General Orders No. 100 by President Abraham Lincoln) states: "Men who take up arms against one another in public war do not cease on this account to be moral beings, responsible to one another and to God."[26] Psychotherapist Edward Tick also reflects on the moral nature of war:

> During warfare, we human beings take over the Divine functions of granting life or administering death and of determining the destinies of peoples and nations. . . . Taking life is the essence of war and is also in essence *a moral and spiritual act* . . . . Precisely because we become arbiters of life, death, and fate, we enter religious and spiritual dimensions and are in a

> world of ultimate matters that Karl Marlantes calls "this wartime sacred space, this Temple of Mars."[27]

This "moral and spiritual act" in the arena of war is why warfighters may experience MI if they "perpetrate, witness, or fail to prevent acts that transgress one's own moral beliefs, values, or ethical codes of conduct."[28] While this article argues that moral enmeshment between the human and machine may be possible in the HMT, and therefore the use of LAWS may potentially contribute to moral injury in the warfighters who deploy them at the tactical level of war, as noted above, the opposite is often suggested—the introduction of LAWS may reduce occurrences of MI. For instance, while Scharre does not necessarily espouse the future use of LAWS, he writes, "In a world where autonomous weapons bore the burden of killing, fewer soldiers would presumably suffer from moral injury. There would be less suffering overall. From a purely utilitarian consequentialist perspective, that would be better."[29] His brief mention of MI comes at the end of a lengthier section on death by LAWS' potential violation of human dignity, yet Scharre never entertains how servicemembers who believe this to be the case (e.g., LAWS violating human dignity) may themselves be morally injured by deploying said weapons. Massimiliano L. Cappuccio, Jai Galliott, and Fady Alnajjar also contend that deploying LAWS in the place of humans will minimize war-related traumas like MI and is, therefore, ethically imperative.[30] Like Scharre, the authors do not illustrate ways in which moral enmeshment may occur between human and machine, nor do they evaluate how LAWS may potentially contribute to moral injury in those who deploy them. These perspectives assume there will be little to no moral connection or moral responsibility between the future LAWS operator and the autonomous robot under their command. In essence, they imply that lethal autonomous technology removes the human combatant from the moral arena of war. Scharre notes, "If we lean on algorithms as a moral crutch, it weakens us as moral agents. . . . Someone should bear the moral burden of war. If we handed that responsibility to machines, what sort of people would we be?"[31] Again, this presumes that LAWS operators will be removed from the moral arena of war and not feel a sense of moral responsibility or moral burden for the lethal decisions autonomous robots make while under their tactical authority.

Bruno Latour's "Collective"

Philosophies of technology theorize and provide insight into how a future operator and LAWS may possibly become morally enmeshed within a human-machine, sociotechnical system, and therefore, how the LAWS operator may experience the moral responsibility and burden for the lethal actions of the autonomous machine, thereby potentially contributing to MI. In French philos-

opher and sociologist Bruno Latour's 1999 essay "A Collective of Humans and Nonhumans: Following Daedalus's Labyrinth," he presents the concept of the "collective—defined as an exchange of human and nonhuman properties inside a corporate body."[32] His concept eschews modernity's strict subject-object dualism and explains how human actors and nonhuman actants are collectively "entangled" in the process and pursuit of a goal. The subject-object duality treats the human as subject and the nonhuman artifact as object, but Latour avers that this distinction in practice does not hold. When describing the "technical mediation" relationship(s) between humans and nonhumans, a "third agent emerges from the *fusion* of the other two."[33] To illustrate, Latour uses the example of a chimpanzee wielding a stick to knock down a banana from a tree. In this scene, how does one identify subject and object? Modernity's dualism views the chimpanzee as the subject instrumentalizing the stick as object to accomplish the goal of knocking down the banana (another object). However, Latour proposes that hybridization and enmeshment occurs when the chimpanzee as actor partners with the stick as actant, and this entanglement of chimpanzee and stick comprises a new "collective" to accomplish the goal—"The chimp plus the sharp stick reach (not reaches) the banana."[34] Notice the syntax of "reach" versus "reaches." Latour's approach employs third-person plural as the chimp plus the stick *collectively* reach. In his construct, the "imbroglios of humans and nonhumans on an ever-increasing scale" occur because of "successive crossovers through which humans and nonhumans have exchanged their properties" in a "deepened *intimacy*, a more intricate mesh, between the two."[35]

How might Latour's theory of the "collective" illuminate the potential of moral enmeshment between the human and machine in a militarized HMT, thereby offering an explanation as to how the LAWS operator remains in the moral arena of war and personally experiences the moral weight of the machine's lethal action? In a traditional dualistic dichotomy, the operator is the subject, and the LAWS is the object. Operator and LAWS are ontologically distinct. However, in Latour's view of enmeshment, operator and LAWS are sociotechnically fused and entangled in pursuit of the goal of engaging a target. In military practice, this is intimated and illustrated by a Marine and a rifle as articulated in the "Marine's Rifle Creed"—"This is my rifle. There are many like it, but this one is mine. My rifle is my best friend. It is my life. I must master it as I master my life. My rifle, without me, is useless. Without my rifle, I am useless. . . . *We will become part of each other*."[36] While the latter phrase is included as an implied symbolic, and not ontological, union between the Marine and the rifle, according to Latour's idea of the collective, there might be more going on that actually creates some kind of ontological, or at least psychological, union or enmeshment. With this sense of oneness between actor (the Marine) and actant (the rifle), the human Marine has moral agency and therefore takes moral

responsibility and feels the moral burden for the outcomes of this hybridized entanglement. When the bullet (another subactant in the sociotechnical imbroglio) is fired from the weapon and strikes another human being, the Marine as human actor feels a sense of moral agency, moral responsibility, and moral burden. The Marine as actor does not dichotomize and disengage from the rifle as actant when dealing with the effects of the rifle's actions because operating together in a collective, they *are* one enmeshed system.

There may be a similar human-machine collective teaming with the future operator and LAWS. One might take issue with this comparison, claiming that with the rifle, the Marine as human actor is involved in every stage of the OODA loop, and the moral component of lethal action is in the ultimate decision to act. However, once the rifle's firing pin strikes the primer, the bullet is now an "uncontrollable" actant, at least in the sense that the Marine cannot *definitively* control where it strikes (e.g., accuracy of the shot, another individual stepping in the way or being in close proximity of the intended target, minute differences in bullet manufacturing, wind conditions, etc.). Yet, through the "oneness" of the Marine-rifle system, the Marine still retains moral agency as well as moral responsibility and the weight of moral burden.

To expand the exploration of moral responsibility residing beyond just the individual's ultimate decision to lethally act, one could also apply this concept to a Marine infantry company commander deploying Marines. Even though discipline has been instilled through rigorous training, the individual Marine, once deployed, is essentially autonomous and uncontrollable by the commander. Yet, the commander still retains a morally weighted "command responsibility" and experiences a moral burden for what those under their command "autonomously" choose to do.[37] If an individual Marine violates LOW, the commander still feels a sense of moral responsibility, experiences the moral burden, and may even in some cases be held legally accountable for the actions of the individual "autonomous" Marine. This moral weight is illuminated by Latour's collective—the commander has been morally enmeshed with the individual Marine (yet another hybridized actor/actant system).

Caroline Holmqvist, senior lecturer in war studies at the Swedish National Defence College, similarly conceptualizes potential enmeshment and entanglement in militarized technologies in her article "Undoing War: War Ontologies and the Materiality of Drone Warfare." She labels the HMT as a "complex human-material assemblage" noting that virtual war is still "humanly experienced," contra the argument that it is game-like:

> Contrary to common perception, drone warfare is "real" also for those staring at the screen and, as such, the reference to video games is often simplistic. . . . The relationship between the fleshy body of the drone operator and the steely body of the drone and its ever-more sophisticat-

> ed optical systems needs to be conceptualized in a way that allows for such paradoxes to be made intelligible.[38]

Holmqvist uses similar language to Latour regarding the potential enmeshment of human and machine in contemporary warfare, explaining that "the human experience is continually altered by human beings' encounters with technology . . . and to understand the human being in war, we need to consider the way in which fleshy and steely bodies *associate, interact, merge—the dissolution between the corporeal and the incorporeal*."[39]

While Latour's idea of the collective does not present an unassailable argument for the moral responsibility and burden of the individual operator who deploys an autonomous system, it does provide philosophical and technological insight into why and how the human in the HMT may feel and experience a sense of moral distress for the lethal effects of the autonomous weapon under their control, even when the human is not specifically the element of the HMT acting in the OODA kill chain loop. Counterintuitively, it could also be that the removal of the human operator's authority and decision to act in a lethal scenario causes moral stress. As Jai Galliott suggests, "If increasingly autonomous systems limit the exercise of autonomy or exert undue power and control over an operator's ability to oversee the execution of lethal action in a just manner or that which accords with one's own values systems and that of their military organization, they may be 'morally injured'."[40] Latour's theory that technologies potentially diminish the modern notion of subject-object distinction supports the exploratory thesis that human moral agency is not deferred or disengaged with the employment of LAWS but instead becomes a complex phenomenon of moral entanglement via this enmeshed, hybridized relationship between human and machine in the militarized HMT.

Anthropomorphism in Militarized Human Machine Teaming

A form of this HMT relational enmeshment and entanglement is documented in warfighters who anthropomorphize the robots they team with in combat. Cappuccio, Galliott, and Eduardo Sandoval cite numerous research studies in human-robot interaction regarding anthropomorphism—the human tendency to perceive various kinds of nonhuman agents, including machines, as human-like. The authors observe:

> Explosive Ordnance Disposal (EOD) operators deployed in Iraq and Afghanistan report at least four remarkable anecdotes about their relationships with the robots that assisted them in carrying out their task in active war scenarios . . . which testify to the pervasiveness of anthropomorphism:

1. EOD robots were assigned names and gendered identities by the soldiers who worked with them in Iraq and Afghanistan;
2. at times, when one of these robots was damaged, its loss was not simply experienced as the destruction of an expensive piece of equipment, but also *grieved* like the death of a teammate, and in some cases, it was accompanied by funeral-like rituals;
3. when one of these robots was sent to the headquarters for repair after suffering structural damage, its human mates requested that its mechanical parts were not replaced, but accurately fixed to preserve the robot's individual identity;
4. in rare occasions, soldiers have endangered themselves to protect the robot from enemy assaults. . . .

> Therefore, anthropomorphistic attributions can be fueled by empathy and narratives of sacrifice, which reinforce each [other's] . . . effects: thus, if robots are portrayed as entities that "sacrifice" themselves, then their destruction feels like a "death," which in turn reinforces the empathic perception of them as person-like entities.[41]

Julie Carpenter similarly researches the sociotechnical relationship between EOD personnel and the robots they use to locate improvised explosive devices. She writes:

> From the armed forces projected standpoint, the robot stands in for the EOD [human] operator as a critical doppelganger or *extension of their physical self*. . . . From the results of research on Human-Robot Interaction, the case is made that EOD personnel may form pseudo-relationships with robots and attribute mental states and sociality to them. The human instinct to anthropomorphize non-living things may be amplified and exploited by the addition of humanlike characteristics in robots, as well as people engaging in prolonged proximity and interactive situations with them.[42]

Victoria Groom et al.'s insightful paper "I Am My Robot: The Impact of Robot-Building and Robot Form on Operations" presents the idea of human self-extension into objects such as robots:

> When interacting with autonomous robots or robots tele-operated by another person, people respond in much the same way they respond to other people. In contrast, teleoperation and other immersive interactions through robots enable interactions between humans and robots that, in the moment of using the robot, *may make people feel like the robot is part of one's self*.[43]

The ideas of collective, assemblage, anthropomorphization, and self-extension may seem initially disparate, but explored together, they support the concept of a deeper sociotechnical relationship in the HMT. In the context of the human operator and LAWS, this hybridized and enmeshed social relationship may explain how a "moral" connection is created between the two, especially if the robot is viewed anthropomorphically as a teammate or as an extension of the human operator. Therefore, taking into consideration these philosophies of technology and theories of social robotics, one can hypothesize how the moral implications of a lethal robot, especially in cases of LOW violations, may be felt and carried by the human operator, thus contributing to potentially morally injurious experiences for warfighters functioning in HMT. Again, the use of a centaur to describe the human-robot relationship in HMT is perhaps more accurate than initially intended.

Moral Luck

In addition to philosophies of technology and psychological theories on HMT, the philosophical concept of moral luck provides further insight as to how the LAWS operator may indeed be more deeply connected and "enmeshed" in the moral arena and effects of war even as autonomous lethal decisions are executed beyond the operator's direct control. Dana K. Nelkin provides a description of moral luck:

> Moral luck occurs when an agent can be correctly treated as an object of moral judgment despite the fact that a significant aspect of what she is assessed for *depends on factors beyond her control*. . . . The problem of moral luck arises because we seem to be committed to the general principle that we are morally assessable only to the extent that what we are assessed for depends on factors under our control (call this the "Control Principle"). At the same time, when it comes to countless particular cases, we morally assess agents for things that depend on factors not in their control [i.e., luck].[44]

Moral philosopher Bernard Williams's classic example of a truck driver, who "*through no fault of his own*," runs over a child who darted in front of the moving vehicle, offers a helpful analogical parallel to the operator whose LAWS executes a lethal algorithmic action violating LOW.[45] In Williams's case, the driver is not "at fault" due to the agency of the child, but nonetheless, the driver should feel a sense of remorse and regret. One might even suggest that something would be morally amiss with the driver if they did *not* feel some sense of moral remorse or regret. Therefore, the driver feels and experiences the moral weight of an action outside of their direct control. David Sussman further explains this seemingly irrational but very real and understandable moral no-

tion: "We expect the truck driver to be strongly inclined to blame himself, even though it would be wrong for the rest of us to feel anything like resentment or indignation toward him. . . . Although the driver should ultimately be 'let off the hook,' he nevertheless should not so release himself, but instead put up real resistance to our attempts to exonerate him."[46] Sussman continues, "Regret often brings with it some kind of self-reproach. . . . We can rationally feel regret for events that are completely and obviously beyond our influence. We need to see that even when there is no culpability, there can still be inescapable forms of personal antagonism that, although innocent, can nevertheless involve many of the features of personal wrongdoing."[47]

A more contemporary moral luck thought experiment might include the use of a self-driving car. Although the environment differs significantly, the moral dynamics of delegation to civilian autonomous systems can illuminate similar tensions in militarized applications. Imagine someone owning a self-driving car and riding as a passenger when the vehicle hits and kills a pedestrian. The vehicle's owner and operator, even when riding as a passenger in self-driving mode, will likely feel a sense of moral responsibility and regret even though the car made an algorithmically programmed, autonomous decision resulting in the fatality. From Williams's "unfortunate" (i.e., bad luck) truck driver example and the self-driving vehicle thoughts experiment, one can easily identify the analogous parallel. The concept of moral luck and feeling of moral responsibility for an outcome shaped by factors beyond one's control serve to demonstrate how the human operator in the HMT may experience the moral weight, regret, and potential self-reproach for an autonomous lethal decision made outside of their control.

War as a Moral Arena (Reprise)

When one surveys the literature on LAWS, authors frequently employ the descriptor "moral." For example, when discussing HMT, Scharre frequently describes humans as "moral beings" and "moral agents" with "moral responsibility."[48] Others echo this use—James L. Boggess's "personal moral code," Mark Coeckelbergh's "moral responsibility," Anthony C. Pfaff's "moral assessment," and Gary E. Marchant et al.'s "moral judgment."[49] If "moral" is used so pervasively in the literature when describing the moral weight and burden humans must retain in war, then why would every warfighter who deploys future LAWS completely and permanently disengage morally when using these type of weapons, even if robotic warfare technology potentially contributes to different classes of moral displacement? More importantly, if the technology does indeed morally displace, distance, or desensitize servicemembers in real time from the kinetic results of the moral arena of war, one cannot assume that they will not at some point in the future evaluate and reflect on their wartime service. Tick writes:

> A unique dimension of modern war *with as yet unknown impact* is that with modern technology, people take lives on the other side of the world but are not in danger of being killed in return. . . . Many troops engaged in distant forms of military action often feel detached from the experience of killing, their victims, and their own status as combat veterans. They may not rehumanize the foe or reconcile with their own histories until long after their service, if at all.[50]

Tick notes that the psychospiritual impact of modern technology is *unknown*, yet also states that distanced warfare may contribute to moral disengagement. However, what is also undetermined, as Tick suggests, is whether the distanced warfighter will or will not morally reflect on their wartime actions. Later in his volume, he further intimates, "Today, warfare has become more deadly, debilitating, and invisible than ever. . . . We can surmise that the greater the destructive reach of our weaponry, *the greater the moral stress and burden on troops and the nation, and the more penetrating yet mysterious the invisible wound will be*."[51] These citations are not highlighted to call Tick to task for proffering seemingly opposing statements regarding the potential moral impact of using militarized emerging technologies. They merely reveal the *unknown* and *mysterious* moral and psychic distress that may result in the warfighter who deploys LAWS due to potential moral enmeshment.

Understanding and further exploring the potential of moral enmeshment may serve as a protective factor for those who will one day deploy LAWS. If the current narrative continues that LAWS will either (1) shield human combatants from the traumas of war or (2) create a context of systematic killing that is construed as dehumanizing, desensitized, and dispassionate with few moral or psychic consequences on the commander or operator, then the military will not be ready for the potential moral distress and harm that results from the use of autonomous weapons in future war. While not all will emerge morally injured, some will—and this number matters.

Conclusion and Recommendations

The aim of this article has been to explore how the human may become enmeshed with the machine in the sociotechnical architecture and hybridized relationship of the HMT. This enmeshment may extend to the moral effects and consequences caused by LAWS, thus contributing to morally injurious experiences for the human warfighter at the tactical level of war, especially if LOW principles of discrimination and proportionality are violated. Using the doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTmLPF-P) framework, below are three recommenda-

tions and areas of research that should be pursued in future studies of LAWS and the potential of moral harm on operators.[52]

The first recommendation involves personnel and policy such as multidisciplinary inflection points in DOD LAWS development and deployment policy. In this author's opinion, to date, the DOD has satisfactorily addressed ethical, moral, and legal issues concerning LAWS and other militarized AI-enabled systems.[53] Dialogue has included military leadership, policy makers, academics, private industry leaders, ethicists, technologists, and engineers. Because military chaplains often focus directly on servicemembers and serve as vanguards in treating psychospiritual injuries, they and other behavioral health care providers with expertise in moral injury should be incorporated into this discussion. The DOD must continue to prioritize and value regular inflection points and pauses in policy development for ethical, moral, and legal considerations before, during, and after the deployment of LAWS. If the nation desires ethical and morally fit warfighters, institutional processes of ideation, development, acquisition, deployment, and evaluation of emerging technologies must model this ethical and moral integrity.

The second area of focus or recommendation is to pursue leadership and education remedies by conducting further research on LAWS and potential psychic and moral harm. The only data and anecdotal information currently existing on militarized emerging technologies and moral distress derives from research on remotely piloted aircraft (RPA, i.e., drone) crews. It is vital to understand how future LAWS might affect the psychospiritual health of warfighters. While some may see this discussion as premature, analogical models such as studies on RPA crews can be leveraged to discern potential adverse results. This does not necessitate slowing or suspending development or deployment of LAWS, but the conversation must continue regarding holistic care of servicemembers. Retired Army psychologist Dave Grossman's proposition of physically distanced weapons reducing innate resistance to killing applies to conventional weapons (e.g., artillery, naval gunfire, bombers, etc.), but RPA with high-definition sensors and screens minimize this distance psychologically via "empathic bridging" and "distant intimacy."[54] M. Shane Riza shares the comments of a former wing commander at Creech Air Force Base in Nevada where a majority of RPA operations are flown, who explained that "it's not really 8,000 miles away, it's 18 inches away. We're closer . . . than we've ever been as a service. There's no detachment. Those employing the system are very involved at a personal level in combat."[55]

Research reveals RPA crews experiencing PTSD and MI at similar, and in some studies higher, rates as compared to conventional manned fighter aircraft. Jean L. Otto and Bryant J. Webber state, "There was no significant difference

in the rates of [mental health] MH diagnoses, including post-traumatic stress disorder, depressive disorders, and anxiety disorders between RPA and [manned aircraft] MA pilots. Military policymakers and clinicians should recognize that RPA and MA pilots have similar MH risk profiles."[56] They also noted the additional challenges of RPA crews could "increase susceptibility to PTSD." Rajiv K. Saini, V. K. Raju, and Amit Chali cite a "variety of studies conducted on drone crews[, which] have consistently provided [a] higher incidence of psychiatric symptoms than their compatriots who operate manned aircraft."[57] Joseph O. Chapa believes that the psychological risks to RPA crews may be higher than the psychological risk to other combatants due to the empathic bridging with the targets they are tracking.[58]

While RPA warfare maintains a human in each aspect of the kill chain, the lessons learned, especially regarding psychological, moral, and spiritual care of technologically distanced operators, will be helpful in developing preventative and responsive care best practices for future LAWS operators. Among branches of the U.S. military, the Air Force currently executes the most RPA missions and has unit-embedded mental health providers and chaplains. Their best practices for crew care modalities may provide a good foundation for practices of care for those who one day deploy LAWS.

The third recommendation is to integrate robust ethics and moral decision-making education and training for military leaders and warfighters as end users. Even though LAWS will make final lethal decisions, their use on the battlefield will require more, not less, moral decision-making education and training for military personnel. In Christian Brose's *The Kill Chain*, he observes:

> As intelligent machines become capable of performing these kinds of technical tasks more effectively than humans can, allowing them to do so *can liberate more members of the military to do work of greater ethical value*. They can spend more of their days solving complex problems with other people, making operational and strategic decisions, contextualizing critical information, distinguishing between right and wrong, and commanding people and machines to perform critical missions. These are the kinds of jobs that Americans actually join the military to do. In this way, *intelligent machines could enable more human beings to concentrate on the ethics of warfare than ever before*.[59]

If this is the case, it will require robust moral instruction, which can occur through focused ethics education and training in basic, intermediate, and advanced schools for officers and enlisted alike, especially as the Services train robotics and unmanned systems military occupation specialties (e.g., the Navy's robotics warfare specialist enlisted rating and the Marine Corps' 73XX Unmanned Aircraft System [UAS] Occupational Fields). Additional instruction

and application may include ethical dilemmas with AI-enabled decision systems woven into training exercises, as well as regular ethical and moral decision-making discussions conducted at the unit level. As the military Services embrace and employ more emerging technologies and correspondingly expect "human beings to concentrate on the ethics of war," warfighters must be trained to think ethically and act morally sound.

The late Isaac Asimov once said, "The saddest aspect of life right now is that science gathers knowledge faster than society gathers wisdom."[60] While this has traditionally been the case, the next chapter of history begins now. As LAWS are likely deployed in the not-so-distant future and the character of war continues to evolve, the citizenry has a moral and social obligation to holistically care for the warfighters who fight the nation's wars. Among other things, this includes sincere reflection on the potential morally injurious effects caused by the weaponized emerging technologies placed in their hands. As the American Civil War General William Tecumseh Sherman once lamented, "War is hell," but it is, and always will be, a moral realm. However, when warfighters see this level of concern for their holistic health from the society that sends them to war, it bolsters their confidence in the cause and empowers them to fight with honor in emerging warfare as "conscientious centaurs"—as those who have considered the moral dynamics and weight of employing autonomous weapons in HMT. Not only is this an obligation, but this is also wisdom.

Endnotes

1. Portions of this article are taken from the author's PhD dissertation. For additional material in a broader context, see Jonathan Alexander, "Lethal Autonomous Weapon Systems and the Potential of Moral Injury" (PhD diss., Salve Regina University, Newport, RI, 2024). Additionally, all research on LAWS originates from open-source, unclassified references.
2. Paul Scharre, *Army of None: Autonomous Weapons and the Future of War* (New York: W. W. Norton, 2018), 4. Emphasis added.
3. For a recent analysis of militarized technologies being deployed in the Russo-Ukrainian War, see Neil Renic and Johan Christensen, *Drones, the Russo-Ukrainian War, and the Future of Armed Conflict* (Copenhagen, Denmark: Djof Publishing and the Centre for Military Studies, 2024); and August Cole et al., *Artificial Intelligence in Military Planning and Operations: Ethical Considerations*, PRIO Paper (Oslo, Norway: Peace Research Institute Oslo, 2024).
4. George R. Lucas Jr. is credited with the phrase "relentless drive toward autonomy." See George R. Lucas Jr., "Engineering, Ethics, and Industry: The Moral Challenge of Lethal Autonomy," in *Killing by Remote Control: The Ethics of an Unmanned Military*, ed. Bradley J. Strawser (New York: Oxford University Press, 2013), 211, http://dx.doi.org/10.1093/acprof:oso/9780199926121.003.0010.
5. Although science fictionalized characterizations of militarized emerging technologies (e.g., *Terminator, 2001: A Space Odyssey, iRobot*) can provide creative visualizations of the potential dystopian downsides of AI and LAWS, the still-future and often implausible orientation and sensationalism harnessed by advocates of a preemptive ban are not constructive in furthering a calm, reasoned, and systematic approach in evaluating

the ethics, morality, and legality of LAWS. Noel Sharkey, a pro-ban on LAWS advocate, provides a good example of this reasoned approach, "It is important to clarify what is meant by 'robot autonomy' here. This is often confused with science fiction notions of robots with minds of their own with the potential to turn on humanity. The reality is very different. The autonomous robots being discussed for military applications are closer in operation to your washing machine than to a science fiction *Terminator*." Noel Sharkey, "Saying 'No!' to Lethal Autonomous Targeting," *Journal of Military Ethics* 9, no. 4 (2010): 376, https://doi.org/10.1080/15027570.2010.37903.

6. Paul Scharre, "Centaur Warfighting: The False Choice of Humans vs. Automation," *Temple International & Comparative Law Journal* 30, no. 1 (March 2016): 164. Robert Sparrow and Adam Henschke take the metaphor a step further, proposing that the future of human-machine teaming is more likely to be expressed with "teams of humans under the control, supervision, and command of artificial intelligence." Robert J. Sparrow and Adam Henschke, "Minotaurs, Not Centaurs: The Future of Manned-Unmanned Teaming," *Parameters* 53, no. 1 (2023): 115, https://doi.org/10.55540/0031-1723.3207.
7. Scharre, "Centaur Warfighting," 152.
8. One exception to the above perspectives is Jai Galliott, "The Soldier's Tolerance for Autonomous Systems," *Paladyn, Journal of Behavioral Robotics* no. 9 (2018): 131–32, https://doi.org/10.1515/pjbr-2018-0008, where he discusses how LAWS' removal of the human operator's decision to use lethal force may contribute to moral distress.
9. For a concise summary of *jus in bello* principles, see "Jus ad bellum and jus in bello," International Committee of the Red Cross, accessed 16 September 2025.
10. Bruno Latour, "A Collective of Humans and Nonhumans: Following Daedalus's Labyrinth," in *Pandora's Hope: Essays on the Reality of Science Studies* (Cambridge, MA: Harvard University Press, 1999).
11. Jim Garamone, "Hicks Discusses Replicator Initiative," DOD Manufacturing Technology Program, 7 September 2023; and "Allied Command Transformation," North Atlantic Treaty Organization, 24 September 2024. At the time of the original writing, the name change from Department of Defense to Department of War had not yet been made.
12. Christopher Toner, "Military Service as a Practice: Integrating the Sword and Shield Approaches to Military Ethics," *Journal of Military Ethics* 5, no. 3 (November 2006): 184–85, https://doi.org/10.1080/15027570600911993.
13. For one of the most accessible volumes discussing these issues, see Scharre, *Army of None*. See also Kenneth Payne, *I, Warbot: The Dawn of Artificially Intelligent Conflict* (New York: Oxford University Press, 2021). Emphasis added.
14. *Department of Defense Directive 3000.09, Autonomy in Weapon Systems* (Washington, DC: Department of Defense, 25 January 2023), 21.
15. *Unmanned Systems Integrated Roadmap, 2017–2042* (Washington, DC: Office of the Assistant Secretary of Defense for Acquisition, Department of Defense, 2018).
16. Col John R. Boyd, U.S. Air Force fighter pilot and strategist, began developing the OODA concept in the 1950s to describe the process of reacting to a stimulus. In combat, the adversary with the shortest OODA loop has the advantage. Current dynamic targeting methodology (the kill chain) is referred to as find, fix, track, target, engage, assess (F2T2EA) by air and naval forces and decide, detect, deliver, assess (D3A) by land component forces. With F2T2EA, LAWS's lethal use of force would take place at engage and for D3A at deliver. Within special operations, find, fix, finish, exploit, analyze, disseminate (F3EAD) is used, with finish being the point of lethal action. For simplicity, OODA is used in this article. See *Joint Fire Support*, Joint Publication 3-09 (Washington, DC: Department of Defense, 2019), xii; and Jimmy A. Gomez, "The Targeting Process: D3A and F3EAD," *Small Wars Journal*, 16 July 2011.
17. Kelley M. Sayler, *Defense Primer: U.S. Policy on Lethal Autonomous Weapon Systems*, In Focus (Washington, DC: Congressional Research Service, 2025).
18. "What Is Moral Injury?," Moral Injury Project, Syracuse University, accessed 22 November 2021.

19. Brett T. Litz et al., "Moral Injury and Moral Repair in War Veterans: A Preliminary Model and Intervention Strategy," *Clinical Psychology Review* 29, no. 8 (December 2009): 699, https://doi.org/10.1016/j.cpr.2009.07.003.
20. Jonathan Shay, "Moral Injury," *Psychoanalytic Psychology* 31, no. 2 (April 2014): 183, https://doi.apa.org/doi/10.1037/a0036090.
21. David Wood, *What Have We Done: The Moral Injury of Our Longest Wars* (New York: Little, Brown, 2016), 8.
22. Jacob K. Farnsworth et al., "The Role of Moral Emotions in Military Trauma: Implications for the Study and Treatment of Moral Injury," *Review of General Psychology* 18, no. 4 (December 2014): 249–62, https://dx.doi.org/10.1037/gpr0000018.
23. Shay, "Moral Injury," 184.
24. Sonya B. Norman and Shira Maguen, "Moral Injury," *PTSD Quarterly* 33, no. 1 (2022).
25. David Wood, "The Grunts: Damned If They Kill, Damned If They Don't," *Huffington Post*, 18 March 2014.
26. *Instructions for the Government of Armies of the United States in the Field* (Lieber Code) (Washington, DC: Adjutant General's Office, 1863).
27. Edward Tick, *Warrior's Return: Restoring the Soul After War* (Boulder, CO: Sounds True, 2014), 74–75. Emphasis added. Karl Marlantes, Vietnam War veteran, emphasizes that warriors must wage war morally with justice. Evoking the Greek god of war Ares (or Mars in the Roman pantheon), he writes, "The connection between the war God and God of justice is evident in the hill in the midst of Athens called the Areopagus, the hill of Ares. The Areopagus is where the Athenians had their principal Court of Justice. Judges were called *areopagitae*." Karl Marlantes, *What It Is Like to Go to War* (New York: Atlantic Monthly Press, 2012), 251.
28. "The Moral Injury Project."
29. Scharre, *Army of None*, 290.
30. Massimiliano Lorenzo Cappuccio, Jai Christian Galliott, and Fady Shibata Alnajjar, "A Taste of Armageddon: A Virtue Ethics Perspective on Autonomous Weapons and Moral Injury," *Journal of Military Ethics* 21, no. 1 (2022): 10, https://doi.org/10.1080/15027570.2022.2063103.
31. Scharre, *Army of None*, 290.
32. Latour, "A Collective of Humans and Nonhumans," 193.
33. Latour, "A Collective of Humans and Nonhumans," 178. Latour additionally explains four relational meanings and facets of the technical mediation between humans and nonhumans: (1) goal translation; (2) composition; (3) reversible blackboxing; and (4) delegation. He describes the following example of the chimpanzee, stick, and banana relationship and "system" as "composition." Latour, "A Collective of Humans and Nonhumans," 182. Emphasis added.
34. Latour, "A Collective of Humans and Nonhumans," 182
35. Latour, "A Collective of Humans and Nonhumans," 201, 196.
36. "Marine's Rifle Creed," Marine Corps University, accessed 18 February 2023. Emphasis added.
37. While *command responsibility* is technically used as a legal term in LOW, there is an implicit moral responsibility of the commander within the definition, and the moral burden is being emphasized here. See James M. Dubik, "Human Rights, Command Responsibility, and Walzer's Just War Theory," *Philosophy and Public Affairs* 11, no. 4 (Autumn 1982): 354–71. Dubik remarks, "Command responsibility . . . [is] moral responsibility" (p. 355). For further discussion of command responsibility and inherent moral responsibility, see also James M. Dubik, "Social Expectations, Moral Obligations, and Command Responsibility," *International Journal of Applied Philosophy* 2, no. 1 (Spring 1984): 39–48, https://doi.org/10.5840/ijap1984212.
38. Caroline Holmqvist, "Undoing War: War Ontologies and the Materiality of Drone Warfare," *Millennium: Journal of International Studies* 41, no. 3 (2013): 541–42, https://doi.org/10.1177/0305829813483350.
39. Holmqvist, "Undoing War," 548. Emphasis added.

40. Galliott, "The Soldier's Tolerance for Autonomous Systems," 131.
41. Massimiliano L. Cappuccio, Jai Galliott, and Eduardo B. Sandoval, "Saving Private Robot: Risks and Advantages of Anthropomorphism in Agent-Soldier Teams," *International Journal of Social Robotics* 14, no. 2 (2021): 2140, https://doi.org/10.1007/s12369-021-00755-z. Peter Singer shares a similar story about an explosive ordnance disposal team's "emotional connection" with their robot in Iraq that was destroyed while disarming an improvised explosive device. See Peter W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (New York: Penguin Press, 2009), 19–21.
42. Julie Carpenter, "Just Doesn't Look Right: Exploring the Impact of Humanoid Robot Integration into Explosive Ordnance Disposal Teams," in *Handbook of Research on Technoself: Identity in a Technological Society*, ed. Rocci Luppicini (Hershey, PA: IGI Global, 2013), 621, 623–24, https://doi.org/10.4018/978-1-4666-2211-1.ch032. Emphasis added.
43. Victoria Groom et al., "I Am My Robot: The Impact of Robot-building and Robot Form on Operations" (paper presented at the 4th ACM/IEEE International Conference on Human Robot Interaction, La Jolla, CA, 11–13 March 2009), https://doi.org/10.1145/1514095.1514104. Emphasis added.
44. Dana K. Nelkin, "Moral Luck," Stanford Encyclopedia of Philosophy, 20 January 2025. Emphasis added.
45. Bernard Williams, "Moral Luck," in *Moral Luck: Philosophical Papers, 1973–1980* (Cambridge, UK: Cambridge University Press, 1981), 28, https://doi.org/10.1017/CBO9781139165860.003. Emphasis added.
46. David Sussman, "Is Agent-Regret Rational?," *Ethics* 128, no. 4 (July 2018): 791, https://doi.org/10.1086/697492.
47. Sussman, "Is Agent-Regret Rational?," 793, 802.
48. Scharre, *Army of None*, 290 (moral beings), 294 (moral responsibility), 322 (moral agents).
49. James L. Boggess, "More Than a Game: Decision Support Systems and Moral Injury," in Samuel R. White, *Closer Than You Think: The Implications of the Third Offset Strategy for the U.S. Army* (Carlisle, PA: U.S. Army War College, 2017), 3; Mark Coeckelbergh, "Drones, Information Technology, and Distance: Mapping the Moral Epistemology of Remote Fighting," *Ethics and Information Technology* 15, no. 2 (June 2013): 88, https://doi.org/10.1007/s10676-013-9313-6; C. Anthony Pfaff, "The Ethics of Acquiring Disruptive Military Technologies," *Texas National Security Review* 3, no. 1 (Winter 2019/2020): 44; and Gary E. Marchant et al., "International Governance of Autonomous Military Robots," *Science and Technology Law Review* no. 12 (2011): 296, https://doi.org/10.7916/D8TB1HDW.
50. Tick, *Warrior's Return*, 83. Emphasis added.
51. Tick, *Warrior's Return*, 102. Emphasis added
52. DOTmLPF-P is part of the DOD's Joint Capabilities Integration and Development System. See *Manual for the Operation of the Joint Capabilities Integration and Development System* (Washington, DC: Department of Defense, 2021).
53. For example, see *Department of Defense Directive 3000.09*, 21; "DOD Adopts Ethical Principles for Artificial Intelligence," Department of Defense, 24 February 2020; and *U.S. Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway* (Washington, DC: Department of Defense, 2022).
54. See LtCol Dave Grossman, *On Killing: The Psychological Cost of Learning to Kill in War and Society*, rev. ed. (New York: Back Bay Books, 2009), 13. Grossman writes, "There is within most men an intense resistance to killing their fellow man. A resistance so strong that, in many circumstances, soldiers on the battlefield will die before they can overcome it" (p. 4); and LtCol Wayne Phelps, *On Kill Remotely: The Psychology of Killing with Drones* (New York: Little, Brown, 2021), 63.
55. M. Shane Riza, *Killing without Heart: Limits on Robotic Warfare in an Age of Persistent Conflict* (Washington, DC: Potomac Books, 2013), 263.
56. Jean L. Otto and Bryant J. Webber, "Mental Health Diagnoses and Counseling Among

Pilots of Remotely Piloted Aircraft in the United States Air Force," *Medical Surveillance Monthly Report* 20, no. 3 (March 2013): 2.

57. Rajiv K. Saini, V. K. Raju, and Amit Chali, "Cry in the Sky: Psychological Impact on Drone Operators," *Industrial Psychiatric Journal* 30, no. 1 (2021): 17, https://10.4103/0972-6748.328782.
58. Joseph O. Chapa, "Remotely Piloted Aircraft, Risk, and Killing as Sacrifice: The Cost of Remote Warfare," *Journal of Military Ethics* 16, nos. 3–4 (2017): 263, https://doi.org/10.1080/15027570.2018.1440501. See also Seth Davin Norrholm et al., "Remote Warfare with Intimate Consequences: Psychological Stress in Service Member and Veteran Remotely-Piloted Aircraft (RPA) Personnel," *Journal of Mental Health and Clinical Psychology* no. 7 (2023): 37–49, https://doi.org/10.29245/2578-2959/2023/3.1289.
59. Christian Brose, *The Kill Chain: Defending America in the Future of High-Tech Warfare* (New York: Hachette Books, 2020), 126. Emphasis added.
60. Isaac Asimov, *Isaac Asimov's Book of Science and Nature Quotations*, ed. Isaac Asimov and Jason A. Shulman (New York: Weidenfeld & Nicolson, 1988), 281.

The Lawful Losers?
Why Democracies Struggle to Deter Cyber Aggression

Paul A. Eisenmann

Abstract: Democratic states are increasingly vulnerable in cyberspace due to inherent ethical constraints, transparency requirements, and legal oversight, significantly hindering their ability to effectively deter cyber aggression. This article critically assesses the strategic disadvantages democracies face using the examples of the United States, the United Kingdom, and Germany, including attribution challenges, threshold ambiguities, and the problematic diffusion of cyber capabilities among state and nonstate actors. It evaluates how strict adherence to international humanitarian law (IHL) further constrains democratic responses, contrasting sharply with the operational flexibility enjoyed by authoritarian adversaries. The article advocates strengthening cyber resilience, promoting global norm-building initiatives, and crucially retaining credible traditional military retaliation options. This integrated strategy enables democracies to uphold their values, effectively counter cyber threats, and actively shape global cyber norms, thereby ensuring strategic stability and digital security.
Keywords: cyber deterrence, democratic constraints, attribution, international humanitarian law, cyber norms, kinetic retaliation, cybersecurity resilience

The Tension between Cyber Deterrence and Democratic Values

As cyberspace increasingly becomes a domain of strategic competition, democracies confront unique and formidable challenges in deterring cyber aggression. Unlike conventional warfare, cyber operations blur

Paul A. Eisenmann is a PhD student serving as a junior officer in the German cyber command. He holds a master's in cyber security from the University of Portsmouth and a bachelor in history from the Open University in the United Kingdom. The views expressed in this article are solely those of the author and do not necessarily reflect the official position of the Kommando Cyber-und Informationsraum, the Bundeswehr, the German Federal Ministry of Defence, or the government of the Federal Republic of Germany. https://orcid.org/0009-0005-8474-3454.
Journal of Advanced Military Studies vol. 16, no. 2
Fall 2025
www.usmcu.edu/mcupress
https://doi.org/10.21140/mcuj.20251602004

the traditional boundaries of attribution, thresholds, and proportionality, leaving states uncertain about appropriate responses and vulnerable to miscalculations.[1] Democracies, bound by transparency, ethical accountability, and legal oversight, find themselves particularly disadvantaged compared to authoritarian states that can exploit these ambiguities without equivalent constraints. Consequently, democracies struggle to establish credible deterrence, often resorting to defensive postures or limited diplomatic sanctions that adversaries view as insufficient or negligible.

This article critically explores why democracies face these struggles and proposes actionable strategies to overcome inherent disadvantages. It investigates how ambiguities surrounding attribution and thresholds complicate deterrent measures, the structural inequalities in cyber capabilities between democratic and authoritarian states, and the problematic diffusion of cyber capabilities among state and nonstate actors. Furthermore, the article examines how strict adherence to IHL and ethical norms, while essential for democratic legitimacy, significantly constrains effective responses to cyber threats.

This article adopts a focused comparative analysis of three liberal democracies—the United States, the United Kingdom, and Germany—as illustrative cases of advanced cyber powers operating under distinct legal and constitutional constraints. These states were selected because they combine significant cyber capabilities, global security roles, and formal commitments to international humanitarian law, yet embody differing constitutional structures and strategic cultures. The United States operates with a strong executive and globally expansive cyber posture; the United Kingdom integrates cyber capabilities into joint operations under a parliamentary system with limited legislative oversight; Germany, constrained by the *Grundgesetz* (Basic Law), maintains a resolutely defensive stance under strict parliamentary control.[2] Examining this variation within a small set of capable democracies allows for sharper identification of how attribution burdens, threshold ambiguity, and IHL obligations interact to shape deterrence outcomes. The aim is to generate conceptual insights into the structural disadvantages democracies face in cyberspace, rather than to claim statistical generalizability across all democracies. Accordingly, all findings and conclusions in this article are scoped to the United States, the United Kingdom, and Germany. While some dynamics may be relevant to other democratic states, no claim is made that the patterns observed here apply universally across all democracies without further empirical examination.

Addressing these strategic vulnerabilities, the article ultimately argues for a balanced yet robust deterrence framework. While advocating for strengthened defensive resilience and international norm-building initiatives, it firmly underscores the necessity of retaining traditional military retaliation options—such as targeted kinetic strikes—under clearly defined and internationally agreed legal

frameworks. This comprehensive approach aims to enable democracies not only to defend their digital infrastructures and institutions effectively but also to shape a secure, stable, and norm-governed cyberspace environment.

Attribution, Ambiguity, and Thresholds

Attribution, ambiguity, and thresholds are central challenges in cyber deterrence, presenting strategic, operational, and technical difficulties that democratic states must navigate carefully. Attribution, or correctly identifying the source of a cyberattack, remains technically and politically challenging due to the inherent anonymity and transnational nature of cyberspace.[3] This examination of democratic approaches—specifically those of the United States, the United Kingdom, and Germany—reveals their struggle with both technical constraints, such as false-flag operations and sophisticated obfuscation, and strategic constraints arising from the political risks of misattribution. For example, the United States has historically embraced "instrumental ambiguity"—a deliberate vagueness about thresholds, red lines, and response options intended to preserve decision-maker discretion and complicate an adversary's risk calculus—to maintain flexibility, avoiding premature attribution that could force an escalation or damage diplomatic relations.[4]

For the three democratic states in this investigation, ambiguity in cyber engagement rules compounds the challenge of attribution by further constraining an already limited set of lawful and ethical response options. The North Atlantic Treaty Organization (NATO) explicitly recognizes that a cyberattack can trigger Article 5, which defines an attack on one member as an attack on all, yet its Cyber Defense Pledge strategically avoids specifying clear thresholds.[5] NATO's ambiguous stance is intended to prevent adversaries from identifying precise red lines, thereby maintaining operational flexibility and deterrence through uncertainty. However, this ambiguity also creates opportunities for adversaries to conduct cyber operations below the threshold of armed conflict, exploiting the uncertainty around what constitutes a sufficiently severe cyberattack to trigger collective defense, as emphasized in Martin C. Libicki's study on crisis and escalation dynamics in cyberspace.[6] While some scholars argue that strategic ambiguity can reduce the risk of automatic escalation by preserving political discretion, the cyber domain's low visibility and rapid tempo often mean that adversaries perceive hesitation rather than resolve, thereby undermining deterrence rather than strengthening it.[7]

National doctrines further complicate this threshold ambiguity. The United States' *2023 Cyber Strategy of the Department of Defense* emphasizes cyber operations below armed conflict thresholds to deter adversaries without escalating into conventional warfare, thus reflecting a careful calibration informed by constitutional principles of proportionality and necessity.[8] Similarly, the UK's

Ministry of Defence outlines cyber capabilities as integrated into broader military operations, emphasizing adherence to IHL and ethical standards derived from British legal norms.[9] Germany, whose Basic Law prioritizes defensive strategies and mandates strict parliamentary oversight of military engagements, established the Cyber and Information Domain Service within the *Bundeswehr* (Federal Armed Forces), balancing operational effectiveness with legal accountability, as reinforced by Germany's *National Security Strategy*, which stresses a "resolutely defensive cyber stance" grounded in democratic oversight, parliamentary control, and a commitment to international law.[10] Thus, while national doctrines reflect an awareness of cyber threats, democratic states' internal legal and ethical frameworks severely limit their operational flexibility compared to authoritarian adversaries who face fewer normative constraints.

Operational constraints significantly influence these strategies. The U.S. Cyber Command's initiatives, like the Cyber Operational Readiness Assessment Program, aim to provide clarity and operational readiness within strict ethical and legal boundaries.[11] Likewise, the UK's National Cyber Security Centre employs active defensive measures under its Active Cyber Defence program, designed to mitigate threats within accountability frameworks under the oversight of publicly elected politicians.[12] These oversight mechanisms, while fundamental to a functioning democracy, puts additional constraints and bureaucratic burden on the agencies responding to cyber threats—defensive and offensive. Germany's Federal Office for Information Security highlights persistent high-threat environments and stresses enhanced resilience through technical preparedness and public-private collaboration.[13]

This reflects that, for the United States, the United Kingdom, and Germany, the intersection of attribution challenges, strategic ambiguity, and uncertain thresholds significantly complicates cyber deterrence. Addressing these issues requires continuous refinement of operational capabilities and legal frameworks to balance effectiveness, legality, and ethical accountability within their respective democratic systems.

Inequality in Cyber Capabilities

The deployment of offensive cyber capabilities by democratic states presents profound ethical, legal, and strategic dilemmas, fundamentally conflicting with core democratic principles such as transparency, accountability, and adherence to the rule of law.[14] Democracies rest on open governance and oversight, wherein executive actions, particularly those involving military capabilities, must be transparent enough to permit public debate and legislative oversight. However, offensive cyber operations typically necessitate secrecy and operational ambiguity, challenging these fundamental tenets.[15] As Bryan Nakayama cautions, "the offensive employment of information operations risks deepening the challenges

that democracies currently face," particularly by expanding state power in ways that are difficult to monitor or contest.[16] The absence of transparency consequently erodes public trust, creating a governance paradox where democracies use nondemocratic means ostensibly to protect democratic freedoms.

Moreover, offensive cyber operations are structurally weakened in the three democratic systems of this article, either by procedural drag or political backlash. In systems with strong legislative oversight, operational agility suffers.[17] For instance, Germany's *Grundgesetz* mandates strict parliamentary oversight of military operations, especially offensive cyber operations, which must navigate legal gray zones that constrain flexibility and undermine the operational effectiveness required for timely and covert responses.[18] Conversely, when offensive cyber activities are primarily directed by the executive, they risk bypassing democratic checks, which can erode public trust and legitimacy. The United States exemplifies this tension: the executive branch frequently uses existing legal authorities expansively, leading to operations that evade detailed congressional review.[19] Similarly, the UK's National Cyber Force, though subject to limited parliamentary scrutiny, has prompted concerns about the appropriate balance between secrecy and democratic accountability.[20] Thus, democratic regimes face a dual vulnerability: either offensive cyber operations become sluggish and bureaucratically encumbered, or they provoke domestic criticism for circumventing transparency and oversight.

Further complicating these operational challenges, offensive cyber operations occupy an uncertain legal and ethical landscape. Current IHL and existing treaties offer only a general framework for cyber warfare, leaving states—particularly the democracies in this investigation—to interpret foundational principles such as proportionality, necessity, and discrimination amid significant ambiguity.[21] The inherently diffuse and unpredictable impacts of cyberattacks raise ethical questions about civilian harm and collateral damage, which are critical under democratic legal frameworks. Democracies also risk setting troubling precedents: the use of intrusive tools such as malware or spyware for offensive purposes—even if targeted at adversarial entities—can inadvertently normalize practices antithetical to democratic ideals like privacy and freedom of speech. The Brookings Institution emphasizes that the creeping normalization of surveillance and disruption tools could erode civil liberties domestically, as the boundaries between legitimate security measures and authoritarian practices become increasingly indistinct.[22] In contrast, authoritarian states face fewer ethical constraints, as their populations are already subject to pervasive digital surveillance and coercive security practices; consequently, these regimes possess greater operational familiarity with intrusive cyber capabilities, conferring them a strategic advantage in potential conflict scenarios.

Strategically, reliance on offensive cyber capabilities also entails substantial

risks of escalation and unintended conflict, particularly troubling for democracies committed to maintaining international peace and stability. The ambiguity intrinsic to cyber operations complicates attribution, increasing the potential for misinterpretation and erroneous retaliation.[23] Such uncertainty may escalate tensions, thereby contradicting democratic states' strategic interests in global stability and predictable international behavior. Given that democracies typically maintain open and digitally integrated infrastructures, these states paradoxically become uniquely vulnerable to retaliatory cyberattacks, potentially inviting devastating consequences far exceeding the initial benefits of offensive cyber engagements. Consequently, offensive operations risk undermining national security rather than enhancing it, compelling democratic states to carefully weigh such tactics against their broader strategic imperatives and commitments to international peace.

These contrasts have practical consequences for deterrence credibility. The United States' willingness to engage in persistent cyber contact operations can signal resolve but also risks normalizing low-level hostilities, potentially eroding escalation thresholds over time.[24] The United Kingdom's emphasis on "responsible cyber power" strengthens normative legitimacy but can create operational hesitancy in crises where rapid offensive action might deliver strategic effect.[25] Germany's defensive posture preserves legal and political legitimacy at home and abroad, yet its highly restrictive authorization process may reduce the deterrent value of its cyber forces by making timely retaliation appear unlikely to adversaries.[26] Together, these variations underscore that even within a small group of high-capability democracies, institutional design and strategic culture can materially shape how deterrence is perceived and contested in cyberspace.

To align cyber policies with democratic values, states should emphasize transparency, clear legal frameworks, and international cooperation rather than opaque offensive strategies. Clearly codified legal structures under strict legislative oversight can bridge the accountability gap, helping to preserve democratic integrity and public trust even amid necessary secrecy. Initiatives promoting international cyber norms and cooperative cybersecurity frameworks, such as Microsoft's proposal for a "Digital Geneva Convention," underscore democratic states' commitment to ethical cyberspace conduct, emphasizing civilian protection and international accountability mechanisms.[27] While the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* constitutes a notable effort to adapt traditional legal principles to cyberspace, it remains fundamentally limited by its NATO-centric origins and lack of formal endorsement by global institutions like the United Nations or the International Committee of the Red Cross (ICRC).[28] Even among NATO members, significant differences persist regarding the permissibility and ethical scope of offensive cyber operations, with countries like the United States favoring a broader interpretation

of lawful cyber force while others, such as Germany, adopt a more restrictive and defensive posture. This divergence further weakens the manual's normative authority and highlights the urgent need for democracies to invest in truly multilateral frameworks if they intend to shape durable, widely accepted cyber norms. Strengthening cyber defense capabilities, international collaboration, and education in cyber resilience would enable democracies to uphold their values while effectively countering cyber threats. Such a balanced approach allows democratic states to assert leadership in setting global norms, ensuring both national security and democratic integrity in the complex digital age.

Diffusion between (Non)state Actors in Cyberspace

Building on the challenges democracies face in establishing and enforcing international cyber norms, the diffusion of cyber capabilities between state and nonstate actors has significantly altered the operational dynamics of cyberspace, complicating traditional distinctions between organized military activities and actions taken by independent entities. Increasingly, states employ nonstate actors—such as private cybercriminal organizations, patriotic hackers, or loosely organized digital militias—to conduct cyber operations aligned with national interests, thereby maintaining plausible deniability and obscuring direct attribution. Russia, notably, has harnessed cybercriminal networks and informal hacking collectives in support of geopolitical objectives. Groups like KillNet and XakNet have launched cyberattacks against states supportive of Ukraine, while also soliciting cryptocurrency donations to fund activities in Russia's favor, often under the guise of volunteerism or patriotic activism.[29] Such state-backed proxy operations blur lines of accountability, challenge traditional methods of attribution, and complicate diplomatic responses to cyber aggression.

Simultaneously, nonstate actors have independently adopted tools and methods historically reserved for state-led cyber operations, enhancing their ability to inflict substantial damage and influence international conflicts. A prominent example includes the IT Army of Ukraine, a civilian-led digital force established in response to Russia's illegal invasion. Comprising thousands of volunteer hackers worldwide, this group has conducted coordinated cyber operations targeting Russian state entities, illustrating the empowerment of nonstate groups through democratized cyber capabilities.[30] This convergence in techniques and technology access reflects a broader diffusion phenomenon, enabled by readily available "turnkey" hacking tools—prepackaged software solutions that lower the technical barriers for sophisticated cyberattacks. As Mohamed Aly Bouke and Ahmed Abdullah argue, the widespread availability of these tools democratizes access to powerful cyber weapons, thereby empowering diverse actors ranging from organized crime syndicates to politically motivated hacktivist groups.[31] Unlike nuclear weapons, whose proliferation is

constrained by technical, material, and international regulatory barriers, cyber capabilities diffuse rapidly and uncontrollably across state and nonstate actors, making traditional nonproliferation approaches largely ineffective in the digital domain. While the diffusion of nonstate cyber capabilities poses risks to both democratic and authoritarian states, the challenge is qualitatively different for democracies. Authoritarian regimes can employ rapid, extrajudicial measures against suspected cyber actors, operate without public disclosure, and mobilize state-aligned proxies without domestic legal repercussions.[32] Democracies, by contrast, are bound by due process, evidentiary standards, and parliamentary or judicial oversight, which slow attribution, limit covert reprisals, and require public justification for countermeasures.[33] This asymmetry means that when nonstate threats operate in the legal or technical gray zone, democracies face higher procedural thresholds to act, greater public scrutiny if mistakes are made, and narrower operational windows before deterrent effects degrade. In effect, the same diffuse threat landscape imposes heavier strategic and political costs on democracies than on nondemocracies.

This dual diffusion—state actors appropriating nonstate entities and nonstate actors adopting state-level cyber capabilities—poses severe challenges to existing legal frameworks and democratic accountability structures. The complex interdependency between states and nonstate actors complicates the enforcement of international norms, making it difficult to clearly attribute cyberattacks and implement proportionate responses.[34] Democracies struggle to develop effective deterrence mechanisms in this ambiguous environment, as traditional diplomatic or military retaliation becomes problematic without unequivocal evidence linking adversaries directly to cyber operations. Consequently, this diffusion increases risks of miscalculation and escalation, particularly problematic for democracies committed to international law and conflict deescalation. The decentralized and diffuse nature of nonstate cyber entities makes diplomatic resolution challenging, as these groups lack formal organizational structures or accountability mechanisms typically available to state-controlled military forces. Without clear attribution or mechanisms to engage these nonstate actors diplomatically, democracies find themselves constrained, facing escalatory risks with limited options to manage crises effectively or peacefully.[35]

Addressing these challenges requires democracies to refine their strategic doctrines, emphasizing cyber resilience, attribution capabilities, and enhanced international cooperation. Effective international norms must explicitly address the roles and responsibilities of both states and nonstate actors, recognizing the diffusion and democratization of cyber capabilities. Democracies must foster clearer norms around state responsibilities in managing relationships with cyber proxies, explicitly prohibiting tacit support for nonstate actors engaged in offensive cyber operations. Strengthening cooperative international frameworks,

such as those proposed in initiatives like the "Digital Geneva Convention," can establish clearer accountability standards, thereby mitigating the risks associated with this diffusion phenomenon and enhancing global cyber stability.

Ethical and Legal Constraints under International Humanitarian Law

Democratic states adhering strictly to IHL face significant strategic and operational disadvantages in cyber warfare compared to authoritarian or noncompliant states, due primarily to ethical and legal constraints inherent in democratic systems. These disadvantages manifest specifically through the difficulty of attribution, the challenge of maintaining proportionality and distinction, and the underdeveloped legal frameworks governing cyber operations. Unlike conventional warfare, where the identity of an aggressor, the target of an attack, and the boundaries of battlefield effects are typically clear, cyber warfare is characterized by profound ambiguity and complex jurisdictional challenges, complicating the lawful execution of cyber operations.[36]

A central constraint is the principle of attribution, which is fundamental in determining lawful responses under IHL. Cyber operations frequently obscure the identity of attackers through sophisticated techniques such as routing attacks via multiple jurisdictions, hijacking civilian networks, or employing false-flag strategies, making attribution highly challenging.[37] While conventional military attacks usually provide immediate and reliable indicators of their source—such as identifiable military units or the geographical origin of artillery fire—cyberattacks rarely leave clear forensic evidence sufficient to justify immediate military response under the rigorous standards of democratic legal oversight. This lack of clear attribution severely limits democracies' lawful retaliatory options, often restricting them to defensive or nonmilitary responses even when facing severe provocations.[38]

Additionally, the principle of distinction, requiring clear differentiation between military targets and civilian objects, is particularly difficult to uphold in cyber operations due to the interconnected nature of digital infrastructure. The ICRC has emphasized that because civilian and military infrastructures frequently overlap in cyberspace, targeting even a seemingly legitimate military objective can inadvertently disrupt essential civilian services such as hospitals, banking systems, and water supplies, causing disproportionate civilian harm.[39] In contrast, conventional warfare typically allows a clearer separation of military objectives from civilian infrastructure, simplifying adherence to IHL principles. Consequently, democracies that would strictly enforce compliance with the principle of distinction would find themselves strategically constrained. In particular, Germany vigorously has promoted IHL adherence as a central element of its foreign policy and therefore could see itself refraining from aggres-

sive cyber operations for fear of inadvertent violations of international law and humanitarian standards.[40]

Similarly, proportionality—the balance between anticipated military gain and potential civilian harm—poses complex ethical and operational challenges in cyber warfare. Cyber operations inherently carry risks of cascading and unpredictable effects, potentially causing extensive collateral damage beyond intended military targets.[41] For example, a targeted cyberattack intended to disable a military communication system could unintentionally incapacitate civilian telecommunications, healthcare services, or critical infrastructure. Such unintended outcomes conflict directly with democratic commitments to minimize civilian harm, creating a significant ethical and legal deterrent against aggressive cyber responses.[42] Conversely, conventional military methods, such as precise kinetic strikes, usually allow more predictable damage assessments and therefore clearer compliance with the principle of proportionality under established IHL guidelines.

Furthermore, democratic states face substantial disadvantages due to the underdeveloped international legal frameworks specifically governing cyber operations, contrasting markedly with the robust treaties and established norms present in conventional warfare. Currently, no comprehensive treaty explicitly addresses cyber warfare, leaving states reliant on interpretations of existing IHL principles developed for conventional kinetic conflicts. The ICRC highlights the resulting legal ambiguity, noting that without precise and universally accepted standards tailored explicitly to cyber warfare, democratic states are forced into cautious interpretations of IHL, restricting their capacity to execute effective offensive cyber responses.[43]

This legal ambiguity contrasts significantly with conventional warfare scenarios, where robust frameworks such as the Geneva Conventions provide clear standards and universally accepted rules governing state conduct, responsibilities, and liabilities. For example, the criteria defining an armed attack or the conditions triggering the right of self-defense under Article 51 of the United Nations Charter are much clearer and widely recognized for physical attacks.[44] In contrast, determining when a cyber operation constitutes an armed attack remains contested internationally, resulting in legal uncertainty and caution among democratic states adhering strictly to international law. Such uncertainty often compels democracies toward defensive postures or diplomatic solutions, limiting their ability to use decisive cyber actions proactively, thereby handing strategic advantages to less scrupulous adversaries who exploit these ambiguities.[45]

Moreover, the transnational nature of cyberspace further complicates adherence to and enforcement of IHL. Cyber operations can originate, transit, and impact multiple jurisdictions simultaneously, complicating attribution, prose-

cution, and enforcement efforts significantly more than conventional military engagements, which typically remain geographically contained.[46] This inherent complexity poses severe jurisdictional and diplomatic challenges for democratic states seeking lawful responses or accountability through international cooperation or prosecution.[47] Authoritarian states or non-state actors operating with implicit state consent exploit these legal gaps, conducting aggressive cyber campaigns from jurisdictions where legal enforcement by democratic states proves impractical or diplomatically costly.

In summary, democratic states' strict adherence to IHL significantly disadvantages them in cyber warfare relative to conventional military engagements due to attribution challenges, complexities around proportionality and distinction, underdeveloped legal frameworks, domestic accountability mechanisms, and jurisdictional issues. Addressing these critical disparities requires the international community, guided by organizations such as the ICRC and relevant think tanks, to develop explicit and robust international norms and treaties tailored specifically to cyber warfare. Until then, democratic states remain strategically constrained, compelled to balance ethical compliance against operational necessity within an ambiguous and rapidly evolving cyber domain.

How Can We Get Global Norms in Cyber Warfare?

The urgent need for global norms in cyber warfare stems from the unique characteristics of the digital domain: anonymity, asymmetry, and the lack of inherent territorial boundaries. Unlike conventional military domains, cyberspace currently lacks a widely accepted and enforceable framework to regulate state behavior. Although efforts like the United Nations' Group of Governmental Experts and the Open-Ended Working Group have confirmed that existing international law, including IHL, applies to cyber operations, these initiatives have fallen short of creating binding agreements or comprehensive enforcement mechanisms.[48] Democratic states, which traditionally anchor their military actions within clear legal and ethical boundaries, find themselves particularly vulnerable in this regulatory vacuum.

Building global norms in cyber warfare will require a multipronged strategy focused on broadening participation, increasing transparency, and forging common interests even among geopolitical rivals. Initiatives like the Global Commission on the Stability of Cyberspace and the Paris Call for Trust and Security in Cyberspace represent important steps toward establishing baseline expectations, particularly the protection of critical civilian infrastructure and prohibitions against indiscriminate cyberattacks.[49] However, these efforts face resistance from authoritarian states that perceive cyber operations as indispensable asymmetric tools to counterbalance Western technological advantages.[50] Moreover, unlike nuclear nonproliferation frameworks where material con-

straints and verification mechanisms can physically limit the spread of capabilities, cyber weapons are often intangible, replicable, and difficult to monitor.[51] As Joseph S. Nye argues, deterrence and dissuasion in cyberspace must therefore rely more heavily on norm-building and reputational costs rather than purely on threat-based strategies.[52]

To foster truly global norms, democracies must expand multilateral engagement beyond traditional Western alliances, including regional organizations and emerging cyber powers. Transparency measures, such as voluntary disclosures of doctrine and restraint pledges, can help build mutual trust. Equally important is reinforcing the idea that sovereignty, civilian protection, and proportionality apply as much in cyberspace as in conventional conflict.[53] However, efforts toward transparency and normative restraint must be calibrated carefully, ensuring that democratic states retain sufficient operational flexibility until reciprocal commitments to norm-building are forthcoming from all major actors. Without sustained commitment to coalition-building, norm promotion, and credible mutual restraint, the digital domain risks further fragmentation into competing spheres of influence governed by conflicting cyber doctrines.

In this context, collective deterrence mechanisms enhance the credibility and capacity of democratic states to shape responsible behavior. Through alliances such as NATO, democracies can coordinate threat intelligence, pool technical expertise, and present a unified front against malicious cyber actors. The NATO Cyber Defense Pledge reflects this commitment, emphasizing not only mutual defense but also sustained national investments in cyber preparedness.[54] Institutions like the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) further contribute by advancing legal, strategic, and operational thinking. Most notably, the *Tallinn Manual 2.0*, produced under the auspices of the CCDCOE, remains the most comprehensive nonbinding attempt to clarify how existing international law applies to cyber operations—serving as a reference point for norm development, even if it has yet to gain universal traction.[55]

In conclusion, shaping global norms in cyber warfare requires democracies to move beyond deterrence thinking alone and toward proactive *norm entrepreneurship*, which means the active promotion and institutionalization of new rules, in this case responsible behavior in cyber warfare. Through inclusive diplomacy, targeted normative agreements, and the reinforcement of ethical cyber behavior, the international community can work toward a cyberspace governed by rules rather than brute force.[56]

Strategies for Ethical and Effective Cyber Deterrence

While the establishment of global norms in cyber warfare remains an essential long-term objective, democracies must also adopt immediate strategies to

safeguard their digital domains ethically and effectively. Strengthening cyber resilience offers a pragmatic path forward, enabling states to uphold democratic values while countering escalating cyber threats.

A core element of resilience is a layered defense-in-depth strategy. Technological safeguards such as firewalls, intrusion detection systems, and regular vulnerability assessments help protect critical infrastructure. The U.S. *Cyber Resilience Review* offers a framework emphasizing operational continuity and adaptive response to evolving threats.[57] Equally essential is cybersecurity education. Enhancing cyber literacy among citizens and IT professionals reduces human error and strengthens societal resilience. Lydia Kraus et al. demonstrate the long-term value of embedding cybersecurity training in academic curricula, while Valdemar Švábenský et al. highlight the importance of cyber ranges and simulations for preparing personnel to respond effectively under pressure.[58] International cooperation further reinforces national efforts. NATO-led initiatives promote shared training, Joint exercises, and interoperable defense systems, fostering collective security among democracies.[59] National legislation also plays a key role: the UK's Cyber Security and Resilience Policy integrates resilience into public infrastructure strategy, ensuring legal frameworks keep pace with dynamic threat environments.[60]

Together, these elements form a comprehensive model of cyber deterrence by denial—one that disincentivizes attacks by reducing their potential impact and increasing the cost of success. Crucially, such an approach avoids the ethical pitfalls of offensive retaliation, aligning with democratic commitments to transparency, proportionality, and civilian protection. By investing in layered defense, human capacity, and cooperative policy, democratic states can strengthen cyber stability while maintaining legitimacy in the international system.

Leave Traditional Deterrence on the Table

Given the escalating threat landscape in cyberspace, democratic states must decisively maintain the option of direct military action to effectively deter adversaries. Cyber aggression can no longer be answered solely through defensive cyber measures, diplomatic condemnations, or limited sanctions—responses that have repeatedly proven insufficient in curbing malicious cyber activities from strategic competitors. James M. Acton clearly illustrates how the absence of clearly defined thresholds and credible attribution emboldens aggressors, increasing the risk of inadvertent escalation.[61] Democracies, therefore, must demonstrate unequivocally that hostile cyber operations will trigger tangible, real-world military consequences.

Kinetic military actions, such as precision airstrikes or missile attacks on adversarial cyber infrastructures—including data centers, communication hubs, and operational command posts—must be firmly established as credible

responses within IHL frameworks. Laurent Gisel and Tilman Rodenhäuser underscore the urgency of explicitly applying IHL principles like proportionality and necessity to cyberspace conflicts.[62] Clearly articulated legal justifications for military retaliation will not only reinforce legitimacy but also strengthen deterrence by signaling serious consequences for cyber provocations. In parallel, democracies should aggressively pursue covert intelligence and special operations to dismantle adversarial cyber capabilities. Tim Maurer compellingly argues for the strategic impact of apprehending or eliminating state-sponsored cyber operatives.[63] Targeted intelligence operations that disrupt adversaries' cyber units and infrastructure send an unmistakable message: cyber aggressions will incur personal and operational risks. While some democracies possess the military reach and legal latitude to credibly threaten kinetic responses to cyber aggression, others—such as Germany—are more constrained by constitutional limits, parliamentary oversight, and force projection capacity. This analysis therefore confines its discussion of conventional military options to states, like the United States and the United Kingdom, whose political and military frameworks make such measures viable and would call upon defense-passive and reactive states like Germany to rethink its overall deterrence strategy in light of the illegal Russian invasion of Ukraine.

In conclusion, to preserve strategic stability and safeguard democratic institutions, states must adopt a robust deterrence posture that explicitly includes direct and decisive military retaliation for cyber aggression. Allowing nations like China and Russia to conduct cyber operations without severe repercussions only encourages further hostility. A deterrence strategy that integrates clear military options within existing legal frameworks is vital to maintaining global security and deterring future cyber threats.

Conclusion

Democratic states currently face significant strategic disadvantages in cyber deterrence, primarily due to their adherence to ethical constraints, transparent governance, and rigorous legal frameworks. These inherent limitations create a challenging operational environment, where attribution remains difficult, thresholds remain ambiguous, and offensive actions risk escalating into broader conflicts. To overcome these issues, democracies must combine immediate defensive strategies—such as strengthening cyber resilience and fostering international cooperation—with the credible threat of traditional kinetic retaliation under explicit IHL frameworks. Moreover, democracies must lead efforts to establish global cyber norms through inclusive diplomacy, clear transparency measures, and concrete accountability standards. While pursuing these norm-building initiatives, democratic states should remain pragmatic, maintaining flexible and credible military options to ensure adversaries clearly un-

derstand the real-world consequences of cyber aggression. These conclusions are drawn from the specific institutional and strategic contexts of the United States, the United Kingdom, and Germany and should be understood within that comparative frame. By strategically balancing defensive resilience, proactive norm entrepreneurship, and decisive traditional deterrence, democracies can effectively protect national security interests, uphold democratic values, and promote global cyber stability. Without these integrated measures, the digital domain risks further fragmentation and heightened vulnerability to cyber threats.

Endnotes

1. Erica D. Borghard and Shawn W. Lonergan, "Deterrence by Denial in Cyberspace," *Journal of Strategic Studies* 46, no. 3 (2021): 534–69, https://doi.org/10.1080/01402390.2021.1944856.
2. The *Grundgesetz* has served as the Federal Republic of Germany's constitution since 1949. *Cyber Capabilities and National Power*, vol. 2 (London: International Institute for Strategic Studies, 2023).
3. Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, nos. 1–2 (2015): 4–37, https://doi.org/10.1080/01402390.2014.977382.
4. Benjamin Jensen and Brandon Valeriano, *What Do We Know about Cyber Escalation?: Observations from Simulations and Surveys* (Washington, DC: Atlantic Council, 2019).
5. NATO, "Cyber Defence Pledge," press release, 8 July 2016.
6. Martin C. Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica, CA: Rand, 2013), https://doi.org/10.7249/MG1215.
7. Jacquelyn G. Schneider, "Deterrence in and through Cyberspace," in *Cross-Domain Deterrence: Strategy in an Era of Complexity*, ed. Erik Gartzke and Jon R. Lindsay (New York: Oxford University Press, 2019), 95–120, https://doi.org/10.1093/oso/9780190908645.003.0005.
8. *Summary: 2023 Cyber Strategy of the Department of Defense* (Washington, DC: Department of Defense, 2023). At the time of this article's writing, the official name of the Department of Defense had not yet changed to Department of War.
9. *Cyber Primer*, 3d ed. (London: Ministry of Defence, 2022).
10. *National Security Strategy* (Bonn, Germany: Federal Ministry of Defence, 2023).
11. *Summary: 2023 Cyber Strategy*.
12. *Active Cyber Defence: The Sixth Year* (London: National Cyber Security Centre, 2023).
13. *The State of IT Security in Germany in 2023* (Bonn, Germany: Federal Office for Information Security, 2023).
14. Nori Katagiri, *How Liberal Democracies Defend Their Cyber Networks from Hackers: Strategies for Deterrence* (Cham, Switzerland: Palgrave Macmillan, 2024), https://doi.org/10.1007/978-3-031-54561-0.
15. *Guidance: Responsible Cyber Power in Practice* (London: National Cyber Force, 2023).
16. Bryan Nakayama, "Democracies and the Future of Offensive (Cyber-Enabled) Information Operations," *Cyber Defense Review* 7, no. 3 (Summer 2022).
17. *Cyber Capabilities and National Power*, vol. 2.
18. Matthias Schulze, "German Military Cyber Operations Are in a Legal Gray Zone," Lawfare, 8 April 2020.
19. Nakayama, "Democracies and the Future of Offensive (Cyber-Enabled) Information Operations."
20. Joe Devanny, "The Ethics of Offensive Cyber Operations," Foreign Policy Centre, 3 December 2020.

21. Maj Benjamin Ramsey, "An Ethical Decision-Making Tool for Offensive Cyberspace Operations," *Air and Space Power Journal* 32, no. 3 (Fall 2018): 62–71.
22. Ted Piccone, *Democracy and Cybersecurity*, Policy Brief (Washington, DC: Brookings Institution, 2017).
23. Rid and Buchanan, "Attributing Cyber Attacks," 4–37.
24. *Cyber Capabilities and National Power*, vol. 2.
25. Joe Devanny and Professor John Gearson, eds., *The Integrated Review in Context: Defence and Security in Focus* (London: Centre for Defence Studies, Kings College London, 2021).
26. Rid and Buchanan, "Attributing Cyber Attacks," 4–37.
27. Jeremy Hsu, "You Are the Target of Today's Cyberwars," *Wired*, 2 March 2017.
28. Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge, UK: Cambridge University Press, 2017), hereafter *Tallinn Manual 2.0*, https://doi.org/10.1017/9781316822524.
29. David Kirichenko, "Crypto Boosts Ukraine—and Russia," Center for European Policy Analysis (CEPA), 5 January 2024.
30. Matt Burgess, "Ukraine's Volunteer 'IT Army' Is Hacking in Uncharted Territory," *Wired*, 27 February 2022.
31. Mohamed Aly Bouke and Ahmed Abdullah, "Turnkey Technology: A Powerful Tool for Cyber Warfare," arXiv.org, 28 August 2023, https://doi.org/10.48550/arXiv.2308.14576.
32. Katagiri, *How Liberal Democracies Defend Their Cyber Networks from Hackers*.
33. *Cyber Capabilities and National Power*, vol. 2.
34. Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, UK: Cambridge University Press, 2018), https://doi.org/10.1017/9781316422724.
35. Maurer, *Cyber Mercenaries*.
36. Kubo Mačák and Tilman Rodenhäuser, "Towards Common Understandings: The Application of Established IHL Principles to Cyber Operations," *Humanitarian Law & Policy* (blog), ICRC, 7 March 2023.
37. Maurer, *Cyber Mercenaries*.
38. "International Humanitarian Law and Cyber Operations during Armed Conflicts," *International Review of the Red Cross* 102, no. 913 (2019): 481–92, https://doi.org/10.1017/s1816383120000478.
39. "International Humanitarian Law and Cyber Operations during Armed Conflicts," 481–92.
40. *Cyber Capabilities and National Power*, vol. 2.
41. Schmitt, *Tallinn Manual 2.0.*
42. Robin Geiss and Henning Lahmann, *Protecting Societies: Anchoring a New Protection Dimension in International Law in Times of Increased Cyber Threats* (Switzerland: Geneva Academy of International Humanitarian Law and Human Rights, 2021).
43. "International Humanitarian Law and Cyber Operations during Armed Conflicts," 481–92.
44. Geiss and Lahmann, *Protecting Societies*.
45. Maurer, *Cyber Mercenaries*.
46. Mačák and Rodenhäuser, "Towards Common Understandings."
47. Maurer, *Cyber Mercenaries*.
48. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (New York: United Nations, 2015); and Arindrajit Basu, Irene Poetranto, and Justin Lau, "The UN Struggles to Make Progress on Securing Cyberspace," Carnegie Endowment for International Peace, 19 May 2021.
49. *Advancing Cyberstability: Final Report, November 2019* (The Hague: Global Commission on the Stability of Cyberspace, 2019); and "Paris Call for Trust and Security in Cyberspace," Ministère de l'Europe et des Affaires Étrangères (MEAE), November 2018.

50. Christian Ruh et al., *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads* (Washington, DC: Carnegie Endowment for International Peace, 2020).
51. Bouke and Abdullah, "Turnkey Technology."
52. Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security* 43, no. 3 (2017): 44–71, https://doi.org/10.1162/ISEC_a_00266.
53. Laurent Gisel and Tilman Rodenhäuser, "Cyber Operations and International Humanitarian Law: Five Key Points," *Humanitarian Law & Policy* (blog), ICRC, 28 November 2019.
54. "Cyber Defence Pledge."
55. Schmitt, *Tallinn Manual 2.0*.
56. Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52, no. 4 (Autumn 1988): 887–917, https://doi.org/10.1162/002081898550789.
57. *Cyber Resilience Review (CRR): Method Description and Self-Assessment User Guide* (Washington, DC: Department of Homeland Security, 2014).
58. Lydia Kraus et al., "Want to Raise Cybersecurity Awareness?: Start with Future IT Professionals," in *ITiCSE 2023: Proceedings of the 2023 Conference on Innovation and Technology in Computer Science Education* (New York: Association for Computing Machinery, 2023), https://doi.org/10.1145/3587102.3588862; and Valdemar Švábenský et al., "Enhancing Cybersecurity Skills by Creating Serious Games," in *ITiCSE 2018: Proceedings of the 23d Annual ACM Conference on Innovation and Technology in Computer Science Education* (New York: Association for Computing Machinery, 2018), https://doi.org/10.1145/3197091.3197123.
59. Alexander Kott et al., "Approaches to Enhancing Cyber Resilience: Report of the NATO Workshop IST-153," arXiv.org, 20 April 2018, https://doi.org/10.48550/arxiv.1804.07651.
60. *Cyber Security and Resilience Policy Statement* (London: Department of Science, Innovation, and Technology, 2025).
61. James M. Acton, "Cyber Warfare & Inadvertent Escalation," *Daedalus* 149, no. 2 (2020): 133–49, https://doi.org/10.1162/daed_a_01794.
62. Gisel and Rodenhäuser, "Cyber Operations and International Humanitarian Law."
63. Maurer, *Cyber Mercenaries*.

Artificial Intelligence-Enabled Military Decision-Making Process
The Forgotten Lessons on the Nature of War

Major Vincenzo Gallitelli, Italian Army

Abstract: This article examines the integration of artificial intelligence (AI) into the military decision-making process (MDMP) through a multidisciplinary approach, with particular attention to the experimental COA-GPT system. While AI offers unprecedented opportunities to accelerate operational tempo, generates multiple courses of action (COAs), and reduces cognitive burdens on commanders and staff, the study warns against overreliance on quantitative metrics and algorithmic processes and outputs. Drawing on Carl von Clausewitz's principles, Trevor N. Dupuy's models, and historical failures such as Robert S. McNamara's "body count" in Vietnam, the analysis highlights the enduring uncertainty and friction of war that cannot be captured by purely mathematical or deterministic models. AI's risks of overfitting, black-box opacity, and the exclusion of moral, human, and contextual factors underscore the indispensable role of human judgment. The article emphasizes the need to adapt doctrine, organization, training, leadership, and infrastructure to the challenges and opportunities introduced by AI. The goal is to ensure that AI is employed as a powerful enabling tool that enhances human decision making rather than replacing it.
Keywords: artificial intelligence, AI, military decision-making process, MDMP, planning process, metrics, COA-GPT, Carl von Clausewitz, Trevor N. Depuy

The integration of artificial intelligence (AI) into the military decision-making process (MDMP) currently represents the most significant technological development in modern warfare, with the potential to

Maj Vincenzo Gallitelli is an amphibious infantry officer of the Italian Army. He served as platoon and company commander in the Lagunari Regiment, being deployed with his units to Iraq and Afghanistan. He is a graduate of the Italian Army Staff Officer Course and the Marine Corps Expeditionary Warfare School.

Journal of Advanced Military Studies vol. 16, no. 2
Fall 2025
www.usmcu.edu/mcupress
https://doi.org/10.21140/mcuj.20251602005

fundamentally transform the traditional approach to planning and conducting operations. Ongoing conflicts and the current geopolitical situation underscore the magnitude of this transformation: on the one hand, Russian and Ukrainian forces are racing to enhance AI-driven systems on the battlefield, striving to accelerate targeting processes and battlefield analysis with ever-greater speed and precision; on the other hand, major global powers such as the United States and China are investing billions of dollars in both civilian and military AI applications, fully aware that these technologies will confer a decisive strategic advantage over potential adversaries, and fueling what is increasingly being called an "AI Cold War."[1]

In the military domain, advancements in AI undoubtedly offer unprecedented potential for a pivotal revolution.[2] The relative speed and effectiveness of decision making are the most critical capabilities to succeed in military operations. The current operating environment, marked by increasingly congested spaces, complex areas, contested domains, interconnected zones, constraints on the use of force, enhanced battlefield firepower and surveillance, and heightened vulnerability to cyberattacks, further emphasizes the need to maintain an operational tempo superior to the adversary.[3] This advantage relies on continuously updated situational awareness that informs a timely decision-making process.

Drawing from the most significant cornerstone of naval warfare, which emphasizes the necessity to strike effectively first, we can assert that in all other domains as well, there is now more than ever a critical need to act effectively and decisively first.[4] To preserve initiative and gain a temporal advantage over the adversary, superiority in the AI field will certainly prove to be a key factor.

Beyond the technical aspects, which fall outside the scope of this analysis, one of the most pressing questions for effectively harnessing this potential is how AI can be integrated into the planning process to ensure the ability to act effectively first.

While prior research has emphasized the benefit of AI's role in military planning processes, weaknesses remain in understanding how to implement it, accounting for the inherent uncertainty of war, avoiding overreliance, and eluding predictable results.[5] This research investigates the integration of AI into MDMP, emphasizing the need for speed while acknowledging the inherent uncertainty of war, commonly referred to as the "fog of war." The study addresses the central problem that while AI can enhance decision-making efficiency, war cannot be reduced to purely mathematical estimates, as demonstrated by historical blunders such as Robert S. McNamara's body count strategy or the "insurgency math."[6]

Aiming to achieve this objective, the investigation follows a multidisciplinary path, integrating insights from military history and theory, philosophy, epistemology, and technology, and unfolds across four analytical phases: first,

establishing theoretical foundations through examination of Clausewitzian principles and historical precedents of quantitative military analysis; second, analyzing the technical capabilities and inherent limitations of contemporary AI systems, particularly machine learning risks of overfitting and opacity; third, conducting a detailed case study examination of the experimental COA-GPT system as a representative example of AI-MDMP integration; and lastly, proposing specific recommendations for further AI-MDMP development and advocating for the renovation of our Services through the doctrine, organization, training, material, leadership, personnel, facilities (DOTMLPF) framework, to ensure that AI is employed as a tool rather than a definitive decision maker, with human judgment remaining indispensable to leverage its tactical advantages while avoiding blind dependence on its outputs.

Deductive and Inductive Reasoning for Predicting Future Outcomes

To set the foundation of this research, it is essential to first reflect on the lessons, frequently cited yet often forgotten, that Carl von Clausewitz offers in his most renowned work on the reliability of numbers, which is as nightmarishly complex and bizarre as Kafka's works.[7] James Willbanks, director of the Department of Military History at the U.S. Army Command and General Staff College, humorously recounted that in 1967, some Pentagon officials ventured into the building's basement, where the computers were located. With great enthusiasm, they began inputting everything quantifiable into punched cards: numbers of ships, tanks, helicopters, artillery pieces, machine guns, and even ammunition. After feeding all this data into the "time machine," they posed the crucial question: "When will we win in Vietnam?" They then left for the weekend, confident that they would have an answer by Monday. After their return, they found a card in the output tray that stated, "You won in 1965."[8]

Although this is merely an old, apocryphal tale, the anecdote recounted by Willbanks reveals how humanity's relentless quest to simplify the complexity of the world into universal laws can lead to an excessive oversimplification of reality, increasing the risk of erroneous predictions.[9] This risk is inherent in inductive reasoning, which, starting from specific premises, seeks to arrive at general conclusions. Unlike deductive reasoning, however, these conclusions can never be deemed entirely certain, even when experience suggests otherwise.[10]

Far from discrediting one reasoning process over the other, it is necessary to highlight that, in the military domain, both deductive reasoning (e.g., studying adversary doctrine) and inductive reasoning (e.g., analyzing recent enemy operations) form the foundation of military intelligence.[11] These methods are essential for predicting an adversary's future actions and supporting a commander's decision-making process. However, the limitation of such predictions is that

they rely solely on past experiences, making them unable to anticipate when or how an adversary might act unconventionally or irrationally, especially given the constant need to adapt to evolving situations.[12]

Consider, for example, Sir B. H. Liddell Hart's analysis of Germany's mobile offensive operations beginning in 1939 (the so-called blitzkrieg) or Eliot A. Cohen and Phillips O'Brien's discussion of Ukraine's fierce resistance against Russia's invasion in February 2022.[13] Both cases illustrate the unpredictability of such events, emphasizing the inherent limitations of rationalization in fully grasping future actions.

The Often-Forgotten Principles of Clausewitz

The observations above emphasize Clausewitz's argument regarding the limitations of doctrine as a theory based exclusively on past historical events, cautioning against using it as a universal model for the art of war in all conditions. Rather, it should be a tool for educating the minds of future commanders, fostering their judgment and intellectual instinct, without reducing warfare to a fixed mathematical formula. Furthermore, Clausewitz continues his critique of rigid rules and fixed schemes based on material factors by outlining three principles that illustrate how such frameworks merely oversimplify reality.[14]

First, he emphasizes the uncertainty of war and critiques the superiority of numerical strength as a metric for success. Such a mechanical simplification neglects key factors such as the enemy's reactions, moral elements such as courage and the will to fight, and the commander's role.

Second, Clausewitz highlights the positive reaction, defined as the uncertainty stemming from the reciprocity of actions between two opponents. This principle underscores that the effects of our actions, as well as those of the enemy, cannot be predicted with certainty and should not rely merely on theoretical assumptions. This concept is further validated by one of the major trends—now almost a constant—outlined by Wayne P. Hughes in his work *Fleet Tactics and Naval Operations*. Hughes asserts that the effectiveness of weapon systems is consistently overestimated before their actual use in conflict.[15]

Finally, Clausewitz underlines the uncertainty of information, which is often unreliable or incorrect, arguing that chance and talent play a crucial role in mitigating these uncertainties. Considering the tragic consequences of the Japanese attack on Pearl Harbor or the Battle of Goose Green during the Falkland Islands War, both events illustrate how flawed intelligence can significantly influence the outcome of a battle.[16]

Although these limitations may seem self-evident, they are frequently overlooked in the face of humanity's intrinsic desire to identify a logical process based on statistics, metrics, and models to address a problem and devise a rational solution with rigorously predetermined probabilities of success. One of

the most notable examples of this mindset is linked to McNamara's tenure as U.S. Secretary of Defense from 1961 to 1968. His technocratic and rationalist approach had catastrophic consequences for the Vietnam War.[17] However, while McNamara later expressed regret for his role, acknowledging in his 1995 memoir *In Retrospect: The Tragedy and Lessons of Vietnam* that the war was "wrong, terribly wrong," critics have noted that this contrition was limited and delayed.[18] Many observers argue that McNamara's reflections often downplayed personal responsibility, framing errors as honest mistakes amid complex circumstances rather than recognizing the human cost of his policies.[19] This partial remorse underscores the enduring tension between technocratic decision-making and the profound, tragic realities of warfare.

The Analytical Approach and Its Contradictions

After his appointment as secretary of defense by President John F. Kennedy, McNamara faced the challenging mission of introducing order and rationality to a fragmented Department of Defense bureaucracy marked by internal conflicts. Leveraging the expanded powers granted to the Office of the Secretary of Defense by the 1958 Defense Reorganization Act, McNamara took decisive steps to assert control over the Pentagon. One of his most significant initiatives was the implementation of the Planning, Programming, and Budgeting System (PPBS), a model inspired by managerial processes at Ford, where he had previously worked. As described in the contemporary publication *How Much Is Enough?: Shaping the Defense Program, 1961–1969*, edited by Alain C. Enthoven and K. Wayne Smith, the PPBS represented an innovative approach.[20] It organized the department's budget around functional objectives tied to specific missions, thereby integrating strategic planning with financial planning. Additionally, the introduction of systems analysis enabled comparative evaluation of various programs, assessing their relative effectiveness in achieving similar operational goals and attempting to reduce uncertainties through scientific analysis. This reorganization aimed not only to optimize resources but also to create a more rational and coherent decision-making structure.

However, the Vietnam War exposed the limitations and contradictions of this methodology. In a war where territorial control, distances covered, or cities occupied held little significance, the enemy's body count emerged as a seemingly more compelling metric of progress and success.[21] This system, based on calculations, charts, and statistics, produced two unintended effects. At the tactical level, units deliberately exaggerated enemy casualty figures while minimizing their losses to appease superiors.[22] At the strategic level, this approach proved inadequate in measuring the Viet Cong's determination to achieve their objectives.[23] The futility of this method was later confirmed by General Douglas Kinnard's historical essay, *The War Managers*, which revealed that only 2 percent

of American commanders considered body count an effective metric for measuring success.[24]

The consequences of McNamara's hyperrational approach, transplanted from the economic sphere to the military domain, underscore how Clausewitz's first and third principles remain unchallenged. On the one hand, mere numerical comparisons of strength fail to account for the moral elements essential in conflict, rendering them ineffective as predictors of victory. On the other hand, the fallacy of numerical metrics becomes exponentially greater when the numbers themselves, such as the Viet Cong body count, are derived from flawed or manipulated information.[25]

The contradictions of this approach are even more apparent in counterinsurgency (COIN) operations. As Jon Krakauer notes in *Where Men Win Glory: The Odyssey of Pat Tillman*, the Pentagon relied on quantitative indicators such as insurgent body counts, completed operations, or secured objectives to monitor progress in the wars on terror in Iraq and Afghanistan.[26] According to Krakauer, this methodology demonstrates McNamara's enduring legacy and the continued reliance on numerical metrics within military and political organizations. Beyond the oversimplification inherent in reducing war to a mere spreadsheet, this system, as David Kilcullen argues in *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One*, ignores critical factors such as local population support ("hearts and minds"), governance capacity—both military and civilian—and the sustainability of operations over time.[27] Moreover, this quantitative criterion fails to link tactical objectives with strategic goals, or, in other words, to establish a coherent process between ways, means, and ends.[28] As a result, it often produces overwhelming tactical victories but fails to achieve the desired end state.[29]

Despite recognizing the fallacy of tightly controlling the relationship between allocated resources and performance expectations (translated into mere numbers), military culture remains deeply entrenched in this mindset. As Edward N. Luttwak observed in his 1984 work, *The Pentagon and the Art of War: The Question of Military Reform*, he reflected: "Much of what went wrong in Vietnam belonged to the time and place, but much derived from military institutions that have not yet been reformed . . . and that continue to fail in converting manpower and money into effective military power."[30]

The Use of Metrics in Planning

Far from condemning the use of metrics, force ratios, and mathematical calculations, the ongoing debate over their effectiveness remains unresolved.[31] In *War by Numbers: Understanding Conventional Combat*, Christopher A. Lawrence, drawing on a database of 752 battles fought between 1904 and 1991 and the exemplary theories of Colonel Trevor N. Dupuy (the Quantified Judgment

Figure 1. Depuy's combat power equation

P= (S x Vx CEV)	P = Combat Power S = Force Strength V = Environmental and Operational Variable Factors CEV = Combat Effectiveness Value

Source: Shawn Woodford, "Dupuy's Verities: Combat Power =/= Firepower," Dupuy Institute, 12 May 2019.

Model), underscores the utility of metrics such as force ratios, rates of advance, and casualty estimates in determining the outcome of battles. Even Clausewitz, in chapter 8 of book III of *On War*, affirms that "in tactics, as in strategy, superiority of numbers is the most common element in victory."[32] However, it is essential to note that this superiority should not be understood in absolute terms but rather in relation to the concentration of a superior force at a decisive point. Both Dupuy and Lawrence, however, identify numerous other factors influencing the conduct of military operations, thereby advocating for a comprehensive analysis. Elements such as morale, training levels, motivation, cohesion, surprise, logistical organization, and the adaptability of commanders and units play a critical role in determining the outcome of combat. These elements contribute to what Dupuy terms *quality of troops*, now more commonly known as *combat effectiveness*.[33]

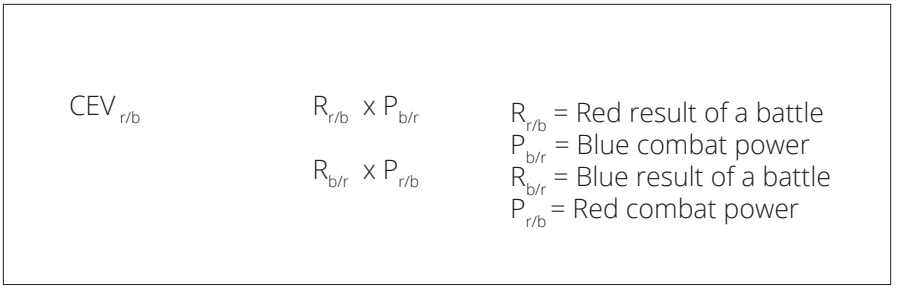
Combat Effectiveness: A Complex and Intangible Factor

Depuy described combat effectiveness (CEV) as the sum of "the intangible behavioral or moral factors of man that determine the fighting quality of a combat force."[34] These factors are meticulously categorized into leadership (encompassing training, experience, logistics, and other multipliers), disarticulation factors (such as surprise, suppression, culmination point), force quality (interpreted as relative combat effectiveness, morale, cohesion, fatigue, and trends over time), and the relationship between physical and moral factors (such as friction, defensive posture, momentum, and luck).[35]

However, as noted by Lieutenant Colonel Z. Jobbagy (Hungarian Defence Forces) in his analysis of fighting power, the "frustrating intangibility" of these factors and the inherent difficulty in quantifying them prevent us from relying on these variables for the effective prediction of battle or campaign outcomes.[36]

Even from a purely mathematical perspective, the attempt to accurately measure CEV and incorporate it into a new "square law," adapted from

Figure 2. Depuy's combat effectiveness equation



Source: Gerhard Geldenhuys and Elmarie Botha, "A Note on Dupuy's QJM and New Square Law," *ORiON* 10, nos. 1–2 (1994): 45–55, https://doi.org/10.5784/10-0-455.

Lanchester's celebrated equations and revised by Dupuy, has been called into question by the Operations Research Society of South Africa (ORSSA).[37] Researchers from the society's Department of Applied Mathematics, after identifying mathematical discrepancies in Dupuy's formula for calculating CEV, argue that "even though Lanchester's theories have been significantly developed and are often used in war games, there are serious doubts about their potential application in real battles."[38]

The Debate on Metrics, Mathematical Models, and the Dynamic Approach

The discussion on the effectiveness of metrics and mathematical models continues with the introduction of a dynamic approach, such as the one developed by Joshua Epstein in 1985.[39] Epstein's model, designed to provide a valid alternative to static analysis for assessing NATO's resource allocation effectiveness during the Cold War, is based on the premise that combat is "a process whose course and outcome depend on factors that cannot be captured in a simple beans count."[40] Among these factors, he lists elements such as "technology (weapon quality); troop training and skills; command, control, communications, and intelligence (C3I); logistics; relative concealment and exposure (use of terrain); ally reliability; readiness; surprise; and the relative willingness to endure attrition and concede territory."[41] To support his argument, Epstein also turns to historical examples, citing battles and campaigns such as Austerlitz (1805), Antietam (1862), the invasion of France (1940), Operation Barbarossa (1941), and Kursk (1943), highlighting how victory can smile even upon those who, under analysis, appear numerically inferior.[42]

Despite its innovative nature and detailed mathematical analysis, Epstein's model has not been immune to criticism. A 1988 publication edited by the U.S. Congress implicitly affirmed the validity of the aforementioned properties

enunciated by Clausewitz, stating: "There are questions about the equations used in the models, whether the model or scenario is biased in favor of or against a particular faction, and the sensitivity of the model to different assumptions."[43] The publication further noted:

> Epstein's model, like any quantitative method for assessing the relationship between two military forces, cannot be used to predict the outcome of a real conflict. No mathematical model, even one attempting to capture the dynamics of war, can replicate all the factors that determine the course of a battle. Some factors that have a significant impact on the outcome of a clash, such as leadership, morale, and tactical competence, cannot be quantified.[44]

Clausewitz's theories and the U.S. Congress's conclusions are further reinforced by the observations of Russian writer and philosopher Leo Tolstoy. In his celebrated work, *War and Peace*, Tolstoy illustrates the complexity, unpredictability, and apparent disconnect between the theory and practice of war through the eyes of those who lived it. Tolstoy, employing a skillful analogy with the game of chess, critiques the rationalistic and deterministic vision of war, underlining how human beings strive to impose order and logic on phenomena that are inherently chaotic and uncertain.[45]

Unlike chess, where the player has a sense of control over events thanks to the complete visibility of the board and its fixed rules, Tolstoy argues that the reality of war introduces numerous unpredictable variables: chance, human emotions, confusion, and the will of combatants. These factors render the claim of total control futile and illusory. Through this comparison, Tolstoy also seeks to diminish the central role often attributed to commanders, who are frequently regarded as the sole architects of decisive victories.[46] He argues that their success is not uniquely dependent on their skill but rather on a network of uncontrollable circumstances and factors, such as the contributions of soldiers, weather conditions, and sheer luck.[47] In other words, Tolstoy asserts that war cannot be reduced to an ordered game like chess but remains an anarchic and chaotic phenomenon where human control is limited.

The discussion thus far allows us to grasp the inherent risks of inductive reasoning—when one attempts to derive a general rule (a mathematical equation) from a particular phenomenon (a specific battle). This risk is further amplified by the heuristic methods employed to formulate mathematical equations for force ratios, which aim to predict and "control" the outcome of a future event using procedures that are not rigorous and whose validation will always remain uncertain.

On the other hand, as previously emphasized, the use of metrics and mathematical equations in the military domain remains indispensable. They are in-

valuable tools for planning the forces to be assigned to specific tasks, helping us determine whether they are proportionate to them and identifying any associated risks. However, to borrow Epstein's words, mathematical models must remain solely a force-planning tool, for which "depictive realism and precision are not absolutely necessary."[48] These models should not cross the feeble line into our unconscious desire to predict an outcome, even though such prediction is not "definitively and eternally precluded."[49]

The Final Frontier of Inductive Reasoning: Artificial Intelligence

The principles of inductive reasoning and their inherent limitations, along with those of metrics based on historical data and heuristic methods previously examined, provide a foundation for introducing what is arguably the most significant technological revolution of our time—AI. According to IBM, AI is defined as "a collection of systems or machines that imitate human intelligence to perform tasks and are capable of iteratively improving themselves based on the information they collect. Applications of AI include natural language processing, image recognition, and the prediction of future events through data analysis."[50]

To fully understand both the potential and the risks associated with the use of AI and its most advanced stage of development, generative AI (GenAI), it is essential to analyze the models upon which these technologies are based. These models include machine learning (ML) and deep learning (DL).

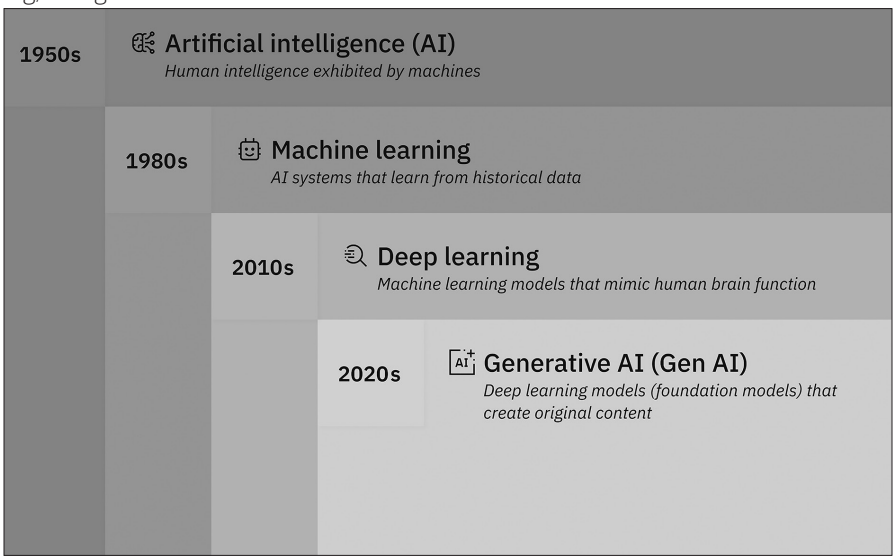
Machine learning refers to the development of algorithms that enable computers to learn from input data and to improve their performance over time without being explicitly programmed for specific tasks.[51] In other words, by analyzing large volumes of data, machine learning systems are capable of identifying recurring patterns and harnessing this information to make decisions or produce predictions.

Deep learning, on the other hand, is a subfield of machine learning that relies on multiple layers of artificial neural networks.[52] The term *deep* refers to the use of numerous layers that allow for the modeling and interpretation of complex data. These deep neural networks are inspired by the structure of the human brain and are particularly effective in processing unstructured data such as images, audio, and text. This architecture enables models to learn hierarchical representations of data, beginning with low-level features and advancing to increasingly abstract and complex concepts.[53]

The Primary Risk of Machine Learning: Overfitting

The use of the aforementioned models, which are fundamental to the learning process of AI, highlights the profound distinction between AI systems and conventional computing. While traditional software works by following fixed

Figure 3. Correlation between artificial intelligence, machine learning, deep learning, and generative AI



Source: IBM.com, adapted by MCUP.

instructions explicitly programmed by humans to convert specific inputs into predetermined outputs, artificial intelligence systems use algorithms designed by humans that enable the system to learn from data and improve over time. Instead of relying solely on predefined rules, AI autonomously builds internal models that map inputs to outputs, allowing it to adapt and handle new situations without explicit reprogramming. Subsequently, AI systems continue to learn through iterative processes involving trial, error, and feedback provided by human developers, thereby reconfiguring internal mappings and the connections among acquired data.[54]

The principal risk associated with this learning process is that AI's neural networks may resort to memorizing responses rather than genuinely learning the underlying principles. This phenomenon, often referred to as the "parrot effect," has been effectively illustrated in an interview conducted by Alexandre Piquard with linguist Emily Bender.[55]

From a technical perspective, this issue is known as *overfitting*, which refers to a model's failure to generalize due to the limited size of the training dataset. Such datasets often lack enough examples to accurately represent the full range of possible input values. As a result, the model's predictions become highly sensitive to variations in new data, leading to unstable and unreliable behavior. This significantly reduces the model's usefulness in complex or real-world scenarios.[56]

In an attempt to provide a simple example illustrating the risks associated

Table 1. Example of overfitting

Weight (g)	Price ($)
100	1.00
150	1.50
200	2.00

Source: courtesy of author, adapted by MCUP.

with overfitting, let us consider a small dataset containing information on the prices of a given product as a function of its weight (table 1).

A model not affected by overfitting would identify a simple relationship, such as:

Weight/100 = Price

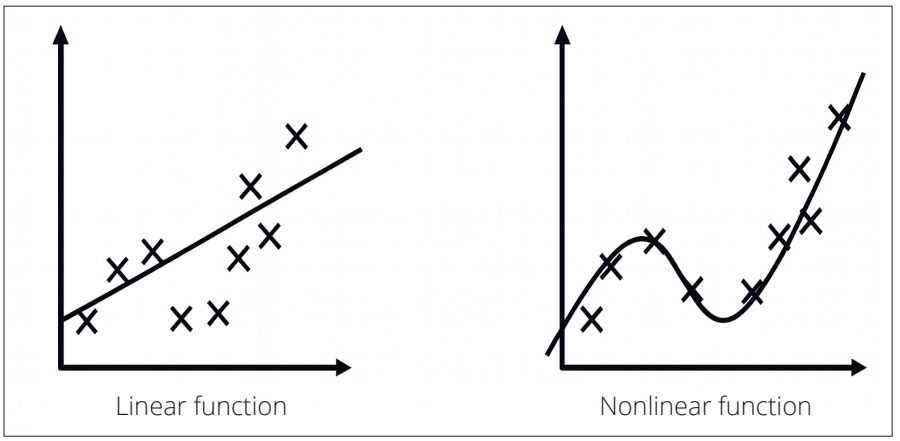
By contrast, a model affected by overfitting would attempt to fit the training data perfectly, producing a complex curve that passes exactly through the given points like a parabola. Although this approach may perform well on the specific dataset used for training, it would likely fail to generalize. For instance, when presented with a new input (e.g., a product weighing 120 grams), the model might produce an inaccurate prediction due to its excessive sensitivity to the original data.

Moving to the military field, a constant in the history of naval warfare says, "Firepower is less effective than anticipated from peacetime tests and firing exercises."[57] Overfitting in AI systems has the same limitations, as algorithms can perform well on training data but may not generalize accurately to the complex and dynamic environments of a real battlefield.[58] Overfitting leads to brittleness, where AI systems are unable to adapt to novel battlefield conditions, resulting in erroneous target identification or misclassification that can have fatal consequences, such as striking friendly forces, civilian objects, or misidentifying combatants.[59] This is exacerbated by the scarcity of high-quality, diverse training data and the use of synthetic or biased datasets, which can embed systematic errors into decision-making processes.[60] Furthermore, overfitting contributes to the following "black box" risk, where AI decisions lack transparency and explainability, undermining human trust or prompting overreliance in high-stakes contexts.

The Second Risk of Machine Learning: The Black-Box Problem

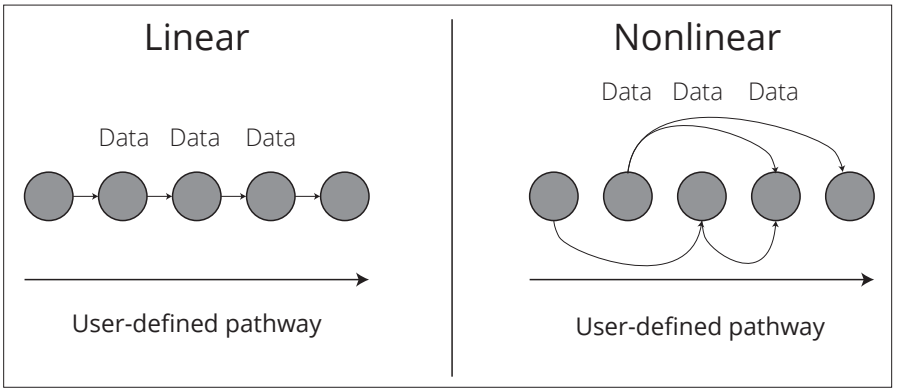
The second major risk associated with the learning models underpinning AI arises from the use of nonlinear regression to represent relationships between

Figure 4. Linear versus nonlinear regression



Source: Medium.com, adapted by MCUP.

Figure 5. Linear versus nonlinear regression network



Source: courtesy of author, adapted by MCUP.

input variables. Nonlinearity implies that the relationship between a dependent variable and an independent variable is neither proportional nor constant. This allows models to capture and represent multiple complex relationships that would be difficult to identify through linear approaches. As a result, AI systems can construct more realistic and accurate representations of data, thereby enabling the resolution of complex problems with greater precision.[61]

However, the intrinsic nature of nonlinear processes introduces what is commonly referred to as the black-box problem, wherein the internal decision-making mechanisms of the AI are not readily interpretable by human observers. In other words, while the algorithm can generate an output, such as a prediction or a classification, it does not make transparent the reasoning or path by which that output was reached.[62]

Table 2. Results of Capaccioni's research about the reliability of bibliographies generated by AI

ChatGPT 3.5		Bard	
Correct quotation/ argument	2	Correct quotation/ argument	4
Incorrect quotation/ argument	8	Incorrect quotation/ argument	6

Source: Andrea Capaccioni, "Sull'affidabilità delle bibliografie generate dai chatbot. Alcune considerazioni," *AIDAinformazioni*, nos. 1–2 (January–June 2024).

In the distinguished work *Genesis: Artificial Intelligence, Hope, and the Human Spirit,* Henry A. Kissinger emphasizes that, although the phenomenon is well known, it has not deterred millions of people from passively accepting the veracity of most outputs provided by AI. This acceptance stands in stark contrast to the principles of enlightened analytical reasoning. In our understanding of rationality, the legitimacy of certainty is grounded in its transparency, reproducibility, and logical validation. However, this principle vanishes in the opaque reasoning processes of AI. The risk, therefore, is that without a critical analysis of AI-generated outputs, "these new 'brains' could appear to be not only authoritative but infallible."[63]

A replicable experiment that demonstrates the fallacy of AI in providing accurate answers, while disguising false information with an authoritative and convincing tone, is to request citations or a bibliography on a specific topic. In many cases, as summarized in the results of a study conducted by Andrea Capaccioni, attempting to verify the requested citation or topic in the AI-provided bibliography will reveal the inaccuracies of the answers (table 2).[64]

The critical consequences arising from the combination of what is known as AI's Dunning-Kruger effect and the phenomenon of anthropomorphism, where humans are more inclined to trust responses from a humanized AI, are readily apparent. [65]

In the military domain, this risk will translate into potentially critical failures in decision-making processes where human operators rely on autonomous systems without a clear understanding of the underlying rationale. Tracing the premises already known from a previous investigation conducted by the Army Research Laboratory on autonomous agents in 2014, the black-box nature of advanced AI models means that commanders and soldiers may receive outputs, such as threat assessments, target identifications, or mission orders, that are not accompanied by transparent explanations of how those conclusions were reached.[66] This opacity can lead to misplaced trust or unwarranted skepticism, both of which impair effective collaboration between humans and machines. Without proper transparency, the ability to calibrate trust appropriately is com-

promised, increasing the likelihood of overreliance or disuse of automation, which in turn can degrade situational awareness and operational effectiveness. Given the high-stakes environment of military operations, where rapid and accurate decision making is crucial to addressing the black-box problem through enhanced agent transparency is essential to ensure that autonomous systems serve as reliable and comprehensible partners rather than inscrutable tools.

AI-Military Decision-making Process: The Future of Military Planning

In the purely military domain, AI has found numerous applications in recent years, sparking an arms race and technological innovation comparable to the nuclear arms race during the Cold War.[67] From autonomous weapon systems and intelligence, surveillance, and reconnaissance (ISR) to predictive logistics and recent advancements in cyber operations, AI permeates every domain and dimension of warfare.[68]

Regarding command and control, the implementation of AI has found fertile ground, particularly in enabling the effective conduct of distributed operations through the creation of a real-time, updated common operational picture, facilitating the targeting process.[69] The ultimate goal is singular: to accelerate the decision-making process of commanders and units to gain a cognitive advantage over the enemy, thus maintaining a favorable operational tempo.

The magnitude of this advantage is particularly evident when viewed in light of the theories of Colonel John R. Boyd, who, based on his experiences in aerial combat during the Korean War, theorized that it is the speed at which the human brain processes information and makes decisions that largely determines who wins or loses a battle or war. According to his theory, victory or defeat is not determined by the performance of a weapon, but by the speed of a continuous cycle of observation, orientation, decision, and action (the OODA loop).[70]

The overwhelming force of the technological revolution brought by AI now seems to break the final barrier of what was once considered a strictly human domain: the tactical level of operations planning. From studies on the automation of intelligence preparation of the battlefield (IPB) to the vision of semiautonomous future command posts, military AI developments continue to work toward an effort to automate the entire MDMP.[71]

As skillfully analyzed by Colonel Michael S. Farmer, the primary objective remains the development of "the ability to understand and react first in a dynamic environment capable of rapidly invalidating previous plans, which will be essential to seizing and retaining the initiative."[72] This ability would manifest in the semiautonomous execution of the entire MDMP, evaluating continuous updates of the current situation, selecting the best course of action (COA) based on it, and anticipating the execution of potential branch plans.

AI-Military Decision-making Process: The COA-GPT Case

A concrete initial attempt to automate the decision-making process by autonomously developing a COA through the use of an algorithm employing large language models (LLMs) is currently under study at the U.S. Army Combat Capabilities Development Command (DEVCOM) Army Research Laboratory.[73] This algorithm, named COA-GPT, appears to be capable of analyzing all mission variables provided by a commander and their staff (inputs) and subsequently proposing a COA (output) that aligns with those from higher levels and can adapt to human feedback. Once the COA is approved, the algorithm will conduct a simulation and performance analysis, evaluating outcomes through objective metrics such as rate of advance and friendly and enemy casualties. This process highlights a human-centered paradigm, where the commander retains decision-making control while benefiting from the speed, adaptability, and creativity of the AI system. The LLM does not merely provide options; it enables the tactical co-creation of the plan.

To fully grasp its potential, it is necessary to first explore the concept of LLMs. These can be defined as artificial systems capable of acquiring linguistic competencies through training on vast amounts of data. During their large-scale learning phase, the models do not store individual facts but rather learn linguistic patterns, such as word co-occurrences, syntactical construction of sentences, and conceptual relationships between terms. Through the repeated application of this process on a massive scale, the model develops the ability to generate coherent text, answer questions, and create content with linguistic characteristics very similar to human expression.[74]

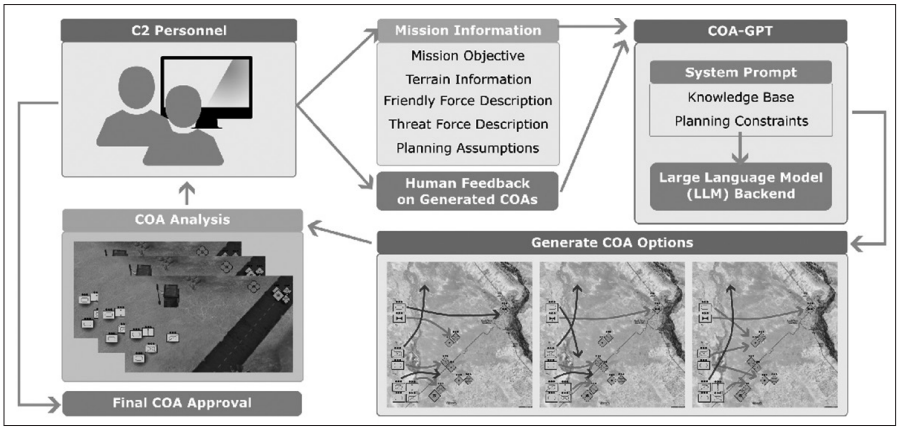
Their architectural structure is based on the Transformer, a layered model that analyzes each word in relation to all others within the textual context, without relying on sequential reading. In other words, the system does not simply read from left to right but understands connections between even distant words within a sentence or context.[75]

In the case of COA-GPT, LLMs previously trained with military doctrine knowledge are used to receive a prompt containing operational information provided by the commander or their staff in the form of text and images, which will then be analyzed by the artificial system. Subsequently, the LLM's ability to interpret free text and images, combined with the assimilation of military doctrine, will enable COA-GPT to simulate tactical reasoning without the need for specific training for each scenario and to modify its outputs in real time based on human feedback.[76]

COA-GPT and the Use of Metrics

The use of quantitative metrics to assess the quality of COAs generated by

Figure 6. Linear versus nonlinear regression network



Source: Vinicius G. Goecks and Nicholas R. Waytowich, "COA-GPT: Generative Pre-Trained Transformers for Accelerated Course of Action Development in Military Operations," *2024 International Conference on Military Communication and Information Systems* (Brussels, Belgium: North Atlantic Treaty Organization, 2024): 1–10, https://doi.org/10.1109/ICMCIS61231.2024.10540749.

COA-GPT represents one of the central elements of the project, but at the same time, it constitutes one of its most critical and delicate areas.

The system evaluates each course of action based on three primary metrics:

1. **Total Reward**: a score that assigns positive values (+10) for the elimination of enemy forces or the seizure of key terrain, and negative values (-10) for the loss or retreat of friendly units.
2. **Friendly Force Casualties**: the total number of friendly units lost.
3. **Threat Force Casualties**: the losses inflicted on the enemy.

At first glance, this approach allows for an objective and comparable evaluation of the different COAs generated, creating a feedback system beneficial both to the machine and to the human commander. However, these metrics present structural limitations that echo historical problems previously discussed.

In the same way that McNamara's body count metric became problematic, the Threat Force Casualties metric adopted in COA-GPT, if isolated or decontextualized, risks replicating the same illusion.[77] A COA that eliminates the highest number of enemies may seem optimal, but it could simultaneously leave out a more favorable form of maneuver (such as penetration, encirclement, or envelopment), which exploits the enemy's gaps and avoids unnecessary attrition, undermines the legitimacy of friendly forces, causes unmeasured collateral damage, and results in a tactical victory but a strategic defeat

A comparison between COA-GPT and the more recent insurgency math

used during the Global War on Terrorism in Iraq and Afghanistan highlights further limitations. The metrics adopted fail to include any measure of the informational domain, the enemy or civilian population's will, the perception of success by the actors involved, or the long-term consequences.[78]

Furthermore, returning to the theories put forward by Clausewitz and Depuy, these limitations demand greater reflection on the future developments of an AI-MDMP. As it stands, it is possible to argue that the Clausewitzian "friction" is completely absent from COA-GPT's metrics. The scores assigned within the system presume a perfectly observable and entirely deterministic world, where every action has a clear and measurable effect.[79] While this approach may be useful in a simulated environment, it violates the fundamental Clausewitzian principle of the "fog of war," excluding the human element of uncertainty, risk, and intuition that is central to the reality of combat.

Finally, returning to Depuy's model, which sought to translate military interaction into a mathematical function, the oversimplification of battle and the predictive fallacy become even more evident. The metrics adopted in the COA-GPT algorithm show disturbing conceptual analogies with the Depuy approach:

1. Total reward is an algebraic sum of kinetic events such as bridge crossings, enemy eliminations, and casualties sustained.
2. Friendly or enemy casualties are mere numerical counts, disconnected from any qualitative consideration (e.g., the symbolic value of a loss or the loss of a leader).
3. The analysis is based on repeated rollouts in simulated environments, which, though diversified, do not introduce structural uncertainty or friction.

In other words, the current system risks confining military planning to an engineering logic, where victory seems to favor those who optimize best, yet loses sight of the Clausewitzian essence of war as a domain of chance, will, and commanders' insight (table 3).

In conclusion, Clausewitz, DePuy, and the metric failures of the past teach us that war is an open, complex system that cannot be reduced to absolute numbers. COA-GPT, despite its technical brilliance, still exhibits a closed ontology, where the model assumes to know the exact position of every unit, assigns absolute and symmetric value to losses, and operates in an environment free from friction or informational distortion. This brings us back to two inherent risks in AI, which were discussed earlier. On the one hand, there is the risk of tactical overfitting, where the algorithm generates perfect COAs for the simulated world, but they are not transferable to the real world. On the other hand, there is the false illusion of objectivity and control for decision makers, leading commanders and staff to underestimate what cannot be quantified.

Table 3. Comparative analysis of aspects related to the art and science of war

Aspect	Clausewitz	DePuy	COA-GPT
fog of war	central	ignored	ignored
friction	inevitable	absent	absent
qualitative parameters	fundamental	secondary	excluded
human context	dominant	marginal	absent
quantitative output	secondary	primary	primary

Source: Courtesy of author, adapted by MCUP.

AI-Military Decision-making Process: Advantages and Opportunities

Despite the limitations of the current development of AI-MDMP, it certainly offers significant advantages and opportunities for maintaining a favorable operational tempo over the enemy. If the opposite were true, the rapid adoption of AI in the Russian-Ukrainian conflict and in strategic initiatives—such as the United States' Project Maven and Russia's command-and-control (C2) programs—would defy comprehension. Project Maven's operational success demonstrates this in practice: brigades equipped with the AI-powered system achieved targeting performance comparable to the 2003 Iraq War using only 20 soldiers instead of 2,000.[80] Russia is pursuing similar objectives: according to the Saratoga Foundation, Russia's 27th Central Research Institute is working on an automated command systems able to analyze intelligence data, generating battle plans while also finding the best variants for a specific situation, based on self-teaching.[81]

Indeed, one of the greatest advantages of COA-GPT is the drastic reduction in the time required to generate, analyze, and compare different COAs. Traditionally, the COA development phase in the MDMP takes hours, if not days, especially in complex and multi-domain environments. COA-GPT can produce valid COAs in just seconds, enabling almost immediate responses to battlefield changes. This results in a drastic reduction of the OODA loop and the overcoming of potential cognitive limitations of the human staff, allowing action to be taken before the enemy can react.

Moreover, it is important to consider that a human commander and their staff can typically evaluate two or three COAs due to time and resource constraints. A system like COA-GPT can generate dozens of alternative COAs from the same initial configuration, each with a different maneuver structure, axis of effort, tactical risk, or fire priority. This ability to explore solutions is a crucial advantage in complex environments, enabling a broader comparative

assessment by the staff and leading to the selection of the COA most aligned with the commander's intent.[82]

Additionally, the incorporation of military doctrine into the prompts of COA-GPT ensures that the generated COAs align with standard operational principles, reducing reliance on the training or experience of individual planners. This automation standardizes the quality of the outputs, even under conditions of limited time, high stress, or varying professional backgrounds.

Finally, the reduction of the cognitive and logistical load on staff officers is a practical, significant advantage. In contested or degraded environments, where command posts must be distributed, mobile, or temporary, an automated MDMP helps reduce the amount of personnel needed while still maintaining a high level of planning capability. In modern warfare scenarios characterized by rapid movements, cyber disruption, and dynamic targeting of decision-making centers, this feature can ensure the survival and continuity of C2 operations.[83]

Proposing COA-GPT 2.0: An Architecture for the Uncertainty of War

The application of AI to the MDMP holds extraordinary potential, but its ultimate usefulness will depend on how well we guide its evolution with a strategic vision that accounts for operational needs, human cognitive limits, and the deep nature of warfare.[84]

For a system like COA-GPT to genuinely contribute to a battlefield decision-making advantage, it is essential to address and overcome some structural challenges. First, the architecture of the model itself must be rethought. COA-GPT 2.0 will need to incorporate uncertainty, not just as a technical variable, but as an essential element of the combat experience.[85] This requires the integration of probabilistic and dynamic models capable of representing the partiality of information, the fog of war, the ambiguity of sources, and operational friction.[86] Using models such as partially observable Markov decision processes (POMDPs), Bayesian networks, and Monte Carlo simulations can allow the system to generate COAs that are not evaluated based on absolute and deterministic scores, but accompanied by confidence estimates, risk intervals, and probabilistic assessments.[87]

At the same time, it will be crucial that the system does not propose rigid plans but adapts in real time to new information and human feedback, even during the execution of the COA. One of the structural limitations of COA-GPT is the discrete command mode, where the system assigns a single order to each unit at the start of the simulation, with no possibility of dynamic intervention during the scenario.[88] While this approach is perfectly compatible with top-down planning logic, it becomes problematic in dynamic operational environments where conditions change rapidly.[89] In the simulated environment

of *StarCraft II*, reinforcement learning-based methods continuously update commands based on evolving tactics, whereas COA-GPT lacks this reactivity. The result is increased vulnerability to change, as evidenced by the higher rate of friendly force casualties compared to more granular control methods.

This limitation could be addressed by adopting a continuous planning logic with rolling time windows, transforming COA-GPT into an "always-listening" assistant during execution. This could be integrated with current C2 systems: Command Post of the Future (CPoF), Android Team Awareness Kit (ATAK), and Joint Operations Center Watch (JOCWatch), or a compromise between discrete control and dynamic autonomy could be adopted through preplanned contingency rules that enable predictive reactivity.[90]

In conclusion, by introducing these dynamic and flexible capabilities, a COA-GPT 2.0 could better reflect the unpredictability of warfare, enhancing its practical utility while also aligning with the inherent uncertainty and complexity that Clausewitz described.

A Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities (DOTMLPF) Approach for the Way Ahead

To ensure a meaningful and responsible integration of AI into the MDMP, a comprehensive analysis across the DOTMLPF framework is required. This evolution must achieve technological enhancement to include fundamental cultural and procedural changes across our Services. Beyond the proposals presented here, which remain subject to revision in light of future research, the ultimate objective must be the development of an effective human–machine team (HMT). This concept rests on overcoming the long-standing debate over the primacy of humans versus machines, thereby paving the way for new levels of cognition, which is defined by General Brigadier Yossi Sariel (IDF) as "supercognition."[91] The latter can indeed be achieved only through the synergistic integration of human and artificial intelligence: while machines are unsurpassed in the analysis of large volumes of data and rapid decision making, we have seen how they remain limited when it comes to addressing uncertain contexts, managing singular events characteristic of warfare, confronting ethical dilemmas, or creatively adapting to novel and uncodified situations. Conversely, humans, despite representing the bottleneck in stages requiring massive computational processes, are indispensable for defining the overall meaning of operations, navigating friction, and managing uncertainty, because "war is the realm of uncertainty" and the battlefield landscape continuously evolves.[92] Therefore, only the genuine collaboration between computational capabilities and human judgment can ensure an effective and adaptive approach capable of providing a real advantage over adversaries.

Doctrine must be updated to formally incorporate AI systems as a core element of MDMP. This entails a clear delineation of roles, responsibilities, and the creation of effective HMT architecture. First, AI must not be described as a decision maker but as a tool for generating, refining, and testing COAs. Second, the doctrine should outline commander responsibilities in validating, questioning, or rejecting AI-generated outputs, especially under conditions of moral ambiguity or when collateral risks are involved. Furthermore, doctrinal revisions must address ethical guidelines for AI use, the acceptable thresholds of risk and uncertainty, and protocols for contested interpretations between human and machine assessments. It must instill the principle that the human commander or operator remains ultimately responsible, with AI serving as an advisory component that requires constant critical scrutiny.[93]

Third, to mitigate the specific risk of overfitting within the doctrinal domain, it becomes essential to integrate granular human control mechanisms, defining precisely in which areas each type is to be applied. The implementation of the human-in-the-loop (HITL) and human-on-the-loop (HOTL) framework represents a fundamental doctrinal necessity to counter the algorithmic brittleness identified by Hoffman and Kim, addressing the challenge that AI systems "work well under ideal conditions but quickly fail in the face of unforeseen changes in the environment or malicious interference."[94]

HITL, characterized by deliberate and direct operator control over every critical AI decision, emerges as a doctrinal imperative in high-ambiguity operational scenarios, such as complex urban environments where the probability of misclassification is statistically elevated. Conversely, HOTL, which permits AI operational autonomy within predefined parameters while maintaining human supervisory and veto capabilities in real time, finds appropriate application in temporally constrained contexts such as anti-missile defense, where decision speed is critical for operational effectiveness. Doctrine must additionally incorporate principles of uncertainty quantification, requiring AI systems to provide quantitative measures of their decisional uncertainty, with predefined thresholds that automatically trigger escalation to human control when uncertainty exceeds critical parameters.[95] An advanced HMT architecture, as proposed by recent research, represents a paradigm shift from the traditional binary human control/machine autonomy approach toward an adaptive model that dynamically calibrates supervision levels based on situational complexity and algorithmic confidence. However, as mentioned earlier, the basic principle in creating a new architecture must be that "humans remain in command, not just in the loop."[96]

Organization must evolve by institutionalizing AI-integrated decision-making teams, where AI agents are effective active members.[97] These could be composed by commanders, military staff, data analysts, AI interface specialists,

and AI agents to ensure a rapid adaptation to the evolving situation.[98] Moreover, such multidisciplinary human-machine collaboration would facilitate the AI output evaluation and interpretation through both military judgment and technical understanding. These organizational changes should also establish internal feedback loops to track the performance of AI recommendations, enabling iterative improvement and trust-building between humans and machines.[99]

Moreover, to mitigate the specific risks of overfitting and data poisoning through organizational reforms, the systematic implementation of specialized AI red teaming units emerges as an indispensable structural necessity.[100] These organizational entities must operate through multidisciplinary approaches that combine machine learning expertise, operational field experience, and electronic warfare competencies to simulate multidimensional adversarial attacks and identify algorithmic cognitive vulnerabilities prior to operational deployment.[101] Research conducted by the Swedish Defence Research Agency demonstrates how adversaries can compromise AI system integrity through data poisoning, rendering red teaming a continuous process rather than a static predeployment verification.[102]

It is also appropriate to specifically mention how the command posts of the future should evolve. Drawing from the consideration of Benjamin Jensen, the military command structures in place today remain largely reminiscent of those established during Napoléon Bonaparte's era, despite two centuries of warfare evolution.[103] Contemporary staff have grown unwieldy, struggling to manage the broader and more complex battlespace that now includes cyberspace, outer space, and information domains. This expansion has led to diminishing returns in coordination and operational effectiveness, exacerbated by vulnerabilities to precision strikes and electronic warfare, as starkly evidenced by Ukraine's targeting of Russian command posts labeled the "graveyard of command posts."[104]

Jensen advocates that AI, in the form of autonomous, goal-driven agents powered by large language models, offers transformative capabilities that can address these structural inefficiencies. By automating routine staff functions such as integrating disparate intelligence inputs, modeling threats, and even facilitating limited decision cycles, AI agents promise to reduce staff sizes while accelerating decision timelines and enabling smaller, more resilient command posts.[105] Human operators remain essential for relevant decisions and ethical judgment, but AI augments their capacity to process vast information streams, generate diverse operational options, and focus on higher-level contingency analysis rather than administrative tasks.

Moreover, the envisioned Adaptive Staff Model, informed by ethnographic sociological approaches, integrates AI and human decision makers in continuous feedback loops, enabling dynamic plan adaptation in complex, Joint opera-

tional scenarios like those involving China-Taiwan contingencies.[106] This model contrasts sharply with static, hierarchical staffs and emphasizes flexible, iterative command rather than linear planning. However, Jensen also cautions against several risks already discussed: reliance on generalized AI models that may lack domain-specific accuracy, and the danger of complacency among human users who might substitute AI outputs for critical reasoning.

These considerations perfectly complement what is advocated by Jim Storr's insights from *Something Rotten*, as the imperative to rethink command structures aligns with his critique of bureaucratic inertia and overly complex decision making in modern militaries. Storr advocates for empowered, decentralized command with streamlined processes, a vision congruent with AI-enabled smaller, agile command posts.[107] Together, these perspectives suggest that military command structures must evolve from cumbersome, industrial-age organizations into adaptive, AI-enhanced entities that maintain human judgment while harnessing computational power and flexibility to survive and be effective in future conflicts. [108]

Training will be the decisive factor in this transformation. To establish an effective human-machine team, it is essential to initially train the individual parties and then their cohesive integration in a holistic manner. First, a commander or operator who lacks the ability to query, interpret, or critically engage with AI risks either overreliance or outright rejection. AI literacy must therefore become a core component of curricula in staff colleges, war colleges, and military academies.[109] Officers and specialists must be educated not only in how to operate AI systems but also in how these systems work.[110] To this end, it will be urgently necessary to proceed with a revision of the training plans of military schools, in alignment with the directives also highlighted by the White House's report, *Winning the Race: America's AI Action Plan*.[111]

Second, in addition to being directed toward commanders and AI system operators, training must also be extended to the system itself. As previously discussed regarding the risk of overfitting, it has been shown that this phenomenon may entail significant collateral effects in the context of military operations. To mitigate this risk, the AI system must therefore undergo dedicated training through the continuous and systematic integration of standard and mission-tailored datasets and adversarial examples, controlling the integration of synthetic data, and conducting rigorous validation against real-world data to prevent model collapse.[112]

Thirdly, and most importantly, it will be necessary to form the team. To create an effective team, as in a basic infantry unit, it is not sufficient merely to assemble individuals and equipment; rather, a specific training progression aimed at developing skills, cohesion, and mutual trust must be followed. These objectives may be pursued through the following concepts:

- **Learning** through synergetic learning, as a new process of mutual learning between humans and machines. By effectively combining the cognitive abilities of humans, which have driven global changes and transformations to date, with those of AI, which is potentially capable of analyzing every event from multiple perspectives, it becomes possible to achieve new and ambitious levels of analytical capability and inductive reasoning.[113]
- **Organizing** by introducing shared mental models (SMM) as a "pattern of cognitive similarity that enables them to anticipate one another's needs and actions and to synchronize their work in a way that is synergistic toward meeting the team's ultimate goals."[114] Introducing specific SMMs to define goals and processes, and outlining roles, tasks, and expectations, it is possible to improve cohesion and mutual trust by facilitating effective communication, reducing misunderstanding, and increasing predictability in interactions. It will lead to an overall increased HMT performance.[115]
- **Testing and evaluating** by conducting practical exercises, such as scenario-based COA testing with live troops, simulations, and wargaming. They will be the final critical events to validate AI-enhanced COAs and foster adaptive decision making, supported by specific benchmarks.[116] These exercises should include feedback mechanisms to assess not only outcomes but especially the quality of human-AI interaction and mutual trust.[117] Above all, as traditional training, the conduct of live force-on-force exercises, with both sides equipped with AI-enabled MDMP, could prove to be the decisive factor for success in real operations.[118] Only such scenarios will in fact make it possible to effectively test the system under conditions of uncertainty; enable the system to learn from real-world rather than synthetic data; assess the effectiveness of HMT by identifying situations of overreliance or insufficient use; and evaluate commanders' ability to manage the unpredictability of the operational environment, applying their "genius," and demonstrating the usefulness or otherwise of AI support.[119]

Materiel must support the integration of AI into operational planning, particularly by minimizing black-box risk. This includes user-friendly interfaces for commanders, real-time battlefield data integration, and visualization tools that enhance transparency in how AI systems arrive at their recommendations. Such tools should allow commanders to trace the logic and assumptions behind AI outputs and provide input to refine them. Moreover, these systems must support feedback collection to train future iterations of AI, creating a continual improvement loop between field experience and model refinement.[120]

Starting from the aforementioned Army Laboratory Research studies, their Situation Awareness-based Agent Transparency (SAT) model seeks to mitigate the risks associated with black-box systems by establishing three distinct levels of situational awareness.[121] The first level pertains to basic information such as the current state of the AI agent, and its goals, intentions, and proposed actions. The second level concerns the rationale underlying the agent's actions, as well as potential environmental or situational constraints that may impact its operation. The third level involves the AI agent's predictions regarding the consequences of its actions, including the likelihood of success or failure and the degree of uncertainty associated with those outcomes.[122] Drawing from the SAT, the current progress made by Defense Advanced Research Projects Agency (DARPA) with Explainable Artificial Intelligence (XAI) demonstrates a significant leap forward in creating transparent, trustworthy AI partners. Initiated in 2015 and formally launched in 2017, the four-year DARPA XAI program successfully developed a portfolio of machine-learning algorithms and explanation techniques that balance predictive performance with interpretability, enabling end users to understand the strengths, weaknesses, and decision logic of AI systems.[123] By 2021, XAI research teams had delivered the prototype Explainable Learners and psychological models of explanation, along with an open-source Explainable AI Toolkit (XAI Toolkit) that consolidates code, datasets, and evaluation frameworks for future development.[124] In the military decision-making context, XAI advances support human-machine teaming by providing user-friendly interfaces that visualize both instance-level and model-level explanations, such as feature-importance heatmaps and decision-tree surrogates, allowing commanders to trace AI recommendations back to specific assumptions and data inputs.[125] Furthermore, DARPA's integration of after-action review modules, mirroring Army war gaming practices, could close the loop between battlefield feedback and model refinement, collecting commander and operator inputs to continually retrain and improve AI responses under realistic mission conditions.[126]

Leadership and education will shape the culture surrounding AI use.[127] Future commanders do not need to be programmers, but they must understand how to engage with the machine, evaluate its suggestions critically, and maintain ethical judgment under uncertainty.[128] Leadership development programs must emphasize cognitive flexibility and a willingness to scrutinize machine outputs. Bias mitigation must be taught not as a technical issue alone but as a leadership responsibility, recognizing that bias can stem not only from algorithms but also from how humans frame queries or interpret outputs.[129] Although extensively addressed by numerous previous studies, it remains necessary to reiterate that leadership education must be centered on the foundational ethical and moral principles of international humanitarian law (IHL) and profession of arms. Empathetic IHL education is essential for learners to internalize the rules,

appreciate their importance, and understand the requirements to apply them effectively.[130]

Indeed, beyond the metrics and probabilistic approaches of artificial intelligence, only human judgment will remain the decisive factor in ensuring the principles of distinction, military necessity, proportionality, and humanity.[131]

Although conceived prior to the advent of AI, the final principle—humanity—is self-explanatory in asserting why the centrality of human judgment in ultimate decision making is a nonnegotiable issue.[132]

Personnel policies should reflect the need for new skill sets. Roles such as AI operations advisors or human-AI interaction specialists may need to be formalized within staff structures. Incentivizing cross-training between military planners and data analysts can bridge knowledge gaps and reduce misinterpretation.[133]

Facilities must be reconfigured to support real-time, high-fidelity human-AI collaboration. In particular, training centers should allow Joint experimentation with AI during exercises, reinforcing the importance of physically colocated or networked human-machine teams. Moreover, facilities must include dedicated spaces for post-operation analysis where AI and human performance can be jointly assessed to improve future decision-making processes.

In summary, the successful integration of AI into military planning and command requires a systemic transformation. Mitigating bias in AI queries, understanding the limits of machine logic, and developing a robust training-feedback ecosystem are not technical challenges alone—they are doctrinal, cultural, and educational imperatives. Only through a deliberate DOTMLPF analysis can armed forces ensure that AI becomes a planning enabler instead of a source of risk or overdependence.

Conclusions

The article's analysis of AI's integration into MDMP, particularly through tools like COA-GPT, reinforces that warfare fundamentally remains a human endeavor. As Clausewitz, Dupuy, and the examination of historical examples like McNamara's body count concept demonstrate, war is characterized by inherent uncertainty, friction, and the critical influence of intangible factors such as will, judgment, and human emotion. While AI offers extraordinary potential as a valuable tool, assisting in processing vast amounts of data, accelerating the OODA loop, and generating multiple courses of action, it cannot replace the human commander and staff.[134] The technology's limitations, including the risks of overfitting, the black-box problem, and the absence of Clausewitzian friction in its calculations, highlight the necessity of human oversight and critical thinking. In the words of Milan Vego:

There is a huge difference between using science and technology to

> enhance the combat potential of one's forces and applying scientific methods in the conduct of war. Our knowledge and understanding of warfare is a science, but the conduct of war itself is largely an art. This will not change in the future regardless of scientific and technological advances. As in the past, the character of war will change, even dramatically, but the nature of war as explained by Clausewitz will not.[135]

The path forward for effectively leveraging AI in military planning, as suggested by the developmental trajectory of COA-GPT, demands a holistic approach. This approach extends beyond technological advancements to encompass cultural, educational, and doctrinal changes within the military. Ultimately, the true success of AI integration hinges on how effectively we prepare our commanders and their staff to exploit these tools, especially when the time-constrained nature of tactical situations may tempt them to over rely on AI-generated solutions. This includes instilling AI literacy, fostering critical thinking, and developing the ability to exercise sound judgment. We must learn to guide AI, challenge its outputs, and, when necessary, override its recommendations. By doing so, we can harness AI's power to enhance our competitive advantage while ensuring that human intellect and acumen remain at the forefront of military decision making.[136]

Endnotes

1. Daniel Boffey, "Killing Machines: How Russia and Ukraine's Race to Perfect Deadly Pilotless Drones Could Harm Us All," *The Guardian*, 25 June 2025; "The Age of AI in U.S.-China Great Power Competition: Strategic Implications, Risks, and Global Governance," Beyond the Horizon, 3 February 2025; and Nicholas Thompson and Ian Bremmer, "The AI Cold War That Threatens Us All," *Wired*, 23 October 2018.
2. Kateryna Stepanenko, *The Battlefield AI Revolution Is Not Here Yet: The Status of Current Russian and Ukrainian AI Drone Efforts* (Washington, DC: Institute for the Study of War, 2025).
3. *Framework for Future Alliance Operations, 2018* (Norfolk, VA: NATO Allied Command Transformation, 2018), 10–12.
4. Norman Hughes, *Fleet Tactics and Naval Operations* (Annapolis, MD: Naval Institute Press, 2000), 29; and *Tactics,* Marine Corps Doctrinal Publication (MCDP) 1-3 (Washington, DC: Headquarters, Marine Corps, 2018).
5. H. W. Meerveld et al., "The Irresponsibility of Not Using AI in the Military," *Ethics and Information Technology* 25, no. 14 (2023): https://doi.org/10.1007/s10676-023-09683-0.
6. A. Trevor Thrall and Erik Goepner, "Counterinsurgency Math Revisited," CATO Institute, 2 January 2018.
7. Carl von Clausewitz, *On War*, ed. and trans. by Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976).
8. Alexis C. Madrigal, "The Computer That Predicted the U.S. Would Win the Vietnam War," *The Atlantic*, 5 October 2017.
9. Karl Popper, *The Logic of Scientific Discovery* (London: Routledge, 1959), 1–20, 122–31; and Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable* (New York: Random House, 2007), 138–50.

10. David Hume, *A Treatise of Human Nature* (Oxford: Clarendon Press, 1888), 92–104.
11. *Intelligence Analysis*, Army Techniques Publication (ATP) 2.33.4 (Washington, DC: Department of the Army, 2014), appendix b, 2.
12. John Boyd, *Destruction and Creation* (Fort Leavenworth, KS: U.S. Army Command and General Staff College, 1976).
13. B. H. Liddell Hart, *History of the Second World War* (London: Pan Books, 1970), 16–22; and Eliot A. Cohen and Phillips O'Brien, *The Russia-Ukraine War: A Study in Analytic Failure* (Washington, DC: Center for Strategic and International Studies, 2024).
14. Clausewitz, *On War*, book II, chap. 2.
15. Hughes, *Fleet Tactics and Naval Operations,* 195–96.
16. Gordon W. Prange, *At Dawn We Slept: The Untold Story of Pearl Harbor* (New York: Penguin Books, 1982), 725–37; and Max Hastings and Simon Jenkins, *The Battle for the Falklands* (London: W. W. Norton & Company, 1983), 267–89.
17. Mark Bowden, *Hue 1968: A Turning Point of the American War in Vietnam* (New York: Grove Press, 2018), 34–42.
18. Robert S. McNamara, *In Retrospect: The Tragedy and Lessons of Vietnam* (New York: Vintage Books, 1996), 3.
19. J. T. Correll, "The Confessions of Robert S. McNamara," *Air & Space Forces Magazine*, 1 June 1995; and K. Eschner, "How Robert McNamara Came to Regret the War He Escalated," *Smithsonian Magazine*, 29 November 2016.
20. Alain C. Enthoven and K. Wayne Smith, *How Much Is Enough?: Shaping the Defense Program, 1961–1969* (Santa Monica, CA: Rand Corporation, 2005), 71–72.
21. John L. Gaddis, *Strategies of Containment: A Critical Appraisal of American National Security Policy during the Cold War* (New York: Oxford University Press, 1982), 255–58.
22. Kenneth Cukier and Viktor Mayer-Schönberger, "The Dictatorship of Data," *MIT Technology Review*, 31 May 2013.
23. Matthew Fay, "Rationalizing McNamara's Legacy," *War on the Rocks*, 5 August 2016.
24. Douglas Kinnard, *The War Managers* (Hanover, NH: University Press of New England, 1977), 74.
25. Kinnard, *The War Managers*, 75.
26. Andrew Marshall, "An Overview of the McNamara Fallacy," Boot Camp & Military Fitness Institute, 31 December 2024.
27. David Kilcullen, *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One* (Oxford, UK: Oxford University Press, 2009), 25–27.
28. In strategic planning, the three fundamental elements proposed in Arthur Lykke's framework are represented by: *ends*, which refer to the objectives or desired outcomes to be achieved; *ways*, meaning the methods, strategies, or courses of action employed to use the available means in order to attain the desired results; and *means*, which encompass the resources and tools, both tangible and intangible, available to the decision maker for achieving the objectives. Harry R. Yarger, "Toward a Theory of Strategy," in *U.S. Army War College Guide to National Security Policy and Strategy*, 2d ed. (Carlise, PA: U.S. Army War College, 2006), chap. 8, 107–13.
29. Nazanin Azizian, *Easier to Get into War Than to Get Out: The Case of Afghanistan* (Cambridge, MA: Belfer Center for Science and International Affairs, 2021).
30. Edward N. Luttwak, *The Pentagon and the Art of War: The Question of Military Reform* (New York: Simon and Schuster, 1985), 23.
31. John J. Mearsheimer, "Assessing the Conventional Balance," *International Security* 13, no. 4 (Spring 1989): 5–53, https://doi.org/10.2307/2538780.
32. Clausewitz, *On War*, book II, chap. 2, 194.
33. Christopher A. Lawrence, *War by Numbers: Understanding Conventional Combat* (Lincoln: Potomac Books, an imprint of University of Nebraska Press, 2017), 30–31.
34. Shawn Woodford, "Dupuy's Verities: Combat Power =/= Firepower," The Dupuy Institute, 12 May 2019.
35. Woodford, "Dupuy's Verities."
36. LtCol Z. Jobbagy, "The Efficiency Aspect of Military Effectiveness," *Militaire Spectator* 178, no. 10 (2009): 431–39.

37. Gerhard Geldenhuys and Elmarie Botha, "A Note on Dupuy's QJM and New Square Law," *ORiON* 10, nos. 1–2 (1994): 45–55, https://doi.org/10.5784/10-0-455.
38. Geldenhuys and Botha, "A Note on Dupuy's QJM and New Square Law," 50–51.
39. Joshua M. Epstein, *The Calculus of Conventional War: Dynamic Analysis without Lanchester Theory* (Washington, DC: Brookings Institution Press, 1985).
40. Joshua M. Epstein, "Dynamic Analysis and the Conventional Balance," *International Security* 12, no. 4 (Spring 1988): 154–65.
41. Epstein, "Dynamic Analysis and the Conventional Balance."
42. Epstein, "Dynamic Analysis and the Conventional Balance."
43. *U.S. Ground Forces and the Conventional Balance in Europe* (Washington, DC: Congressional Budget Office, 1988), 83.
44. *U.S. Ground Forces and the Conventional Balance in Europe*.
45. Leo Tolstoy, *War and Peace* (Oxford, UK: Oxford University Press; originally 1869), book X, chap. 7, 1667.
46. Tolstoy, *War and Peace*, book II, chap. 17, 411–12.
47. Tolstoy, *War and Peace*, book X, chap. 25, 1816–1829.
48. Joshua M. Epstein, "Dynamic Analysis and the Conventional Balance," *International Security* 12, no. 4 (Spring 1988): 154–65.
49. Joshua M. Epstein, "Why Model?" (Second World Congress on Social Simulation, George Mason University, Fairfax, Virginia, 2008).
50. Cole Stryker and Eda Kavlakoglu, "What Is Artificial Intelligence (AI)?," IBM, 9 August 2024.
51. Ian Goodfellow, Yoshua Bengio, and Aaron Courville, *Deep Learning* (Cambridge, MA: The MIT Press, 2016), 1–4.
52. Goodfellow, Bengio, and Courville, *Deep Learning*, 5–6.
53. Goodfellow, Bengio, and Courville, *Deep Learning*, 96–114.
54. Christopher M. Bishop, *Pattern Recognition and Machine Learning* (New York: Springer, 2006), 1–29.
55. Alexandre Piquard, "Chatbots Are Like Parrots, They Repeat without Understanding," *Le Monde*, 7 October 2024.
56. Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed. (London: Pearson, 2020), 721–49.
57. Hughes, *Fleet Tactics and Naval Operations*, 212.
58. Riley Simmons-Edler et al., "Military AI Needs Technically-Informed Regulation to Safeguard AI Research and its Applications," ArXiv, 23 May 2025.
59. Paul Scharre, *Army of None. Autonomous Weapons and the future of War* (New York: Norton & Company, Inc., 2018), 140–63; and Wyatt Hoffman and Heeu Millie Kim, *Reducing the Risks of Artificial Intelligence for Military Decision Advantage* (Washington, DC: Center for Security and Emerging Technology, 2023), 8–9.
60. *Synthetic data* is data that is artificially generated in the digital world with properties that are often derived from an "original" set of data. This is in contrast to real-world data, which, as the name suggests, is data collected from real-world events and inputs. Harry Deng, *Exploring Synthetic Data for Artificial Intelligence and Autonomous Systems: A Primer* (Geneva, Switzerland: UNIDIR, 2023).
61. Bishop, *Pattern Recognition and Machine Learning*, 1–10.
62. Christoph Molnar, *Interpretable Machine Learning* (self-published: 2025), 10–13.
63. Henry A. Kissinger, Craig Mundie, and Eric Schmidt, *Genesis: Artificial Intelligence, Hope, and the Human Spirit* (New York: Little, Brown and Company, 2024), 48–49.
64. Andrea Capaccioni, "Sull'affidabilità delle bibliografie generate dai chatbot. Alcune considerazioni," *AIDAinformazioni*, January–June 2024.
65. Hammad Abbasi, "The Dunning-Kruger Effect and LLMs: Confidence vs. Competence in AI: Understanding How AI and Humans Misjudge Their Own Abilitie," Medium, 18 August 2024; and Amanda Bickerstaff and Ben Garside, "Anthropomorphizing AI: The Impact on Students & Education," AI for Education, YouTube video, 52:58.

66. Jessie Y. C. Chen et al., *Situation Awareness–Based Agent Transparency* (Adelphi, MD: Army Research Laboratory, 2014).
67. Kristian Humble, "War, Artificial Intelligence, and the Future of Conflict," *Georgetown Journal of International Affairs*, 12 July 2024.
68. Steven D. Sacks, "A Framework for Lethal Autonomous Weapons Systems Deterrence," *Joint Force Quarterly* no. 110 (2023). Similarly, MajGen Mark T. Simerly, "Predictive Logistics in Data-Driven Sustainment," *Army Sustainment* (Fall 2023); and Michael Clark, "Intervention at AI Defense Forum," U.S. Cyber Command, 10 September 2024.
69. Gennady Staskevich, "Artificial Intelligence and Next Generation Distributed Command and Control," Department of Defense, 31 August 2023; LtGen Clint Hinote, USAF, *Reimagining Command and Control with Human-Machine Team*s, Defense Paper Series (Arlington, VA: Special Competitive Studies Project, 2024); and Maj Matthew R. Voke (USAF), *Artificial Intelligence for Command and Control of Air Power* (Montgomery, AL: Air Command and Staff College, 2019).
70. John R. Boyd, "New Conception for Air-to-Air Combat" (unpublished manuscript, 1976).
71. John Larue, "Automating Intelligence Preparation of the Battlefield: An Enabling Concept for Intelligence" (master's thesis, Marine Corps University, 2019); and John Brennan and Ararsh Kulkarni, "Fighting for Seconds: Warfare at the Speed of Artificial Intelligence," Modern War Institute, 2 November 2023.
72. Michael Farmer, "Four-Dimensional Planning at the Speed of Relevance: Artificial-Intelligence-Enabled Military Decision-Making Process," *Military Review*, November–December 2022.
73. Vinicius Goecks and Nicholas Waytowich, "COA-GPT: Generative Pre-trained Transformers for Accelerated Course of Action Development in Military Operations," arXiv, 1 February 2024.
74. Ashish Vaswani, "Attention Is All You Need" (presentation, Thirty-First Annual Conference on Neural Information Processing Systems [NIPS], Long Beach, CA, 4–9 December 2017).
75. Tom B. Brown et al., "Language Models are Few-Shot Learners" (presentation, Proceedings of the 34th International Conference on Neural Information Processing Systems, Vancouver, Canada, 6–12 December 2020).
76. Nicolás Rojas and Katherine H. Van Dyke, "COA-GPT: Leveraging Large Language Models for Military Course of Action Generation" (presentation, 2024 International Conference on Military Communication and Information Systems [ICMCIS], Koblenz, Germany, 23–24 April 2024).
77. Robert S. McNamara, *In Retrospect: The Tragedy and Lessons of Vietnam* (New York: Times Books, 1995), 319–36.
78. Koen van der Zwet et al., "Promises and Pitfalls of Computational Modeling for Insurgency Conflicts," *Journal of Defense Modeling and Simulation* 20, no. 3 (2022): 333–50, https://doi.org/10.1177/15485129211073612.
79. Brendan C. Raymond, "A Question of Balance: Metrics or Art for Joint Force Decision-Making?" (dissertation, Naval War College, Newport, RI, 23 April 2008).
80. Edward Targett, "Palantir Says AI Means Pentagon Can Use 20 People Instead of 2000 to Target Enemies, Rakes in Cash," The Stack, 5 November 2024.
81. Timothy Thomas and Glen Howard, "Emerging Russian Perspectives on the Military Uses of AI in Warfare," The Saratoga Foundation, 6 February 2025.
82. David S. Alberts, John J. Garstka, and Richard E. Hayes, *Power to the Edge: Command and Control in the Information Age* (Washington, DC: Department of Defense, 2004), 105–7.
83. Jonathan Nielsen and Eric Cannon. "Utilizing the Integrated Tactical Network in Mobile Command Posts," Line of Departure, 18 October 2024.
84. Michael Zequeira, "Artificial Intelligence as a Combat Multiplier: Using AI to Unburden Army Staffs," *Military Review*, 18 September 2024.
85. Jenna Brady, "Army Researchers Suggest Uncertainty May Be Key in Battlefield Decision Making," Army.mil, 17 July 2018.

86. Burak Yuksek et al., "Intelligent Wargaming Approach to Increase Course of Action Effectiveness in Military Operations" (AIAA SciTech Forum 2023, National Harbor, MD, 23–27 January 2023).
87. *Partially observable Markov decision process (POMDP)*: A decision-making model that represents scenarios in which the system's state is not fully observable, allowing for the planning of optimal actions based on probabilities that are updated as new information becomes available. *Bayesian networks*: Probabilistic structures that model causal dependencies between variables, allowing for the dynamic updating of estimates as observed evidence changes; useful for reasoning under uncertainty. *Monte Carlo simulations*: A computational method that uses repeated random experiments to estimate the probabilistic impact of uncertain variables on an outcome, often used for risk analysis and complex scenarios.
88. Goecks and Waytowich, "COA-GPT."
89. *Marine Corps Planning Process*, Marine Corps Warfighting Publication (MCWP) 5-10 (Quantico, VA: Headquarters, Marine Corps, 2020).
90. Warren Marlow, "First Army Trained on New Software Suite That Enhances Warfighting Capability," U.S. Army, 31 January 2022; Thomas Myers, "Exploring the Potential of ATAK for Field Operations," accessed 17 November 2025; and NCI Academy, "JOC Watch Administrator," Credly by Pearson, accessed 17 November 2025. For example, if the armored unit suffers more than 30 percent casualties within the first 10 minutes, then retreat to Attack Position Bravo and activate indirect fire.
91. Y. Sariel, *The Human-Machine Team* (self-published, 2021), 29.
92. Sariel, *The Human-Machine Team*, 41–42; and Carl von Clausewitz, *On War*, book I, chap. 3, 101.
93. *U.S. Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway* (Washington, DC: Department of Defense, 2022), 5.
94. Hoffman and Kim, *Reducing the Risks of Artificial Intelligence for Military Decision Advantage*, 4.
95. Ayla R. Reed, "Uncertainty Quantification: Artificial Intelligence and Machine Learning in Military Systems," *Air & Space Operations Review* 2, no. 1 (Spring 2023).
96. Dian Chen et al., "Advancing Human-Machine Teaming: Concepts, Challenges, and Applications," arXiv, 6 May 2025; and Benjamin Jensen and Matthew Strohmeyer, *Agentic Warfare and the Future of Military Operations: Rethinking the Napoleonic Staff* (Washington DC: CSIS, July 2025), 23.
97. Chen et al., "Advancing Human-Machine Teaming," 41.
98. Sariel, *The Human-Machine Team*, 39.
99. Chen et al., "Advancing Human-Machine Teaming," 10–19.
100. Fergal Glynn, "What Is AI Red Teaming?," Mindgard, 24 July 2025.
101. Subhabrata Majumdar, Brian Pendleton, and Abhishek Gupta, "Red Teaming: AI Red Teaming," arXiv, 7 July 2025.
102. *Data poisoning* is the deliberate manipulation of data sets used for training. Pinlong Zhao, "Data Poisoning in Deep Learning: A Survey," arXiv, 27 March 2025, https://arxiv.org/html/2503.22759v1; and Fazrad Kamrani et al., *Attacking and Deceiving Military AI Systems* (Stockholm, Sweden: Swedish Defence Research Agency, 2023).
103. Benjamin Jensen, "AI Is about to Radically Alter Military Command Structures that Haven't Changed Much since Napoleon's Army," The Conversation, 18 August 2025.
104. LtGen Milford Beagle, USA, BGen Jason C. Slider, USA, and LtCol. Matthew R. Arrol, USA, "The Graveyard of Command Posts: What Chornobaivka Should Teach Us about Command and Control in Large-Scale Combat Operations," *Military Review*, May–June 2023.
105. Jensen, "AI Is about to Radically Alter Military Command Structures."
106. Jensen and Strohmeyer, *Rethinking the Napoleonic Staff*, 10.
107. Jim Storr, *Something Rotten: Land Command in the 21st Century* (Aldershot, UK: Howgate Publishing, 2022), 75–112; and Mollie Ryan, "Future Conflicts Demand Flexible and Mobile Command Posts," U.S. Army, 2 June 2024.

108. Anna Madison et al., " 'New' Challenges for Future C2: Commanding Soldier-Machine Partnerships," arXiv, 11 March 2025.
109. Kate Egerton et al., "Not-So-Artificial Intelligence: Teaching and Learning AI Literacy in a PME Community," Air University Public Affairs presentation, 8 December 2023, video, 1:01:31.
110. Benjamin Jensen and MajGen Jake S. Kwon, "The U.S. Army, Artificial Intelligence, and Mission Command," *War on the Rocks*, 10 March 2025.
111. Jensen, "AI Is about to Radically Alter Military Command Structures that Haven't Changed Much since Napoleon's Army."
112. *Adversarial examples*: intentionally manipulated inputs designed to induce AI systems to make critical errors in classification or decision-making, thereby undermining the reliability of operational functions such as target recognition, autonomous navigation, and threat identification. Their incorporation enhances resilience against deliberate manipulation and deception, including sensor spoofing, visual camouflage, and electromagnetic interference, strengthening robustness in contested environments, a progressive degradation that occurs when AI systems are repeatedly trained on synthetic data, leading to loss of accuracy and diversity in their outputs. Mayra Macas, Chunming Wu, and Walter Fuertes, "Adversarial Examples: A Survey of Attacks and Defenses in Deep Learning-Enabled Cybersecurity Systems," *Expert Systems with Applications* no. 238 (2024): https://doi.org/10.1016/j.eswa.2023.122223. *Model collapse*: a progressive degradation that occurs when AI systems are repeatedly trained on synthetic data, leading to loss of accuracy and diversity in their outputs. Sarah Magazzo, "AI Model Collapse: What It Is, Why It Matters, and How to Prevent It," Mondo Insights, 18 June 2025.
113. Sariel, *The Human-Machine Team*, 29–35, 57–58. "Synergetic learning is the new, systematic, mutual process of a human and a machine as a learning team."
114. Leslie A. DeChurch and Jessica R. Mesmer-Magnus, "Measuring Shared Team Mental Models: A Meta-Analysis," *Group Dynamics: Theory, Research, and Practice* 14, no. 1 (2010): 1–14, https://doi.org/10.1037/a0017455.
115. Chen et al., "Advancing Human-Machine Teaming," 28.
116. *Military Artificial Intelligence Test and Evaluation Model Practices*, ed. R.S. Panwar, Li Qiang, and John N. T. Shanahan (Washington, DC: Center for a New American Security, 2024), 6.
117. *Trustworthiness for AI in Defence: Developing Responsible, Ethical, and Trustworthy AI Systems for European Defence* (Brussels, Belgium: European Defence Agency, 2025).
118. Cody Martin, *The Importance of Force on Force Training: Maximizing Preparedness* (Fort Worth, TX: Risk Strategy Group, 2023).
119. Harry Deng, *Exploring Synthetic Data for Artificial Intelligence and Autonomous System*: *A Primer* (Geneva, Switzerland: United Nations Institute for Disarmament Research, 2023), 6–7; Jean-Marc, "Human-Machine Teaming in Artificial Intelligence-Driven Air Power: Future Challenges and Opportunities for the Air Force," *Air Power Journal*; and Cameron Hunter and Bledden E. Bowen, "We'll Never Have a Model of an AI Major-General: Artificial Intelligence, Command Decisions, and Kitsch Vision of War," *Journal of Strategic Studies* 47, no. 1 (2024): 116–46, https://doi.org/10.1080/01402390.2023.2241648.
120. "Researchers Improve Human-AI Interaction for Combat Vehicles," U.S. Army, 28 July 2020.
121. Jessie Y. C. Chen et al., "Situation Awareness-Based Agent Transparency and Human-Autonomy Teaming Effectiveness," *Theoretical Issues in Ergonomics Science* 19, no. 3 (2008): 259–82, https://doi.org/10.1080/1463922X.2017.1315750.
122. Chen et al., "Situation Awareness-Based Agent Transparency and Human-Autonomy Teaming Effectiveness," 259–82.
123. David Gunning et al., "DARPA's Explainable AI (XAI) Program: A Retrospective," *Applied AI Letters* 2, no. 4 (December 2021): https://doi.org/10.1002/ail2.61.
124. Gunning et al., "DARPA's Explainable AI (XAI) Program."
125. Linus J. Luotsinen et al., *Explainable Artificial Intelligence: Exploring XAI Techniques in*

Military Deep Learning Applications (Stockholm, Sweden: Swedish Defence Research Agency, 2019).

126. Jonathan Dodge et al., "After-Action Review for AI (AAR/AI)," *ACM Transactions on Interactive Intelligent Systems* 11, nos. 3–4 (2021): 1–33, https://doi.org/10.1145/3453173.
127. Sarah Starr, "Professional Military Education in the Age of AI," Medium, 29 June 2023.
128. LtGen Clint Hinote, *Reimagining Command and Control with Human-Machine Teams* (Arlington, VA: Special Competitive Studies Project, 2024).
129. C. Anthony Pfaff et al., *Trusting AI: Integrating Artificial Intelligence into the Army's Professional Expert Knowledge* (Carlisle, PA: U.S. Army War College, 2023).
130. Matthias Klaus, "Transcending Weapons System: The Ethical Challenges of AI in Military Decision Support System," *Humanitarian Law & Policy* (blog), 24 September 2024.
131. Julia Gawlas, "Use of AI DSS in Military Operations: An Assessment under International Humanitarian Law," *ASA International Law*, 4 July 2025.
132. Joanna L. D. Wilson, "AI, War, and (In)humanity: The Role of Human Emotions in Military Decision-making," *Humanitarian Law & Policy* (blog), 20 February 2025.
133. John R. Hoehn, *Joint All-Domain Command and Control: Background and Issues for Congress* (Washington, DC: Congressional Research Service, 2022).
134. Szymon Otto and Gabriel Mănescu, "Will Artificial Intelligence (AI) Replace a Human Commander in the Army?," *Scientific Bulletin* 28, no. 1 (June 2023), https://doi.org/10.2478/bsaft-2023-0009.
135. Milan Vego, "Science Vs. the Art of War," *Joint Force Quarterly* no. 66 (3d quarter 2012): 62–70.
136. M. Meleiro and M. Passos, "Future Warfare: Navigating AI Integration in Military Combat Decision-Making" (master's thesis, Lunds University, Lund, Sweden, May 2024), 57.

Synthesizing Strategic Frameworks for Great Power Competition

Major Gavin Holtz, USMC

Abstract: This article examines the theoretical foundations necessary for conceptualizing and operationalizing modern great power competition through the innovative synthesis of three influential military frameworks: Colonel John R. Boyd's observe, orient, decide, act (OODA) loop, Colonel John A. Warden's systems analysis, and Chinese colonels Qiao Liang and Wang Xiangsui's unrestricted warfare theory. The research demonstrates how complementary frameworks provide strategic practitioners with comprehensive capabilities for identifying systemic vulnerabilities, orchestrating cross-domain effects, and maintaining decisive advantage through superior decision-making processes. The analysis reveals how modern competition transcends traditional military boundaries, necessitating organizational architectures capable of implementing synchronized operations across multiple competitive domains. This theoretical synthesis supports the proposal for an Interagency Action Committee on China (IAC-C) and identifies the foundational principles of a cross-domain organizational framework.

Keywords: observe, orient, decide, and act loop, OODA, systems analysis, unrestricted warfare, great power competition, cross-domain operations, interagency coordination, gray zone warfare, liminal warfare

Introduction

Modern great power competition demands strategic frameworks beyond traditional boundaries. As the 2018 *National Defense Strategy* identifies, "inter-state strategic competition, not terrorism, is now

Maj Gavin Holtz, USMC, is a weapons and tactics instructor currently assigned to Marine Fighter Attack Squadron 122 in MCAS Yuma, AZ. He has a bachelor of arts in history from University of Arizona and a master in military operational studies from the U.S. Army Command and General Staff Officers Course.

Journal of Advanced Military Studies vol. 16, no. 2
Fall 2025
www.usmcu.edu/mcupress
https://doi.org/10.21140/mcuj.20251602006

the primary concern in U.S. national security," requiring capabilities to operate across diplomatic, informational, military, and economic domains simultaneously.[1] Chinese colonels Qiao Liang and Wang Xiangsui's revolutionary unrestricted warfare theory provides essential insights that complement the pinnacle of American operational thought represented by Air Force colonel John R. Boyd's OODA loop theory and Colonel John A. Warden's systems analysis.[2] Understanding contemporary competition requires synthesizing these frameworks: Qiao and Wang identify expanded competitive space, Boyd's OODA loop maintains advantage through superior observation and adaptation, and Warden's analysis enables systematic parallel targeting. This synthesis provides a comprehensive approach for an era where technological integration and globalization blur military and nonmilitary boundaries while creating novel capabilities and vulnerabilities.

Understanding contemporary competition requires examining how these three frameworks complement each other. We begin with unrestricted warfare's expansion of the competitive space, then examine Boyd's decision-making framework, before exploring Warden's systems analysis, and finally demonstrate their synthesis in the IAC-C and principles for a cross-domain organization.

Unrestricted Warfare by Colonels Qiao Liang and Wang Xiangsui

The People's Liberation Army's (PLA) sobering assessment of its technological and doctrinal deficiencies drove China's military modernization in the 1980s.[3] The PLA, shaped by Mao Zedong's "people's war" doctrine emphasizing massive infantry formations and guerrilla tactics, found itself increasingly outpaced by modern warfare capabilities demonstrated in conflicts like the 1982 Falklands War and the 1983 U.S. operation in Grenada. Although Deng Xiaoping initiated significant reforms through his 1985 "Strategic Transformation," reducing troops by one million and investing in air force, navy, and missile capabilities, PLA leaders recognized their persistent technological disadvantage against Western militaries. This made the search for asymmetric counters to American military superiority particularly urgent.[4]

Operation Desert Storm (17 January–28 February 1991) provided Chinese strategists Qiao Liang and Wang Xiangsui—both PLA Air Force political warfare officers at senior colonel rank—their first detailed assessment of American military capabilities.[5] Their political warfare backgrounds shaped their theoretical approach to unrestricted warfare, extending analysis beyond conventional military operations into comprehensive national power employment. Operation Desert Shield's five-month buildup demonstrated America's capability to mobilize and deploy strategically significant combat forces globally, while the combat phase revealed technological superiority that rendered conventional

military competition futile.[6] Their analysis of both U.S. advantages and vulnerabilities led to the unrestricted warfare theory—a framework for defeating technologically superior adversaries by expanding conflict beyond traditional military domains.[7]

The Coalition's opening night attacks crystallized the scale of America's technological advantage. Within hours, Lockheed F-117 Nighthawk stealth aircraft and Tomahawk cruise missiles had penetrated Iraq's integrated air defense system to strike key command and control nodes across Baghdad. This demonstration of precision strike capabilities and systematic targeting methodology represented warfare at a level of sophistication far beyond China's capabilities. By the second day of the air campaign, Iraq's nationwide air defense network had effectively collapsed, leaving Coalition aircraft free to operate with near impunity.[8]

The U.S.-led Coalition's systematic isolation of Iraq demonstrated sophisticated integration of military and nonmilitary power through United Nations resolutions and economic sanctions.[9] This revealed how coordinated diplomatic, economic, and military actions could create compounding effects beyond battlefield impact, degrading civilian morale, political stability, and economic activity.[10]

These observations shaped three interconnected theoretical concepts forming unrestricted warfare's foundation.[11] The first, supranational combinations, built on Operation Desert Storm's Coalition-building approach but envisioned expanding beyond traditional military alliances. While the U.S.-led Coalition demonstrated effective international coordination for military operations, Qiao and Wang saw opportunity for more comprehensive integration of state and nonstate actors. From China's perspective, coordinating actions across international organizations, multinational corporations, criminal organizations, terrorist groups, media entities, and individual actors could create strategic effects without relying on conventional military operations.[12] The Gulf War's United Nations mandates and international sanctions demonstrated this potential, but the authors believed future conflicts would require orchestrating an even broader range of state and nonstate actions.[13]

Their second concept, supradomain combinations, extended Operation Desert Storm's successful military domain integration into a broader theory of cross-domain operations.[14] The authors noted how Coalition air strikes against Iraqi electrical infrastructure impacted not just military command systems but created cascading effects across multiple domains. This observation led them to theorize that deliberately orchestrating actions across political, economic, technological, cultural, and psychological domains could achieve strategic objectives more efficiently than pure military force. The authors specifically cited how media coverage of precision strikes against Baghdad shaped both Iraqi and

international perceptions, demonstrating warfare's expansion into the information domain.[15]

Supra-means combinations, their third concept, directly addressed limitations they perceived in America's technology-centric approach.[16] While Operation Desert Storm demonstrated the devastating potential of precision weapons and information warfare, Qiao and Wang argued that any method capable of achieving strategic effects constitutes a legitimate instrument of warfare. They noted how economic sanctions damaged Iraq's military capabilities as effectively as airstrikes, leading them to advocate developing integrated capabilities for financial warfare, lawfare, ecological warfare, psychological operations, and cyberattacks alongside traditional military means. China needed to transcend conventional military boundaries, coordinating all instruments of national power to achieve strategic effects.[17]

Qiao and Wang outlined specific scenarios like countering the U.S. intervention in Taiwan through synchronized cyberattacks, financial operations, lawfare, and media warfare—avoiding domains where American military advantages dominate.[18] This would allow China to achieve situations of fait accompli, ensuring their goals are achieved without successful American military intervention. This comprehensive approach offered China a viable path to compete with technologically superior adversaries.[19]

Qiao and Wang inverted America's Operation Desert Storm model. Instead of using nonmilitary means to support military operations, they advocated nonmilitary operations as the main effort through networks of state and nonstate actors to achieve objectives without armed conflict. The authors specifically criticized America's sequential approach in Operation Desert Storm—using economic sanctions, diplomatic pressure, and information operations to set conditions for military action. Instead, they advocated simultaneous employment of multiple instruments in ways that would make a military response difficult or counterproductive.[20]

This approach reflected China's strategic position relative to the United States. Rather than attempting to match American military capabilities directly, unrestricted warfare theory sought to exploit the very interconnectedness and technological dependence that gave the United States its conventional advantages.[21] By orchestrating effects across multiple domains using diverse means, China could potentially achieve strategic objectives without having to overcome America's conventional military superiority. Their framework called for using the very institutions, organizations, and networks that supported American power—international financial systems, global media, multinational corporations, and international law—as instruments to constrain U.S. freedom of action.[22]

Operation Desert Storm served as both a demonstration of American

power and a catalyst for developing strategies to nullify conventional military advantages. Qiao and Wang's analysis revealed how warfare can evolve in an interconnected world, where coordinated multidomain actions transcend traditional frameworks.[23] This raises fundamental questions about how government and military organizations must adapt to operate effectively across multiple domains while integrating diverse instruments of power. Understanding and applying these concepts becomes crucial for developing comprehensive approaches to modern strategic competition.[24] Having examined how unrestricted warfare expands the competitive space beyond traditional military domains, we now turn to Boyd's framework for maintaining decision-making superiority within this expanded battlespace.

A Discourse on Winning and Losing by Colonel John Boyd

The observe, orient, decide and act (OODA) loop originated as Boyd's framework for understanding success in aerial combat but evolved into a comprehensive theory of competition applicable from tactical to strategic levels. Through rigorous analysis of military history and scientific principles, Boyd demonstrated how superior decision-making processes create compounding advantages in competitive environments.[25]

Boyd's theory originated from Korean War observations where North American F-86 Sabre pilots consistently outperformed technically superior Mikoyan-Gurevich MiG-15s flown by Soviet, Chinese, and North Korean pilots through better visibility and hydraulic controls enabling quicker transitions between maneuvers. This tactical insight led Boyd to explore how superior decision-making processes create compounding advantages in competitive environments.[26]

Observation in Boyd's framework extends far beyond simple information gathering. It encompasses active collection and filtering of information across all relevant domains of competition.[27] Organizations must deliberately structure their observation processes to gather comprehensive information while filtering irrelevant data that could slow decision making.[28]

Orientation serves as the cognitive engine of Boyd's framework, shaping how organizations interpret and understand their observations.[29] Boyd identified this as the most crucial element because it determines how organizations process information and generate options for action. Orientation integrates cultural traditions, institutional experience, and information to create a better understanding of the competitive environment.[30]

The *decision* element operates through two distinct pathways: explicit analytical processes and implicit guidance control. Explicit decisions involve conscious analysis and choice, while implicit guidance enables rapid action based

on deeply ingrained understanding. The balance between these pathways shifts based on time available and the nature of the competition.[31]

The *action* element completes the OODA loop, but Boyd emphasized that effective action requires more than simple execution of decisions. Action in Boyd's framework must be purposeful, decisive, and designed to shape the competitive environment.[32] Organizations must structure their actions to simultaneously accomplish immediate objectives while setting conditions for future success. This dual nature of action—achieving current goals while influencing future competitive dynamics—highlights why Boyd insisted that activity must flow from clear strategic intent rather than tactical convenience.[33]

Boyd's analysis revealed that principles determining success in tactical air combat applied across all levels of competition. His framework illuminates how organizations achieve decisive advantages through superior decision-making processes, whether at strategic, operational, or tactical levels. The true power emerges through operating inside the OODA loop—creating conditions where an opponent's orientation becomes increasingly disconnected from reality. As the adversary's understanding deteriorates, their actions become progressively less relevant to the actual competitive environment, eventually leading to decision-making paralysis.[34]

The complexity of modern competition, with its interconnected domains and rapid technological change, makes Boyd's emphasis on mental agility increasingly vital.[35] His "destruction and creation" process (the cognitive mechanism for decomposing existing mental models and synthesizing new understanding) provides organizations a systematic methodology to analyze existing concepts and synthesize new understanding while maintaining both speed and accuracy in their decision cycles.[36] This process is particularly relevant today as organizations must process unprecedented volumes of information across multiple domains while maintaining strategic coherence.[37]

Boyd's emphasis on orientation explains why simply gathering more information or acting more quickly fails to guarantee success in modern competition. Organizations must instead develop robust processes for analyzing information and updating their understanding of the competitive environment. This is especially critical given how emerging technologies and interconnected systems create novel competitive dynamics that can quickly invalidate existing mental models. Orientation thus serves as the fulcrum of modern competition, determining how organizations interpret information and generate options for action in increasingly complex environments.[38]

Organizations achieve this adaptive capability through what Boyd termed *fingerspitzengefühl*—an intuitive mastery enabling rapid, effective action without requiring explicit analysis.[39] Boyd borrowed this German military term, which translates as "fingertip feeling," from his extensive study of the *Wehr-*

macht's command philosophy during World War II. The concept was central to German military doctrine that emphasized decentralized decision making (*auftragstaktik*) and developed through the German General Staff system since the late nineteenth century.[40] This capability develops through repeated application of the destruction and creation process, systematically breaking down and reconstructing understanding to better match reality. The resulting implicit guidance allows appropriate action at a high tempo while maintaining strategic coherence.[41]

The framework's enduring relevance stems from its focus on mental processes rather than physical capabilities.[42] Whether in military operations, business competition, or strategic rivalry between nations, success flows from the ability to maintain accurate orientation while operating at a faster tempo than opponents. Boyd's contribution lies in systematically explaining how organizations can develop and maintain these crucial capabilities through repeated application of the destruction and creation process.[43]

While Boyd focused on decision-making processes, John Warden approached military theory from a different angle. His revolutionary systems theory emerged from a fundamental challenge to traditional military thought. Where Carl von Clausewitz emphasized defeating an adversary's center of gravity through decisive battle, Warden argued that enemies should be understood as complex interconnected systems, with military forces representing only one component of national power.[44]

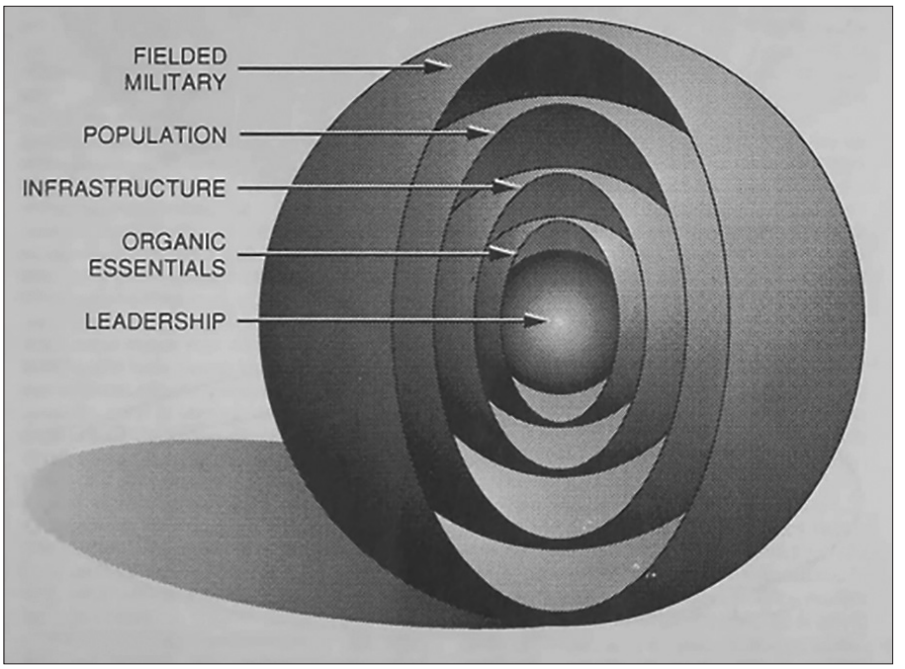
The Enemy as a System by Colonel John Warden III

Colonel John Warden III's approach marked a decisive break from earlier strategic bombing theories due to the increasing complexity and interrelated nature of nation-states. Unlike the Italian airpower theorist Giulio Douhet, who focused on industrial centers and population morale, Warden targeted leadership and critical nodes for strategic paralysis.[45] This approach leveraged precision weapons and recognized how systematic pressure, not widespread destruction, could compel state behavior change.[46]

Drawing from systems analysis in biology and physics, Warden observed that all complex organisms shared similar organizational patterns—from human bodies to electrical grids to nation-states. This observation led him to develop a universal model for analyzing and affecting enemy systems that could be applied across different scales and types of conflict.[47]

Warden's "Five Rings" model presented a dynamic framework for analyzing enemy vulnerabilities through concentric rings, with leadership at the center as the system's brain (figure 1).[48] The model's power lay in its adaptability—the specific composition of each ring could be adjusted based on the target system being analyzed, whether a nation-state, terrorist organization, or military unit.[49]

Figure 1. The Five Rings model



Source: John A. Warden III, "The Enemy as a System," *Airpower Journal* 9, no. 1 (Spring 1995): 47.

The innermost ring, leadership, remains constant as it encompasses both strategic decision makers and their command-and-control mechanisms—the only elements capable of altering strategic direction or surrendering. The second ring, system essentials, contains critical processes necessary for the system's function.[50] For a nation-state, this includes electrical power generation and petroleum refineries. For a terrorist organization, it might include financing networks and bomb-making facilities.[51]

The infrastructure ring comprises the physical and organizational networks that connect and support other system components. In a state system, this includes transportation networks and industrial facilities.[52] For a military unit, it would include supply lines and communications systems. The population ring represents the human dimension: the workforce, supporters, or fighters, depending on the system analyzed. The outermost ring contains protective elements—conventional and paramilitary forces for a state.[53]

The model's revolutionary aspect lay in its systematic analysis of ring interactions. Damage to inner rings multiplied effects throughout the system—destroying electrical facilities simultaneously degraded military command and control, civilian telecommunications, and industrial output.[54] The advent of

precision-guided munitions made this systematic approach viable by enabling reliable strikes against specific vulnerabilities.[55]

Having established the theoretical framework, Operation Desert Storm provided the crucial first test of Warden's systems theory through parallel warfare—striking multiple rings simultaneously to overwhelm Iraq's ability to adapt or repair critical systems.[56] The campaign's opening night demonstrated this revolutionary approach as Coalition aircraft struck more than 150 separate targets across all five rings within the first 24 hours—more targets than the Eighth Air Force hit in all of 1943.[57]

These coordinated attacks immediately validated Warden's theory about system interdependence. The systematic targeting of Iraq's electrical grid cascaded into nationwide communications failures, degraded air defense capabilities, and disrupted military command and control. Within hours, Iraqi phone service fell precipitously, key leadership offices were isolated, and air defense centers lost contact with their units.[58] This demonstrated how attacking critical nodes could achieve strategic impacts far beyond direct damage.

The campaign's effectiveness stemmed from precise identification of Iraqi system components within each ring. Leadership targets included command bunkers and communications nodes. System essentials focused on electrical generation and oil refineries. Infrastructure targets encompassed transportation networks and military supply lines. While population centers were avoided for political reasons, military forces were systematically isolated and degraded through attacks on other rings.[59]

The Five Rings model, while revolutionary in Operation Desert Storm, requires adaptation based on the specific adversary system being analyzed. Not all systems exhibit the same degree of centralization or vulnerability patterns.[60] Therefore, in future applications of this model, adjustment to each ring, especially the core, must be informed by the assessment of the adversary. The rings must be adapted as adversary behavior changes within its system, as political objectives change, or with the methods with which we are attacking the system.

Synthesis and Application of Three Theories

Contemporary military doctrine recognizes six warfighting domains where competition and conflict occur: air, land, maritime, space, cyberspace/electromagnetic spectrum, and the cognitive domain.[61] The synthesis of unrestricted warfare, Boyd's OODA loop, and Warden's systems analysis provides frameworks for operating across all domains simultaneously, as modern competition rarely confines itself to single-domain operations.

Modern great power competition requires strategists to identify systemic vulnerabilities, orchestrate multidomain operations, and maintain decisive

advantage through superior decision making. The synthesis of Warden's systems analysis, unrestricted warfare theory, and Boyd's OODA loop creates this framework by combining systematic vulnerability analysis, comprehensive methods for exploitation, and a process for maintaining initiative across all domains of competition. This integration enables strategists to understand complex interstate systems, develop coordinated cross-domain campaigns, and maintain competitive advantage through superior observation and adaptation.

The synthesis begins with Warden's systems analysis revealing how components of national power form complex networks of interdependence. Applied to China's Belt and Road Initiative, for example, systems analysis shows how infrastructure investments create interconnected diplomatic, economic, and security effects throughout Southeast Asia. These investments simultaneously generate economic leverage, establish potential military logistics networks, and create diplomatic pressure points that can be exploited through coordinated action.[62] The hydroelectric dams along the Mekong River demonstrate this interconnection—Chinese control of upstream water resources simultaneously affect regional food security, economic development, and inter-state relations.[63]

Unrestricted warfare theory transforms this systems analysis into operational advantage by providing methods for simultaneously affecting multiple system components. Where Warden identifies critical nodes, unrestricted warfare's supradomain combinations enable synchronized application of diplomatic, economic, and information operations to subtly create opportunities for compounding effects.[64] For instance, systems analysis reveals vulnerabilities in China's semiconductor supply chain, while unrestricted warfare theory enables coordinated response through export controls (economic), diplomatic pressure on supplier nations (political), and information operations highlighting technological dependencies (informational).[65] This operational framework allows strategists to orchestrate effects across multiple domains while maintaining coherence between tactical actions and strategic objectives.[66]

Boyd's OODA loop completes the synthesis by providing the cognitive framework for maintaining advantage while conducting parallel operations. His emphasis on rapid observation and orientation enables processing of information from multiple domains while maintaining an accurate understanding of the competitive environment.[67] When economic data reveals limited Chinese access to cheap food and energy, faster OODA loops allow rapid adjustment of diplomatic and economic efforts to exploit this insight.[68] Most crucially, Boyd's concepts of tempo and initiative explain how to maintain advantage while conducting parallel operations across domains.[69]

This theoretical integration—combining Warden's systematic analysis, unrestricted warfare's multidomain operations, and Boyd's decision cycle framework—creates compounding advantages in practice. Consider China's

maritime militia operations in the South China Sea. Systems analysis reveals how these operations connect to broader territorial claims, economic interests, and regional influence efforts. Unrestricted warfare theory enables simultaneous counterpressure through partner nation capacity building, economic initiatives, and information operations exposing coercive behavior. Boyd's OODA loop ensures these efforts maintain coherence while adapting to changing conditions faster than adversary response cycles.[70] This synchronized application of multiple instruments of power creates effects that would be impossible through single-domain operations. [71]

The theoretical synthesis of these three frameworks requires organizational innovation to enable practical implementation. Traditional interagency processes, designed for sequential policy development rather than integrated operational execution, cannot achieve the speed and synchronization this framework demands. To operationalize this theoretical synthesis, leaders should establish an Interagency Action Committee on China (IAC-C) positioned adjacent to the National Security Council's Deputies Committee with a focus on policy execution, rather than policy recommendations.[72] This organizational structure enables rapid OODA loop completion crucial to Boyd's framework while aligning with national objectives.[73]

The IAC-C's mission centers on countering Chinese unrestricted warfare operations through coordinated defensive measures and competitive actions below the threshold of armed conflict, while also executing synchronized cross-domain operations to advance U.S. policy objectives within American legal and ethical constraints.[74] Rather than conducting unrestricted warfare as defined by Qiao and Wang—which remains outside U.S. doctrine—the IAC-C would orchestrate whole-of-government campaigns that both defend against adversary operations and proactively shape the competitive environment. This dual approach includes defensive measures such as countering political warfare, protecting critical infrastructure and economic systems, and exposing malign influence operations, while simultaneously executing offensive initiatives including economic statecraft, information campaigns, diplomatic pressure, and technology competition to achieve strategic advantage. When necessary and legally authorized, the IAC-C would coordinate competitive actions across all domains—diplomatic, informational, military, and economic—to impose costs on adversary behavior and advance American interests, always maintaining adherence to U.S. legal frameworks and ethical standards that distinguish American statecraft from authoritarian approaches. By combining representatives and leaders from relevant agencies with regional combatant commanders under a flattened organizational structure, the IAC-C enables the speed and adaptability that Boyd's framework requires while maintaining the coherence that Warden's systems approach demands.[75]

The IAC-C's value as a coordinating body naturally diminishes as competition escalates toward open conflict. During crisis, leadership should transition to the appropriate combatant commander, with other agencies moving into supporting roles to maintain cross-domain coordination while enabling clear military command and control.[76] This organizational flexibility ensures effective execution of irregular warfare during competition while preserving unity of command during conflict.[77] The IAC-C thus provides leaders and commanders with the organizational framework needed to implement this theoretical synthesis across the full spectrum of inter-state relations.

It is important to acknowledge, however, that the IAC-C represents merely one potential organizational manifestation of this theoretical synthesis. Multiple institutional configurations could effectively implement these principles, depending on strategic or operational context, existing organizational architectures, and specific competitive domains. Nevertheless, any organizational framework designed to execute this theoretical synthesis must incorporate several fundamental capabilities that transcend specific structural arrangements. While the IAC-C provides one concrete organizational model for implementing this theoretical synthesis, any effective structure must embody certain fundamental principles that transcend specific institutional arrangements. Understanding these core principles illuminates how organizations must evolve to meet the demands of modern great power competition.

Principles of a Cross-Domain Organization

The synthesis of Boyd's OODA loop, Warden's systems analysis, and unrestricted warfare theory demands an organizational structure that can implement these concepts effectively. While the Interagency Action Committee on China represents one potential manifestation, any organization executing this theoretical framework must incorporate several fundamental capabilities.

Understanding Across Domains

A successful cross-domain organization requires a sophisticated understanding of perspectives across diplomatic, economic, military, technological, and informational domains, transcending simple data collection to achieve genuine analytical integration. This shared understanding, which Boyd emphasized through his concept of "similar implicit orientation," establishes the foundation for unity of effort.

The IAC-C demonstrates this principle by bringing together representatives from the Department of State, Department of Defense, Treasury, Commerce, Intelligence Community agencies, Department of Justice, and Department of Homeland Security.[78] This composition ensures coverage of diplomatic,

military, economic, legal, and domestic security equities while maintaining a manageable span of control. Law enforcement participation through the Department of Justice (DOJ) and the Department of Homeland Security (DHS) proves essential for addressing adversary operations within U.S. borders, while Treasury's inclusion enables synchronized economic statecraft.[79] When an economic analyst identifies potential vulnerabilities in China's energy supply chain, diplomatic and military representatives immediately grasp the strategic implications without lengthy explanations.

Flexibility in Structure

Structural agility enables four critical functions: delegating authority to appropriate organizational levels; flexibly designating main effort domains based on strategic priorities; rapidly incorporating subject matter experts; and minimizing friction from hierarchical structures.

Within the IAC-C, this flexibility manifests through its unique position adjacent to the Deputies Committee. This placement allows it to quickly shift priorities when opportunities arise while maintaining alignment with national objectives. For example, if intelligence reveals a new Chinese influence operation targeting Pacific Island nations, the IAC-C can rapidly reallocate resources and attention without waiting for a lengthy approval processes, demonstrating the adaptability that Boyd identified as crucial for maintaining initiative.

Smart Analysis of Systems

The organization must integrate sophisticated systems analysis methodologies that not only identify vulnerabilities within Warden's five rings but also map how these vulnerabilities intersect across domains. This enables identification of critical nodes where synchronized actions can generate compound effects.

The IAC-C applies this principle through Joint analytical cells that continuously examine China's system components—from leadership structures to economic vulnerabilities—and identify where coordinated pressure can achieve strategic effects. When analyzing China's Belt and Road infrastructure investments in Southeast Asia, these cells identify connections between economic leverage, potential military logistics networks, and diplomatic pressure points that can be exploited through coordinated action.

Coordinated Action Across Boundaries

Effective implementation requires cross-domain operational synchronization underpinned by appropriate authorities from senior leadership. This enables the simultaneity that Warden identified as crucial while providing the operational flexibility Boyd's OODA loop demands.

The IAC-C exemplifies this principle through its authority to coordinate operations across traditional agency boundaries. For instance, when countering China's maritime militia operations in the South China Sea, the IAC-C can synchronize partner nation capacity building (Department of Defense), economic initiatives (Treasury/Commerce), and information operations (State Department) to create effects that would be impossible through single-domain efforts. This synchronized application of multiple instruments generates the compound effects that unrestricted warfare theory identifies as decisive in contemporary competition.

Strategic Merit of the Concurrent Integrated and Synchronized Approach

Organizations implementing these principles represent a fundamental departure from conventional interagency coordination. Where traditional frameworks operate through sequential planning processes with minimal synchronization, cross-domain organizations function through concurrent integration from the outset. Rather than developing separate plans that must later be reconciled, representatives with decision-making authority collaborate simultaneously from conception through execution. This shift from "retrofitted integration" to "inherently integrated" planning eliminates the temporal gaps that adversaries exploit through accelerated decision cycles.[80] The resulting operational tempo enables the compounding effects that unrestricted warfare theory identifies as decisive in modern competition, while maintaining the precision targeting that Warden's systems analysis demands. The IAC-C exemplifies this approach by enabling senior representatives to develop comprehensive implementation strategies incorporating mutually reinforcing effects across all competitive domains, rather than attempting to harmonize separate agency initiatives after they have been developed.

Conclusion

The synthesis of Boyd's OODA loop, Warden's systems analysis, and unrestricted warfare theory provides military and civilian leaders with a powerful framework for modern great power competition. This integration enables systematic identification of vulnerabilities, orchestration of cross-domain effects, and maintenance of decisive advantage through superior observation and adaptation. The proposed Interagency Action Committee on China demonstrates how organizations can implement this synthesis. As interconnected technologies and societies create novel vulnerabilities while enabling new methods of exploitation, states that master this integrated approach—systematically analyzing adversary systems, orchestrating cross-domain effects, and maintaining faster decision cycles—will dominate twenty-first century competition.

Endnotes

1. *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Department of Defense, 2018), 2.
2. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999); John R. Boyd, "A Discourse on Winning and Losing," unpublished collection of briefings, Air University Library, Document No. M-U 43947 (August 1987); Boyd, "Patterns of Conflict," unpublished briefing (1986); John A. Warden III, "The Enemy as a System," *Airpower Journal* 9, no. 1 (Spring 1995): 40–55; and John A. Warden III, "Air Theory for the Twenty-first Century," in *Challenge and Response: Anticipating U.S. Military Security Concerns*, ed. Karl P. Magyar (Maxwell AFB, AL: Air University Press, 1994).
3. The PLA's modernization marked a fundamental shift from Mao's mass mobilization doctrine toward recognizing the vital role of technology in modern warfare. This transformation reflected both internal assessments of PLA capabilities and external observations of evolving warfare requirements. Geoff Babb, "China's Military History and Way of War: A Backgrounder," *Military Review* (March 2023): 1–6.
4. Babb, "China's Military History and Way of War," 2–3.
5. Operation Desert Storm was the combat phase of the Gulf War, preceded by Operation Desert Shield's five-month buildup. The 42-day air campaign and 100-hour ground war demonstrated revolutionary advances in precision strike, stealth technology, and information warfare that fundamentally changed military thinking worldwide. See Keith L. Shimko, *The Iraq Wars and America's Military Revolution* (Cambridge, UK: Cambridge University Press, 2010), 51–89, https://doi.org/10.1017/CBO9780511845277. Their political warfare backgrounds shaped their theoretical approach to unrestricted warfare, extending analysis beyond conventional military operations into comprehensive national power employment. See Dean Cheng, "Chinese Lessons from the Gulf War," in *Chinese Lessons from Other Peoples' Wars*, ed. Andrew Scobell, David Lai, and Roy Kamphausen (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2011), 5–7.
6. Prior to Operation Desert Storm, Chinese military doctrine focused primarily on continental defense against Soviet-style armies. The conflict forced a wholesale reevaluation of how warfare could be conducted across multiple domains simultaneously.
7. Qiao and Xiangsui, *Unrestricted Warfare*, 8–12.
8. Thomas A. Keaney and Eliot A. Cohen , *Gulf War Air Power Survey: Summary Report* (Washington, DC: Department of Defense, 1993), 235–51.
9. Desert Storm demonstrated how coalitions could leverage UN legitimacy and economic sanctions to shape the operational environment before military action. See Thomas G. Mahnken and Barry D. Watts, "What the Gulf War Can (and Cannot) Tell Us about the Future of Warfare," *International Security* 22, no. 2 (Fall 1997): 151–62, https://doi.org/10.1162/isec.22.2.151.
10. Qiao and Wang, *Unrestricted Warfare*, 21–25.
11. The concept of "unrestricted warfare" does not mean warfare without any limits, but rather warfare unconstrained by traditional boundaries between military and nonmilitary activities. The authors argue that maintaining artificial distinctions between these spheres creates strategic vulnerabilities.
12. Supranational combinations represent coordinated actions between state and nonstate actors to achieve strategic effects. During Operation Desert Storm, this manifested primarily through UN sanctions and Coalition military operations, but the authors envisioned broader applications.
13. Qiao and Wang, *Unrestricted Warfare*, 177–79.
14. *Supradomain combinations* refer to orchestrating actions across multiple spheres (military, economic, diplomatic, etc.) to create synergistic effects that compound and re-

inforce each other. The authors believed Operation Desert Storm demonstrated this potential but did not fully exploit it.

15. Qiao and Wang, *Unrestricted Warfare*, 134–37.
16. *Supra-means* combinations expand available tools beyond traditional military hardware to include any method capable of achieving strategic effects. This concept reflects traditional Chinese strategic thought about indirect approaches while incorporating modern financial, technological, and nonstate actors.
17. Qiao and Wang, *Unrestricted Warfare*, 141–46.
18. While focusing on Chinese perspectives, the authors acknowledged that any actor could potentially employ unrestricted warfare concepts. They specifically warned that nonstate actors might prove particularly adept at coordinating actions across multiple domains.
19. Qiao and Wang, *Unrestricted Warfare*, 162–66.
20. Qiao and Wang, *Unrestricted Warfare*, 189–93.
21. This framework fundamentally reframes competition by shifting focus from matching capabilities to exploiting systemic vulnerabilities through coordinated multidomain operations. This approach particularly appeals to actors facing technologically superior adversaries.
22. Qiao and Wang, *Unrestricted Warfare*, 199–202.
23. The authors drew heavily from Sun Tzu's concept that "supreme excellence consists in breaking the enemy's resistance without fighting." Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (Oxford, UK: Oxford University Press, 1963), chap. 3. They saw unrestricted warfare as a modern application of this principle using twenty-first century tools and methods.
24. Qiao and Wang, *Unrestricted Warfare*, 208–10.
25. John R. Boyd, "Destruction and Creation" (unpublished paper, 3 September 1976), 1–9.
26. Chet Richards, "Boyd's OODA Loop," *Necesse* 5, no. 1 (2020): 142–65; and Boyd, "Destruction and Creation," 2–3.
27. *Active information collection* refers to deliberate efforts to gather and filter data rather than passive receipt of information. This requires dedicated resources and attention across all relevant competitive domains.
28. Richards, "Boyd's OODA Loop," 146–47.
29. Orientation represents the process by which organizations create meaning from observations. It combines cultural traditions, genetic heritage, information, and previous experience to generate understanding.
30. Boyd, "Destruction and Creation," 3–4.
31. Richards, "Boyd's OODA Loop," 148.
32. *Purposeful action* refers to operations designed to shape the competitive environment by affecting both immediate conditions and future possibilities, rather than simply responding to current circumstances.
33. Richards, "Boyd's OODA Loop," 149.
34. Richards, "Boyd's OODA Loop," 149–52; and Boyd, "Destruction and Creation," 4–5.
35. Domains encompass all areas where organizations must gather and process information, including physical, electromagnetic, informational, and cognitive realms.
36. Richards, "Boyd's OODA Loop," 150–51.
37. *Strategic coherence* refers to maintaining alignment between actions at all levels while adapting to changes in the competitive environment.
38. *Fulcrum* in this context refers to the pivotal point around which competitive advantage is generated and maintained through superior information processing.
39. *Fingerspitzengefühl* describes an intuitive mastery developed through repeated application of Boyd's destruction and creation process, enabling rapid and appropriate action without conscious analysis.
40. Richards, "Boyd's OODA Loop," 155–56.
41. David S. Fadok, *John Boyd and John Warden: Air Power's Quest for Strategic Paralysis* (Maxwell AFB, AL: Air University Press, 1995).

42. *Tempo* refers to the relative rate that organizations can complete effective observation-orientation-decision-action cycles compared to their opponents.
43. Richards, "Boyd's OODA Loop," 157–58.
44. Warden III, "Air Theory for the Twenty-first Century."
45. *Strategic paralysis* refers to rendering an enemy's leadership unable to effectively command and control their forces or respond to attacks, even if those forces remain physically intact.
46. John A. Warden III, "The Enemy as a System," *Airpower Journal* 9, no. 1 (Spring 1995): 40–55.
47. Warden, "The Enemy as a System," 43–44.
48. A system in Warden's model can be any organized entity with clear leadership, essential processes, connecting infrastructure, human elements, and protective mechanisms.
49. Warden, "The Enemy as a System," 45–46.
50. *System essentials* refers to those processes or capabilities without which the system cannot function. Their specific nature varies based on the system being analyzed but always represents critical enabling functions.
51. Warden, "The Enemy as a System," 46–47.
52. The Five Rings maintain consistent functional relationships even as their specific components change based on the system being analyzed. Each ring serves the same role regardless of scale or type of organization.
53. Warden, "The Enemy as a System," 47–48.
54. *Centers of gravity* represent nodes within each ring whose destruction would create disproportionate systematic effects compared to the effort required to attack them.
55. Warden, "Air Theory for the Twenty-first Century," 47–48.
56. *Parallel warfare* represents a departure from traditional "serial" warfare where targets were attacked sequentially. By striking multiple targets simultaneously across different rings, parallel warfare overwhelms an enemy's ability to adapt or repair damage.
57. Warden, "Air Theory for the Twenty-first Century," 238–39.
58. Warden, "The Enemy as a System," 52–53.
59. Cohen and Keaney, "Gulf War Air Power Survey," 240–41.
60. Warden, "The Enemy as a System," 52–53.
61. *Joint Operations*, Joint Publication 3-0 (Washington, DC: Department of Defense, 2022), I-10–I-12.
62. System components create networks of interdependence where changes in one area necessarily affect multiple other components through cascading effects across domains.
63. Jeffrey S. Lehmkuhl, "Irregular Influence: Combating Malign Chinese Communist Party Actions in Southeast Asia," *Journal of Indo-Pacific Affairs* (15 November 2023): 38–40.
64. Qiao and Wang, *Unrestricted Warfare*, 189–93.
65. Jason English, "Taming the Dragon: Countering China's Asymmetric Warfare," *Babel Street* (blog), accessed 28 August 2025.
66. Warden, "The Enemy as a System," 47–48.
67. Richards, "Boyd's OODA Loop," 146–47.
68. Orientation enables rapid processing of information while maintaining accurate understanding of the competitive environment across all relevant domains.
69. Richards, "Boyd's OODA Loop," 146–47.
70. *Response cycles* refer to the time required to observe, orient, decide, and act in response to changes in the competitive environment. Faster cycles enable maintaining initiative through superior adaptation.
71. Qiao and Wang, *Unrestricted Warfare*, 204–6.
72. Additional committees such as IAC-Russia and IAC-Iran should be considered for other strategic competitors. "What Is the National Security Council?," Council on Foreign Relations, 15 September 2025.
73. Richards, "Boyd's OODA Loop," 155–56.
74. Frank G. Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," *PRISM* 7, no. 4 (2018): 30–47; and *Summary of the Irregular Warfare*

Annex to the National Defense Strategy (Washington, DC: Department of Defense, 2020), 2.

75. "What Is the National Security Council?" Flattened organizational structure reduces decision-making layers while maintaining coordination across all elements of national power, enabling faster OODA loops in complex operations.
76. R. Kim Cragin, "Confronting Irregular Warfare in the South China Sea: Lessons Learned from Vietnam," *Military Review* (November–December 2024): 72–73. Unity of command becomes increasingly critical as competition escalates toward conflict, requiring clear lines of authority while maintaining interagency coordination capabilities.
77. The IAC-C's operations align with the doctrinal definition of irregular warfare as employing "the full range of military and other capabilities" to influence populations and erode adversary power through indirect approaches. See *Summary of the Irregular Warfare Annex to the National Defense Strategy*, 2.
78. The shift from sequential to concurrent planning reflects lessons from Joint operations. See *Joint Planning*, Joint Publication 5-0 (Washington, DC: Department of Defense, 2020), III-32–III-35.
79. Lehmkuhl, "Irregular Influence," 42–45.
80. Lehmkuhl, "Irregular Influence," 42–45.

The Role of Artificial Intelligence in the U.S. Military Strategy in Proxy Wars, 2020–2024

Ehsan Ejazi and Mahsa Ahmadyan

Abstract: Proxy war has been a dynamic U.S. military strategy since the Cold War. In recent decades, however, artificial intelligence (AI) as a new manifestation of technology has played a significant role in these wars. The United States has been a pioneer in this field, making substantial investments, annually allocates multibillion-dollar budgets to advance robotic and automated weapons to win future wars. Artificial intelligence proxy wars can manage the competition between international actors as a mediating factor without wasting human resources. The main question of this article is as follows: What is the role of artificial intelligence in U.S. military strategy, and how much can this new technology help win proxy wars? The findings indicate that the United States, by applying artificial intelligence technology to its military equipment with remote control capabilities, robots, and automated guided weapons, has reduced human and financial costs while increasing the probability of triumph on the battlefield. However, the obtained data, according to moral and humanitarian criteria, suggest a high rate of civilian casualties in such military conflicts.
Keywords: artificial intelligence, AI, proxy war, military strategy, drones, automated weapons

Many analysts view the world order and American hegemony as influenced by nuclear arms races, economic shifts, and various treaties and alliances. The United States has consistently leveraged these factors

Ehsan Ejazi is a board member of the Iranian Association of West Asian Studies and a lecturer at various Iranian universities. He earned a PhD in international relations from the University of Guilan. His research focuses on U.S. foreign policy, Iran-U.S. relations, U.S. military strategy, and conflicts in the Middle East, particularly the Palestine-Israel conflict. Mahsa Ahmadian is a researcher in the American Studies Group at the Iranian Association of West Asian Studies. She holds a master's degree in North American studies from Allameh Tabataba'i University.

Journal of Advanced Military Studies vol. 16, no. 2
Fall 2025
www.usmcu.edu/mcupress
https://doi.org/10.21140/mcuj.20251602007

to maintain its position. According to Samuel Huntington's predictions, the current international order is transitioning toward a unipolar-multipolar dynamic, where emerging technological issues in the economy and military could become key challenges.[1] The rise of AI in these areas, along with its critical role in optimizing resources and preserving hegemony, has made it a strategic asset for U.S. rivals like China in pursuing global competitiveness.

World leaders, including Barack H. Obama, Donald J. Trump, Xi Jinping, and Vladimir Putin have made critical statements about the prominence of AI. This importance can be summed up in Putin's September 2017 speech: "Whoever becomes the leader in AI will rule the world."[2] This context has developed since 1956, but interest in this field has increased since 2010. Despite the existence of opponents and supporters in AI war applications, Daniel Araya and Meg King have provided predictions about the scale of the impact of AI on the future nature of war that have three possible positions: minimal effect, evolutionary effect, and revolutionary effect.[3] This technology is viewed as a significant advantage for countries that possess it, benefiting both civilian and military sectors.

Specifically, China and the United States gain substantial economic and military benefits over their competitors, which could lead to a redefinition of the current balance of power. Gloria Shkurti Özdemir emphasizes that this technology should not be considered a unique weapon, but it should be regarded as an "enabler and all-purpose technology with multiple applications."[4] Therefore, while it can potentially enable several military innovations, it is not an army innovation itself.[5] The study of AI extends beyond military and hardware applications; it also encompasses cyberspace and media, where psychological warfare, fake news, and manipulated videos can alter the speeches of prominent figures and politicians, as well as their facial expressions. This technology enables the creation and execution of attacks against rival states.

AI functions as a proxy instrument with even greater efficiency than traditional forms of proxy warfare in managing the dynamics of competition and conflict between state and non-state actors. To date, this technology has functioned as a strategic deterrent, shaping the dynamics of international authority and prestige and has remained a focal point of bargaining and competition among major powers such as the United States. The main question of this article is what place AI has in the U.S. military strategy and how much this new technology can help the United States in proxy wars. The United States seeks to use AI in the form of hardware and software to achieve the most in future fights with the least cost.[6] In this regard, the U.S. Army is trying to conduct proxy wars in remote areas with the most negligible financial and human costs through remotely controlled military equipment, such as drones and robots. These platforms provide several advantages over traditional irregular warfare

weapons: they are smaller and more cost-effective, offer unparalleled surveillance capabilities, and minimize risks to soldiers.[7] The available evidence indicates that proxy wars through AI reduce the number of civilian casualties. In this context, the effective use of AI can positively impact civilian harm reduction.[8] Lauren Gould argues that, contrary to proponents of using drones in warfare, "In practice, AI is accelerating the kill chain—the process from identifying a target to launching an attack."[9]

Moreover, autonomous systems must be designed to minimize economic costs. This task is complex, as economic costs encompass not only the platform or munitions but also logistics, information technology, and the manpower needed for operation and maintenance. Furthermore, autonomy may be most cost-effective without human oversight, though this compromises control and safety. Therefore, autonomy may be best suited for missions that reduce overall warfare costs rather than those that replace manned missions.[10] For instance, robots do not have to be expensive or complicated; the Ukrainian military has successfully used modified commercial drones against Russian invaders.[11]

Research Background

In a report by Maggie Gray and Amy Ertan entitled *AI and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment*, they suggested that AI and autonomous systems will play an increasing role in enabling future military operations. Gray and Ertan, pointing to the evidence of China and Russia's active and aggressive efforts in acquiring military AI systems, emphasize the disastrous consequences of falling behind this technology. In addition to the importance of the military and weapons aspect, North Atlantic Treaty Organization (NATO) states must share information among their members in the field of supplies and facilities between the members and the recruitment of specialist forces, as well as create sufficient confidence for the military systems to remain advanced.[12] Brandon Tyler McNally wrote a thesis entitled "United States AI Policy: Building toward a Sixth-Generation Military and Lethal Autonomous Weapon Systems," which discussed and explained the capacity of AI as a new revolution in changing the strategic balance of power. He believes the United States, entangled in the Middle East and pursuing a long-term strategy for AI, has reduced its readiness for the sixth generation of military power. The United States' ability to harness talent and innovative capabilities across the military/civilian spectrum will be a determining factor in maintaining its strategic advantage over its competitors through the mid-twenty-first century.[13]

In her report entitled *Artificial Intelligence and the Future of Warfare*, Mary Louise Missy Cummings states that the development of autonomous military systems has been gradual at best, and its progress has been fragile compared to

the autonomous systems of the commercial sector. Indeed, research costs and development in this direction will significantly impact its types and quality. One of the essential issues in this field is whether defense companies can develop and test safe and controllable autonomous systems, especially weapons capable of firing. In other words, using nascent technologies without comprehensive testing can put the military and civilians at unnecessary risk.[14] Kai-Fu Lee's book, *AI Superpowers: China, Silicon Valley, and the New World Order,* examines China's progress in AI and discusses its tight competition with the United States for new technologies. China has developed at an astonishing and unexpected speed in AI and surpassed its rival, the United States. Kai Foley believes China will be the next superpower in the technology.[15] AI and autonomous systems are increasingly crucial in shaping military power and strategic balance. The United States and NATO must expedite innovation, collaboration, and talent development to counter advances from rivals like China and Russia, while ensuring these technologies remain safe and controllable. Achieving this balance is vital for maintaining security, stability, and global influence in the coming decades.

Theoretical Framework

Offensive realism posits that a government can best ensure its security by maximizing its power. This concept has sparked considerable debate among realists. For instance, some realists argue that excessive force can undermine a state's security, as it may provoke other states to counterbalance that power.[16]

John Mearsheimer argues that the anarchic nature of the international system is responsible for issues such as doubt, fear, security competition, and conflicts among great powers.[17] States are compelled to maximize their offensive capabilities and prevent rivals from gaining advantages at all costs. A state's ultimate goal is to achieve hegemony in the international system, as this is the only way to ensure its security fully. In this anarchic environment, the most effective strategy for maximizing safety is to pursue power maximization. However, one criticism of offensive realism is its inability to explain why costly wars sometimes occur against the interests of the initiating governments. Additionally, Mearsheimer and other realist analysts recognize that power maximization can be counterproductive, leading some countries to disaster.[18]

Proxy Wars in the Contemporary Era

The proxy war is a method between classical and modern war. A third actor manages this type of war to achieve strategic results. The host actor is out of the conflict, and their proxies enter this strategic field by providing financing, training, and weapons to the host. A proxy war is a logical alternative for states that seek to advance their strategic goals but refrain from engaging in direct,

costly, and bloody war.[19] One of the most widely used definitions for this concept during the Cold War belongs to Karl Deutsch. He defines *proxy war* as an international conflict in which two foreign powers use a third actor's military might and other resources to align with their interests, goals, and strategies.[20]

The origin of proxy wars dates back to the Cold War, during which the Soviet Union engaged nonstate actors in conflicts instead of confronting the United States directly.[21] After the Cold War, despite initial optimism about reduced conflicts and the emergence of pacifist models, war remained a dominant force in international politics. The expansion of the concept of "region" in security studies allowed regional actors to independently provide financial and military support to vulnerable groups and governments, thereby regionalizing proxy wars. Additionally, rising costs and the destructive impacts of direct warfare prompted both regional and global powers to adopt strategies focused on proxy conflicts. During these conflicts, two parties engage indirectly, with a third party acting on behalf of one side. The aim is to limit the conflict's scale to prevent it from escalating into a full-scale war. Proxy wars typically occur in strategically significant areas near the rival's borders or even within their territories, using internal resources for their execution.[22] Scholars like Geraint Hughes argue that governments cannot serve as proxies, as history demonstrates that they will intervene when it aligns with their interests.[23] Consequently, the intervention of a proxy agent may be negligible. In contrast, Yaakov Bar-Siman-Tov categorizes proxies into two types: those that intervene by force and those that do so voluntarily due to "compatibility of interests."[24] State A may initially request state B to represent it, whether through coercion or voluntary agreement.[25]

The following summary explains the total realistic approach to proxy wars. With proxy war and strategic changes, neorealists claim that states do not act with the rational decision-making process they enter into. Indeed, their decisions are related to the position of the respective actors and competitors in the system.[26] The existence of new proxy wars somehow reproduces international anarchy within the state. Therefore, it is impossible to distinguish the domestic territory from the foreign domain.[27] Offensive realists highlight the ability of states to initiate proxy wars driven by material capabilities, viewing the power of the sponsoring state as the most critical aspect of the discussion.[28]

When there is a lack of trust between states, proxy war becomes a tool to validate alliances and coalitions. Conversely, if state A is more powerful than state B, the best option for state B is to resort to a proxy war. Moreover, the importance of public opinion in democratic countries and concern about international reactions to direct entry into war with another country increases the tendency to proxy war.[29] Many experts analyze this component within the framework of offensive realism, as it channels the hostile motives of conflicting

actors toward maximizing power. Consequently, the costs of war are minimized due to the absence of direct confrontation with the host state.

From Early Concept to Strategic Leverage: The U.S. Artificial Intelligence Trajectory

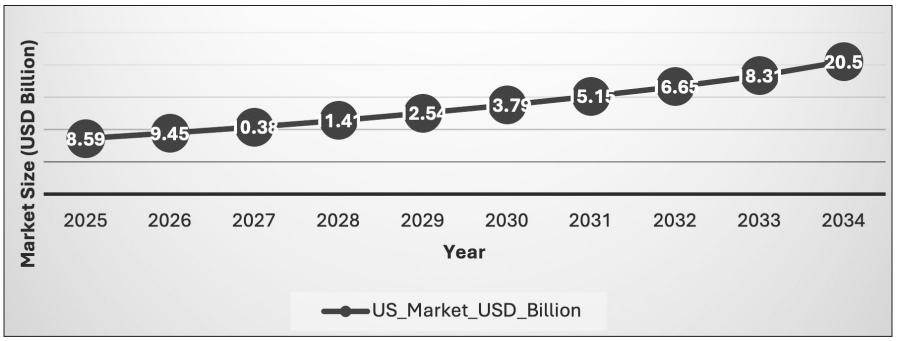
The term AI was first coined by John McCarthy in 1956 when he held the first academic conference in this field. In this regard, Alan Turing wrote an article about the concept of machines that can simulate humans with the ability to perform intelligent tasks such as playing chess. Using the brainpower of experts to help others has always been the main driving force behind the development of expert systems. This issue is one of the most positive potentials of AI.[30] In 2010, America's big tech attracted more than 60 small AI companies.

The President's Council of Advisors on Science and Technology predicted that American companies will spend more than $100 billion annually on AI research and development by 2025. Many of the world's largest AI companies are American. These companies pay more than $76 billion annually on research and development, making the total value of their investment markets more than $5 trillion.[31] The research and development activities of U.S. multinational companies abroad can strengthen the technological ecosystem of other states in different ways. Some industry experts argue that if Microsoft had not established its Asian research, China could not have created its own AI ecosystem. In 2019, then chairman of the Joint Chiefs of Staff, General Joseph F. Dunford, stated that Google's work in China indirectly benefits the Chinese military. Despite these claims, Microsoft and Google have rejected them.[32] The U.S. competition with China and its proxy wars, particularly in the Middle East, are significant factors. The U.S. AI market in aerospace and defense was valued at $7.82 billion (USD) in 2024 and is projected to reach approximately $20.50 billion by 2034.[33]

Military Dimensions

The deployment of AI as a part of the Third Offset Strategy of the United States was launched in 2014 by then Secretary of Defense Chuck Hagel to revive the U.S. military. The main focus of the Third Offset Strategy is on robotics and autonomy, in which AI plays an important role. Despite the opportunities that previous presidents created to become the world leader in AI, they always faced internal and external limitations.[34] The Defense Advanced Research Projects Agency (DARPA), which leads the Department of Defense regarding AI research and development, requested $3.17 billion in 2018 and $3.44 billion in 2019. Additionally, in 2018, DARPA announced a multiyear investment of more than $2 billion in new and existing programs called the AI Next Campaign.[35]

Figure 1. U.S. AI in aerospace and defense market size and forecast 2025 to 2034



Source: "AI in Aerospace and Defense Market," Precendence Research, 10 July 2025.

The military uses AI, which is widely related to drone technology. Drones are uncrewed aerial vehicles that have a variety of uses. When drones were first used, they were controlled remotely and manually. However, today, the integration of drones equipped with AI and advanced technologies—such as high-resolution cameras, infrared and thermal imaging, microphones, various sensors, and both guided and unguided missiles—into the command, control, computers, communications, cyber, intelligence, surveillance, and reconnaissance (C5IRS) system greatly enhances the effectiveness of combat units. This advanced technology provides real-time, accurate information about events and allows for target destruction without endangering human lives, while simultaneously relaying situational updates to the battlefield command center.[36] The following table shows examples of drones used by the Pentagon.

Unmanned systems operating underwater, on the surface, on land, and in the air require exceptionally high processing power to function autonomously.[37] Mike Southworth, a production manager in the defense field, says an automated device needs different technologies to function properly. Analyzing large volumes of data and complex algorithms requires significant processing capabilities.[38] AI is now a military reality. For example, guided weapon systems can make decisions independently of the human agent. Also, AI systems allow independent and autonomous decision making through a network of operators who work with computers. Such systems can perform several actions consecutively and quickly, even in uncertain conditions. Soon, intelligent and autonomous platforms will have faster maneuvering speed and use force more accurately than platforms that work with human guidance.[39] AI has driven the development of autonomous weapons, including drones. They can perform a range of operations, from long-range aerial surveillance and deterrence to monitoring nuclear developments in other countries and executing attacks.[40]

DARPA has transferred newly developed defensive capabilities from its

Table 1. Drones used by the Pentagon

Drones	Service	Performance details of drones in the U.S. armed forces
General Atomics MQ-1C Gray Eagle	Ground force	The MQ-1C Gray Eagle is a ground-force drone operated through a dedicated and highly reliable command system. It offers long endurance and supports multimission capabilities across strategic, operational, and tactical levels. Its payload includes a laser rangefinder, laser designator, synthetic aperture radar, ground moving target indicator, communications relay, and Hellfire missiles. The Gray Eagle has been deployed in various operational theaters, including Iraq, Syria, Afghanistan, South Korea, India, and the Republic of Niger.
AAI RQ-7 Shadow 200	Ground force	In the U.S. Army, the U.S. Marine Corps, the Australian Army, and the Italian and Swedish armed forces, the AAI RQ-7 Shadow 200 is used to locate and identify targets up to 125 kilometers from a tactical operations center. This system detects vehicles day and night from a height of 800 feet and a slope range of 3.5 kilometers. The Shadow UAV was deployed in Iraq in January 2004 and Afghanistan in August 2010 by the Australian Ministry of Defence.
Northrop Grumman RQ-4 Global Hawk	Air Force	This high-altitude and long-endurance drone can fly at 60,000 feet and stay in the air for more than 34 hours. The range of its cameras and sensors is confidential. However, the line of sight is about 340 miles. The U.S. Air Force has used it since 2001 in Afghanistan, Iraq, and North Africa.
General Atomics MQ-9A Reaper (a.k.a. Predator)	Air Force	The MQ-9A Reaper boasts an endurance of more than 27 hours, a speed of 240 knots true airspeed, and an operational ceiling of 50,000 feet. It has a payload capacity of 3,850 pounds (1,746 kilograms), which includes 3,000 pounds (1,361 kilograms) of external stores. This aircraft can carry five times more payload and has nine times the horsepower than other drones. Predator, the world's first armed drone, mainly operates in Iraq, Afghanistan, and Pakistan.
AeroVironment RQ-20	Navy	This unmanned aerial vehicle (UAV) is used for tactical information, surveillance, reconnaissance, targeting, maritime patrol, search and rescue, combating illegal smuggling, and supporting ground operations. Its length is 1.4 meters, and it weighs 6.3 kilograms. Only two people are needed to assemble it. Its functions have been in Afghanistan for reconnaissance.
AeroVironment RQ-11 Raven	Navy	This lightweight UAV is designed for rapid deployment and high mobility in military and commercial operations. Additionally, it fulfills the Army's requirements for reconnaissance, surveillance, and low-altitude target acquisition. The U.S. Army, Air Force, Marine Corps, and Special Operations Command are the primary users of Raven. U.S. allies such as Australia, Italy, Denmark, Great Britain, and Spain also use it. It is the most advanced small unmanned aircraft system in the U.S. Armed Forces. Examples of its operational use have been in Afghanistan for surveillance and reconnaissance.

Sources: *MQ-1C Gray Eagle Unmanned Aircraft System (MO-1C Gray Eagle)* (Washington, DC: Department of Defense, 2019); "Shadow 200 RQ-7 Tactical Unmanned Aircraft System," *Army Technology*, 13 March 2020; Hanan Zaffer, "Japan Receives First of Three RQ-48 Global Hawks from U.S.," *Defense Post*, 18 March 2022; "MQ-9A 'Reaper'," General Atomics Aeronautical, accessed 20 August 2022; "RQ-20B Puma AE Small Unmanned Aircraft System (UAS)," *Naval Technology*, 15 August 2016; and "RQ-11 Raven Unmanned Aerial Vehicle," *Army Technology*, 22 July 2021.

Guaranteeing AI Robustness Against Deception (GARD) program to the Chief Digital and Artificial Intelligence Office. GARD is part of DARPA's broader artificial intelligence efforts, which the agency has pursued since its founding in 1958 and has intensified in recent years.

Currently, approximately 70 percent of DARPA's programs focus on AI, machine learning, or autonomous systems. The Pentagon requested $10 million for the program in its fiscal year 2024 budget, but no funding was allocated for 2025 as the initiative is concluding.[41]

In President Donald J. Trump's 2025 budget request, $20 billion is invested in primary research agencies, an increase of $1.2 billion during fiscal year 2023, to advance and strengthen America's leadership in scientific research and discovery. An additional $32 million is earmarked for digital and public services and personnel to support AI talent.[42] Research, development, testing, and evaluation have played a crucial role in advancing the department's innovative initiatives to align with the Department of Defense's strategic goals, bolster national security, and enhance defense capabilities. Of the $143.2 billion invested in this area, $17.2 billion is designated for science and technology, particularly in artificial intelligence and next-generation programs.[43]

These investments not only advance technological innovation but also shape how the United States leverages military strategy in contemporary conflicts. Today, military strategists use proxy wars to avoid the costs of direct conflict. Proxy wars serve as a strategic alternative for states aiming to achieve their goals while avoiding direct, costly, and bloody conflicts.[44] Proxies provide a means to combat escalation. States frequently deny their support for these proxies; for instance, Russia asserted it was not involved in Ukraine, despite having funded various groups opposing the Kyiv government and supplied them with arms and support.[45]

Russia supported its former client states in Syria and Libya by deploying Chechen task forces and private military contractors. This aligns with its long-standing strategy of using private forces to extend its influence in areas where direct intervention would be challenging. This approach was evident in the Black Sea region and Ukraine, where Moscow's use of "little green men" allowed it to operate below the threshold for U.S. intervention while maintaining plausible deniability.[46]

In the meantime, the United States is trying to avoid the expense and risks of military occupation and direct rule over a hostile state or nonstate actor through proxy forces. In addition to great powers like the United States, nonstate actors can achieve their strategic goals at a lower cost by using advanced technologies such as remote targeting, cyber warfare, and AI. Nevertheless, the investigation of the number of deaths on the battlefield in the Middle East shows that the number of deaths in proxy wars in the years after 2011 has in-

creased compared to Middle East wars during the Cold War. Additionally, the number of refugees has been higher since the end of World War II, all of which were caused by civil and proxy wars in Syria, Yemen, and Libya following the Arab Spring in 2011.[47] Statements like "we will develop innovative, low-cost, and compact approaches to achieve our security objectives" and "the U.S. military will invest as needed to ensure effective operations in anti-access and area denial (A2/AD) environments" reflect an understanding of the potential for utilizing proxy war strategies in regions where direct military intervention may be too costly or risky in the coming years.[48]

The Pentagon's Use of AI in Military Strategy

The U.S. Project Maven is one of the most well-known cases of AI combining intelligence, surveillance, and reconnaissance applications. This project was designed to support the war against Islamic State of Iraq and Syria (ISIS) in Iraq and Syria. This ongoing project processes and interprets information received from videos taken by drones. As algorithms are developed, AI may be used for command and control, including managing battles, by analyzing large data sets with predictions to guide human activities.[49] The U.S. military is trying to step into the field of AI in future wars. In this regard, internal Pentagon documents and senior government officials clearly show that the Department of Defense is working to prevent this technology's rejection and create a plan that may be used in a new type of warfare.[50]

In June 2018, Google withdrew from the aforementioned Project Maven, which uses AI software, and then published a set of AI principles that indicated that the company did not use AI to create weapons and technologies that harm people. Defense officials have long worried that Google might aid China, America's chief competitor in AI, and its withdrawal from Project Maven left the Pentagon frustrated and scrambling for alternatives. Maven, the military's first serious AI experiment, aimed to create algorithms that could help intelligence analysts identify potential targets from drone footage, but Google's exit underscored the Pentagon's vulnerability in attracting top tech talent.[51] Since then, Google has intensified its commitment as a military contractor. In early 2025, to capitalize on federal contracts available under Trump, the company abandoned its pledge not to develop AI for weapons or surveillance.[52]

The Pentagon is researching combat scenarios in which AI would be allowed to operate automatically after receiving instructions from a human. Although the Pentagon has promised to establish an ethical AI army, such an undertaking will take work. Of course, the Pentagon realizes that arming existing commercial drones with human cognitive skills through AI can turn them into valuable weapons for insurgent and terrorist forces. Drones can be used to collect sensitive information, bypass physical obstacles on the ground, and carry out air

strikes with high efficiency. Meanwhile, political leaders want drones to have more autonomy and for the servicemembers to be able to delegate important and dangerous tasks to the drones. For example, in areas where the Global Positioning System (GPS) does not work or where there is severe electromagnetic interference, drones can significantly help the military forces with surveillance and reconnaissance.[53]

The limited progress in advancing autonomous military technologies stems not only from high costs and technical challenges but also from significant organizational and cultural resistance. In the United States, internal rivalries and a preference for manned systems have hindered the deployment of UAVs. For example, despite the Lockheed Martin F-22 Raptor's technical issues and minimal combat use, the Air Force is considering restarting its costly production rather than expanding drone programs, even though UAVs like the Predator are far cheaper and capable of most missions. Similarly, the X-47B is a groundbreaking unmanned aircraft developed by Northrop Grumman for the U.S. Navy, demonstrating significant advancements in carrier operations and autonomous refueling.[54] Both Services continue to prioritize the troubled, expensive Lockheed Martin F-35 Lightning II over unmanned alternatives. Many in the military accept drones only in support roles, as their broader adoption threatens traditional hierarchies and prestige associated with piloted aircraft.[55] Conversely, drone pilots are akin to video gamers, disconnected from the real-world consequences of their actions.[56] The Kratos XQ-58 Valkyrie serves as an excellent example of a stealthy unmanned combat aerial vehicle. Originally designed and built by Kratos, it was demonstrated to the U.S. Air Force through the Low-Cost Attritable Strike Demonstrator program, part of the Air Force Research Laboratory's Low-cost Attritable Aircraft Technology (LCAAT) project portfolio. The LCAAT initiative aims to reduce the rising costs of tactically relevant aircraft by offering an affordable, lightweight solution as an unmanned escort or wingman alongside crewed fighter aircraft in combat.[57]

Armed drones can fly to bases thousands of kilometers away to destroy the intended targets. The main advantage of drones is that they allow the military to attack the enemy while minimizing damage and casualties. However, drone attacks cause significant collateral damage, so many innocent citizens are killed along with the intended target. To reduce the cost of operating drones, manufacturers are increasingly producing them so that they can run automatically; they do not need instructions and human interaction. However, the automatic operation of military weapons raises severe ethical issues about liability for collateral damage from brutal drone strikes. The separation of humans from the decision-making process of drones during drone strikes makes it unclear who is responsible for the consequences of drone strikes: the robot, the programmer, or the military.[58] Therefore, it may be necessary to address the legal and ethical

dilemmas posed by drones, whether due to the technology or its application.[59] One of the main ethical dangers of drones is moral hazard. The low cost and growing accessibility of drone technology to various states and nonstate actors make targeted killings easier and, consequently, more frequent.[60]

In 2013, the prototype of the X47B autonomous drone landed, and in 2015, it performed automatic aerial refueling; in both cases, human intervention was only for the command to land or in-flight refueling, which was done by software. In 2016, the United States displayed 103 drones that flew together independently. The Pentagon described the move as systems that share a distributed brain to make decisions and coordinate with each other.[61] In 2020, for the first time, an automatic drone operating with AI, without any human consultation, targeted the Libyan forces of General Khalifa Haftar.[62] In addition to drones, the Department of Defense can employ other autonomous weapons. The Navy conducted a similar test in November 2016, when five uncrewed boats patrolled a particular section of the Chesapeake Bay and intercepted an opposing vessel.[63] The *Sea Hunter* is the first uncrewed antisubmarine warfare ship that DARPA transferred to the Department of the Navy. It was the first to travel autonomously from California to Hawaii and then back.[64]

In a report by *Foreign Policy*, the U.S. military has provided a robotic dog named Spot to help with demining and unexploded ordnance in Ukraine. Boston Dynamics announced the removal of mortar shells and cluster munitions in formerly Russian-controlled areas near the capital of Kyiv.[65] However, the Pentagon claims to use AI to help the military and not replace soldiers.

While the U.S. military will not allow a computer to pull the trigger, it has developed a "target recognition" system in drones, tanks, and infantry.[66] Also, one of the features of AI is that it can act quickly.[67] The U.S. Department of Defense must accept that nonstate groups and actors will acquire weapons powered by AI technology. These weapons are inexpensive for nonstate actors and, in contrast to nuclear weapons, are appealing because their development is relatively accessible to them. Even great powers may make AI weapons available to nonstate actors like conventional weapons.[68] Alex Karp, CEO of military contractor Palantir, has stated that AI-enabled warfare and autonomous weapons systems have reached their "Oppenheimer moment."[69] The affordability and ease of deploying AI weapons prompt both governmental and nongovernmental actors to incorporate them into their military strategies, as they involve lower financial and human costs.

Pentagon's AI Drones to Ukraine: A Proxy War Boost

U.S.-German autonomous software company Auterion has secured a Pentagon contract to provide 33,000 AI strike kits for Ukrainian drones, enhancing Kyiv's

efforts against Russia. This deal, part of Washington's latest security aid package, will increase the use of Auterion's technology in Ukraine tenfold, with deliveries anticipated by year-end. The technology has already been implemented in Kyiv and is currently utilized in autonomous combat missions against invading forces.[70] Ukraine's adoption of AI-enhanced weapons is not merely a step toward military modernization; it is a crucial act of survival. In an increasingly digitized battlefield, these systems provide speed, reach, and lethality while minimizing human risk. Ukraine's experience highlights both the potential and dangers of such technologies.[71] Ukrainian companies have developed various AI solutions for battlefield and defense applications. These include unmanned aerial and ground vehicles for tasks such as reconnaissance, surveillance, fire adjustment, target identification, logistics, and evacuation as well as electronic warfare systems to protect cities from enemy drones.[72] The Ukraine war has demonstrated that both urban centers and military sites are vulnerable to low-cost drones. Cities, public venues, and critical infrastructure should be regarded as potential targets.[73] Ultimately, the key factor in using drones in Ukraine is not about a less politically risky approach to warfare; it is primarily a matter of cost.[74]

Conclusion

The cost effectiveness and ease of deployment of AI weapons have enabled the United States to increase the use of this technology in line with its military strategies with less financial and forced cost. The recognition of AI technology as a part of the United States' Third Offset Strategy shows the importance and strategic position of this concept for the Pentagon, which focuses on robotic and automatic weapons. Despite the Pentagon's investments in projects such as Maven, due to the noncooperation of some companies and the opposition of a group of Pentagon officials due to violating moral and humanitarian rights, this project faced stagnation. Furthermore, the rise of AI presents challenges for nonspecialists and workers due to the potential for job displacement. A significant advantage of AI in proxy wars is its capacity to operate quickly and achieve optimal results by leveraging advanced hardware and software, thus gaining an edge in remote conflicts.

Drones enable the military to strike targets quickly and accurately. They can also communicate with other drones and jet fighters to locate targets more efficiently. These automated systems gather intelligence on various targets, providing valuable information for proxies. Additionally, drones facilitate easier and faster access to remote areas for both proxies and their supporters. Moreover, drones help save the lives of U.S. Marines and reduce collateral damage. Finally, by using drones, the United States can avoid deploying ground forces and aircraft carriers to equip and support its proxies abroad.

Endnotes

1. William C. Wohlforth, "The Stability of a Unipolar World," *International Security* 24, no. 1 (Summer 1999): 5–41, https://doi.org/10.1162/016228899560031.
2. Gloria Shkurti Özdemir, *Artificial Intelligence Application in the Military: The Case of United States and China* (Ankara, Turkey: SETA, 2019).
3. Daniel Araya and Meg King, *The Impact of Artificial Intelligence on Military Defence and Security* (Waterloo, Canada: Centre for International Governance Innovation, 2022).
4. Özdemir, "Artificial Intelligence Application in the Military."
5. Özdemir, "Artificial Intelligence Application in the Military."
6. In this article, the authors describe artificial intelligence (AI) as a cutting-edge technology utilized in the design, production, and operation of drones and other automated weapons.
7. Seth G. Jones, *The Tech Revolution and Irregular Warfare: Leveraging Commercial Innovation for Great Power Competition* (Washington, DC: Center for Strategic & International Studies, 2025).
8. Patrick Tucker, "Special Operators Hope AI Can Reduce Civilian Deaths in Combat," DefenseOne, 26 August 2024.
9. "Does AI Really Reduce Casualties in War?: 'That's Highly Questionable,' Says Lauren Gould," Utrecht University, 27 January 2025.
10. Jacquelyn Schneider and Julia Macdonald, "Looking Back to Look Forward: Autonomous Systems, Military Revolutions, and the Importance of Cost," *Journal of Strategic Studies* 47, no. 2 (2024): 162–84, https://doi.org/10.1080/01402390.2022.2164570.
11. Christopher Wall, "The Ghost in the Machine: Counterterrorism in the Age of Artificial Intelligence," *Studies in Conflict & Terrorism* (March 2025): https://doi.org/10.1080/1057610X.2025.2475850.
12. Maggie Gray and Amy Ertan, *Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment* (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2021), 19–22.
13. Brandon Teylor McNally, "United States Artificial Intelligence Policy: Building Toward a Sixth-Generation Military and Lethal Autonomous Weapon Systems" (PhD diss., Johns Hopkins University, 2021), 33–35.
14. M. L. Cummings, *Artificial Intelligence and the Future of Warfare* (London: Chatham House for the Royal Institute of International Affairs, 2017), 1–18.
15. Kai-Fu Lee, *AI Superpowers: China, Silicon Valley, and the New World Order* (Boston, MA: Houghton Mifflin, 2018).
16. Dominic D. P. Johnson and Bradley A. Thayer, "The Evolution of Offensive Realism: Survival under Anarchy from the Pleistocene to the Present," *Politics and the Life Sciences* 35, no. 1 (2016): 6, https://doi.org/10.1017/pls.2016.6.
17. Johnson and Thayer, "The Evolution of Offensive Realism," 17–18.
18. Johnson and Thayer, "The Evolution of Offensive Realism," 17–18.
19. Andrew Mumford, *Proxy Warfare* (Cambridge, UK: Polity Press, 2013), 1.
20. Vahít Güntay, "Analysis of Proxy Wars from a Neorealist Perspective: Case of Syrian Crisis," *TESAM Academy Journal* 7, no. 2 (2020): 499, http://dx.doi.org/10.30626/tesamakademi.788857.
21. Güntay, "Analysis of Proxy Wars from a Neorealist Perspective," 500.
22. Mohammad Hossein Ghanbari Jahromi, "Philosophy of Proxy Wars in the New Era," *Defense Policy Magazine* 29, no. 13 (2019): 21, 25.
23. Geraint Hughes, *My Enemy's Enemy: Proxy Warfare in International Politics* (Brighton, UK: Sussex Academic Press, 2012).
24. Yaacov Bar-Siman-Tov, "The Strategy of War by Proxy," *Conflict and Cooperation* 19, no. 4 (1984): 263–73, https://doi.org/10.1177/001083678401900405.
25. Benjamin Vaughn Allison, "Proxy War as Strategic Avoidance: A Quantitative Study of Great Power Intervention in Intrastate Wars, 1816–2010" (conference paper, Midwest Political Science Association 76th Annual Meeting Conference, Chicago, IL, 5–8 April 2018), 3.

26. Güntay, "Analysis of Proxy Wars from a Neorealist Perspective," 500.
27. Daniel Byman, *Deadly Connections: States that Sponsor Terrorism* (Cambridge, UK: Cambridge University Press, 2005), 37, https://doi.org/10.1017/CBO9780511790843.
28. Byman, *Deadly Connections,* 39.
29. Jahromi, "Philosophy of Proxy Wars in the New Era," 27, 46.
30. Chris Smith et al., *The History of Artificial Intelligence* (Seattle: University of Washington, 2006), 4, 16.
31. Roxanne Heston and Remco Zwetsloot, *Mapping U.S. Multinationals' Global AI R&D Activity* (Washington, DC: Center for Security and Emerging Technology, 2020), 4, https://doi.org/10.51593/20190008.
32. Heston and Zwetsloot, *Mapping U.S. Multinationals' Global AI R&D Activity,* 5.
33. "AI in Aerospace and Defense Market," Precedence Research, 10 July 2025.
34. Adam Lowther and Stephen Cimbala, "Future Technology and Nuclear Deterrence," *Wild Blue Yonder* (February 2020).
35. Özdemir, "Artificial Intelligence Application in the Military," 14, 16.
36. Aleksandar Petrovski, Marko Radovanović, and Aner Behlic, "Application of Drones with Artificial Intelligence for Military Purposes" (paper presented at the 10th International Scientific Conference on Defense Technologies OTEH 2022, Belgrade, Serbia, 13–14 October 2022), 99.
37. AI makes it possible for autonomous surface vessels and underwater drones to be used in the following applications: autonomous sea mine detection and neutralization are known as mine countermeasures. Ashikur Rahman Nazil, "AI at War: The Next Revolution for Military and Defense," *World Journal of Advanced Research and Reviews* 27, no. 1 (2025): 1998–2004, https://doi.org/10.30574/wjarr.2025.27.1.2735.
38. As quoted in Jamie Whitney, "Artificial Intelligence and Machine Learning for Unmanned Vehicles," Military & Aerospace Electronics, 26 April 2021.
39. Kenneth Payne, "Artificial Intelligence: A Revolution in Strategic Affairs?," *Survival* 60, no. 5 (2018): 8–9, https://doi.org/10.1080/00396338.2018.1518374.
40. Jeremy Julian Sarkin and Saba Sotoudehfar, "Artificial Intelligence and Arms Races in the Middle East: The Evolution of Technology and Its Implications for Regional and International Security," *Defense & Security Analysis* 40, no. 1 (2024): 97–119, https://doi.org/10.1080/14751798.2024.2302699.
41. Jon Harper, "DARPA Transitions New Technology to Shield Military AI Systems from Trickery," DefenseScoop, 27 March 2024.
42. Ed Pagano et al., "President Biden Unveils Key AI Priorities in FY2025 Budget Request," Akin, 20 August 2025.
43. Department of Defense, "Department of Defense Releases the President's Fiscal Year 2025 Defense Budget," press release, 11 March 2024.
44. Andrew Mumford, "Proxy Warfare and the Future of Conflict," *RUSI Journal* 158, no. 2 (2013): 40–46, https://doi.org/10.1080/03071847.2013.787733.
45. Daniel L. Byman, "Why Engage in Proxy War?: A State's Perspective," Brookings, 21 May 2018.
46. Candace Rondeaux and David Sterman, *Twenty-First Century Proxy Warfare: Confronting Strategic Innovation in a Multipolar World* (Washington, DC: New America, 2019).
47. Rondeaux and Sterman, *Twenty-First Century Proxy Warfare*.
48. Mumford, "Proxy Warfare and the Future of Conflict," 40–46.
49. Özdemir, "Artificial Intelligence Application in the Military," 10–17.
50. Zachary Fryer-Biggs, "Inside the Pentagon's Plan to Win Over Silicon Valley's A.I. Exports," *Wired,* 21 December 2018.
51. Fryer-Biggs, "Inside the Pentagon's Plan to Win Over Silicon Valley's AI Experts."
52. Emma Jackson, "I've Worked at Google for Decades. I'm Sickened by What It's Doing," *Nation,* 16 April 2025.
53. K. Preetipadma, "Artificial Intelligence in Military Drones: How Is the World Gearing up and What Does It Mean?," Analytics Drift, 14 August 2021.
54. "X-47B UCAS," Northrop Grumman, accessed 9 September 2025.

55. Cummings, *Artificial Intelligence and the Future of Warfare,* 9.
56. Mark Bowden, "The Killing Machines," *Atlantic,* September 2013.
57. "Uncrewed Tactical Aircraft," Kratos, accessed 20 August 2025.
58. Anna Konert and Tomasz Balcerzak, "Military Autonomous Drones (UAVs)—From Fantasy to Reality. Legal and Ethical Implications," *Transportation Research Procedia*, no. 59 (2021): 294, https://doi.org/10.1016/j.trpro.2021.11.121.
59. Michael J. Boyle, "The Legal and Ethical Implications of Drone Warfare," *International Journal of Human Rights* 19, no. 2 (2015): 107, https://doi.org/10.1080/13642987.2014.991210.
60. Boyle, "The Legal and Ethical Implications of Drone Warfare," 121.
61. Özdemir, "Artificial Intelligence Application in the Military," 19.
62. Charles Q. Choi, "A.I. Drone May Have 'Hunted Down' and Killed Soldiers in Libya with No Human Input," Live Science, 3 June 2021.
63. Özdemir, "Artificial Intelligence Application in the Military," 16.
64. Özdemir, "Artificial Intelligence Application in the Military," 17.
65. Jack Deutsch, "Ukraine's Bomb Squads Have a New Top Dog," *Foreign Policy,* 22 June 2022.
66. Sydney Freedberg, "How A.I. Could Change the Art of War," Breaking Defense, 25 April 2019.
67. Jeremy Straub, "Artificial Intelligence Is the Weapon of the Subsequent Cold War," Conversation, 29 January 2018.
68. Daniel Egel et al., "A.I. and Irregular Warfare: An Evolution, Not a Revolution," *War on the Rocks,* 31 October 2019.
69. David Gray Widder, Sireesh Gururaja, and Lucy Suchman, "Basic Research, Lethal Effects: Military AI Research Funding as Enlistment," arXiv, 26 November 2024, https://doi.org/10.48550/arXiv.2411.17840.
70. Rojoef Manuel, "33,000 AI Drone Strike Kits Headed to Ukraine in Pentagon Deal," *Defense Post,* 29 July 2025.
71. Ramesh Jaura, "Ukraine War: Use of AI Drones Signals a Dangerous New Era," *Eurasia Review,* 8 June 2025.
72. Vitaliy Goncharuk, *Russia's War in Ukraine: Artificial Intelligence in Defence of Ukraine* (Tallinn, Estonia: International Centre for Defence and Security, 2024).
73 Viktoriia Rafalovych et al., *Beyond the Border: What Ukraine's Deep-Strike Drone Attack Means for the Future of Proxy and Drone Warfare* (Brussels, Belgium: Centre of Youth and International Studies, 2025).
74. Dominika Kunertova, "Drones Have Boots: Learning from Russia's War in Ukraine," *Contemporary Security Policy* 44, no. 4 (2023): 576–91, https://doi.org/10.1080/13523260.2023.2262792.

Beyond Linear Planning
How Artificial Intelligence Multiagent Systems Can Redefine Operational Art and Decision Making in Warfare

Lieutenant Colonel Jani Liikola, PhD,
and Commander Petteri Blomvall

Abstract: Artificial intelligence (AI) is already reshaping work methodologies, but future disruptions will inevitably extend further, fundamentally influencing how we conceptualize and understand reality. The scale and pace of this disruption will accelerate significantly with the integration of AI agents and multiagent systems. Traditional linear military planning processes, which depend solely on human cognition, have repeatedly proven inadequate in confronting the complexities of contemporary battlespaces. This article explores the potential impacts of AI on operational art and highlights opportunities for military organizations to successfully reimagine operational cognition through collaborative frameworks that seamlessly integrate human and AI capabilities. The findings suggest multiple transformative impacts on existing linear cognitive paradigms and propose enhanced human-machine collaboration mental models.
Keywords: operational art, multiparadigm design, multiagent system, warfare

The world is currently facing a technological disruption, as artificial intelligence is fundamentally reshaping not only our methods of work but also the ways we conceptualize and comprehend reality. This article

LtCol Jani Liikola, PhD, has more than 20 years of experience within Finland's security administration, serving in the Finnish Border Guard. He currently serves at the border guard headquarters between Finland and Russia. Liikola earned his doctor of military sciences degree from the Finnish National Defence University in 2019 and graduated as a general staff officer in 2023. Cdr Petteri Blomvall is an officer with 23 years of military service, currently serving at the Finnish Border Guard Headquarters. He is currently a PhD candidate at Finland's National Defence University, researching operational art, operational design, and creative approaches. Note: artificial intelligence (ChatGPT 4.0) was utilized to translate this article into English. The authors remain fully accountable for the accuracy, integrity, and originality of the final translation.

Journal of Advanced Military Studies vol. 16, no. 2
Fall 2025
www.usmcu.edu/mcupress
https://doi.org/10.21140/mcuj.20251602008

examines the potential impacts of AI on operational art and discusses opportunities for military organizations to successfully reconceptualize operational cognition through syndicates that seamlessly integrate human-AI collaboration. The traditional linear military planning process—reliant exclusively on human cognition—has repeatedly proven insufficient when confronted by the complexities inherent to contemporary battlespaces. Information saturation, rapidly unfolding events, and ambiguous operational contexts consistently challenge the effectiveness of reductionist decision-making paradigms. Planners frequently resort to oversimplifying complex realities to achieve clarity, despite complexity being an inherent characteristic of the modern operational environment. While humans simplify reality due to cognitive limitations, artificial intelligence simplifies due to computational efficiency and goal-driven optimization. This fundamental divergence in cognitive approaches underscores the necessity of an integrated human-AI paradigm shift in military planning processes.

One of the most disruptive advancements in artificial intelligence is AI agent technology.[1] AI agents integrate automation and generative AI, enabling greater adaptability and emergent decision making. Within military planning processes, this leap in technology offers new pathways for dynamic operational design, allowing planners to retain cognitive depth while optimizing execution. Operational planning in the military domain has traditionally relied on hierarchical command structures, doctrinal principles, and predefined scenarios.[2] However, the growing complexity of the modern battlespace, the accelerating tempo of decision making, and the increasing adaptability of adversaries challenge these conventional approaches, which remain constrained by human cognitive limitations.[3] Human decision making is inherently susceptible to heuristic biases, cognitive overload, and errors stemming from incomplete situational awareness, all of which can contribute to strategic failures.[4] In this evolving operational landscape, the integration of AI agents and multiagent systems (MAS) into planning of operations or campaigns represents a radical paradigm shift, one that has the potential to redefine the foundational principles of military planning and decision making. In this article, planning is seen in a broad manner, encompassing processes throughout the whole conflict continuum and extending to the planning during phases of execution.

Military planning can and should be comprehended as inherently nonstatic, as temporal and spatial rigidity cannot be sustained in warfare. Future planning will therefore emphasize dynamism, emergent organization, and self-organization, where time, space, and force composition happen in tandem with AI agents.[5] This transition redefines classical military planning principles—systematic logic and frame-by-frame snapshot of warfare—by shifting their meaning in relation to space, time, and strategic actors. Objectives no longer have to be fixed endpoints but rather fluid constructs that emerge within

the continuous evolution of the planning syndicate. Rather than being merely a challenge, uncertainty becomes a fundamental premise of operational design. Critical decision-making convergence points arise where AI agents and human planners converge into a continuously evolving decision-making rhizome.[6] This transformation moves military planning beyond rigid linearity and traditional group decision-making constraints toward adaptive, self-regulating syndicates, leveraging AI's cognitive and analytical capabilities. AI agents cease to be mere reactive tools and instead become active participants in operational design—shaping strategy rather than merely executing predefined tasks.

Winning in peer-to-peer conflict, or even against a numerically superior adversary, has historically relied on superior cognition to generate sudden and unforeseen disruption.[7] From a Finnish perspective, it is evident that the country's survival during the 1939 Winter War would not have been feasible had static trench warfare been favored over tactical mobility, counteroffensives, and leveraging the local battlespace conditions for engagements. Surprise has consistently been a transient phenomenon—a fleeting window of opportunity sustained solely through tempo, defined as the dynamic interplay of speed and unpredictability. This, in turn, necessitates decentralized command structures, an acute awareness of risk, and cognitively demanding military judgment.[8] The fundamental principles of operational-level warfare have remained largely unchanged. Contemporary conflicts further substantiate this reality: the Russo-Ukrainian War has exemplified disruptive applications of unconventional operational thinking, incorporating a synergistic combination of disinformation campaigns, land-based maneuvers, and the denial of maritime dominance through unmanned surface vessels. Similarly, the annexation of Crimea, executed by unmarked military personnel colloquially referred to as "little green men," parallels historical instances of strategic deception, such as the Trojan horse or the airborne assault on Belgium's Fort Eben-Emael—operations that profoundly redefined prevailing conceptions of what is operationally feasible in warfare.

This article contends that the rapid advancements in AI technology have the potential to elevate operational art to unprecedented levels of unconventional thinking. While traditional maneuver warfare theories have predominantly centered on the physical domains, emerging technologies are increasingly dismantling these boundaries, enabling a more expansive and fluid conceptualization of conflict. This article argues that the core principles of warfare—surprise and speed—will remain integral; however, the operational maneuvers of the near future will progressively transcend conventional domains, continuously redefining feasibility and broadening the spectrum of possible military actions.

This article analyzes how AI multiagent systems reframe operational art and disrupt planning processes in warfare. This posits that military operational thinking and decision making will face a paradigmatic shift, catalyzed by the

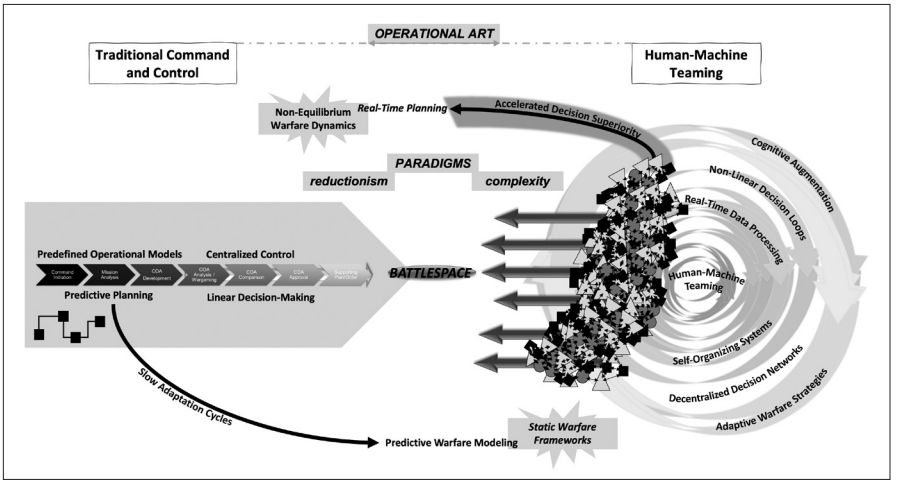
emergence of AI agents and multiagent systems as defining constructs in future operational environments. Artificial intelligence is no longer an abstract theoretical construct but a tangible and operationally integrated force multiplier, as evidenced already by the ubiquitous deployment of generative AI architectures, such as ChatGPT. The AI-driven paradigms analyzed in this study—AI agents and MAS—represent an advanced evolutionary leap in computational autonomy, characterized by disruptive potential that redefines the foundational principles of operational art and strategic command structures. Gordon Moore's 1965 prediction of exponential technological progress, based on the doubling of transistor density, laid the foundation for decades of innovation. Today, the advent of AI agents and MAS systems accelerates this trajectory, granting agile and adaptive organizations a decisive strategic advantage. In contrast, entities that remain reliant on rigid, bureaucratic planning structures and cumbersome processes risk obsolescence. Within military organizations, human-centered decision making may become a limiting factor if legacy planning paradigms continue to be maintained without adaptation to the evolving technological landscape.

The Need for a Paradigm Shift in Military Convention

Ben Zweibelson has argued that artificial intelligence challenges the foundational philosophical pillars of operational art.[9] The integration of AI agents can help shift military planning away from deterministic, Newtonian-style linearity and toward a model that embraces complexity, emergence, and dynamism. This transition necessitates not only technological investment but also a fundamental cultural and paradigmatic shift within military organizations. The military profession must evolve beyond institutional inertia and actively integrate complexity-driven operational methodologies to leverage AI-human collaboration. Linear and hierarchical planning processes are no longer sufficient to win against an opponent also aiming for relative advantage through leveraging rapidly emerging dilemmas. This will necessitate a paradigm shift in military doctrine toward more flexible and self-organizing decision making to keep up with the rate of change possible.

The excessive reliance on bureaucratic control mechanisms and doctrinal standardization within military organizations presents a structural impediment to innovative cognition and the evolution of adaptive decision-making frameworks.[10] This institutional rigidity fosters a competency trap, wherein organizations become self-referentially entrenched in established methodologies, misperceiving them as universally optimal, thus impairing their capacity for epistemic adaptation and strategic responsiveness in dynamic operational contexts.[11] Hierarchical decision making and static planning may result in a loss of operational flexibility, allowing an adaptive enemy to outmaneuver overly rigid

Figure 1. The tension between complexity and linearity in multiparadigmatic battlefield planning



Source: courtesy of the author, adapted by MCUP.

operational thinking. The operations in Afghanistan and Iraq exemplified how rapidly changing battlefield conditions rendered traditional planning models ineffective, leading to strategic miscalculations.[12]

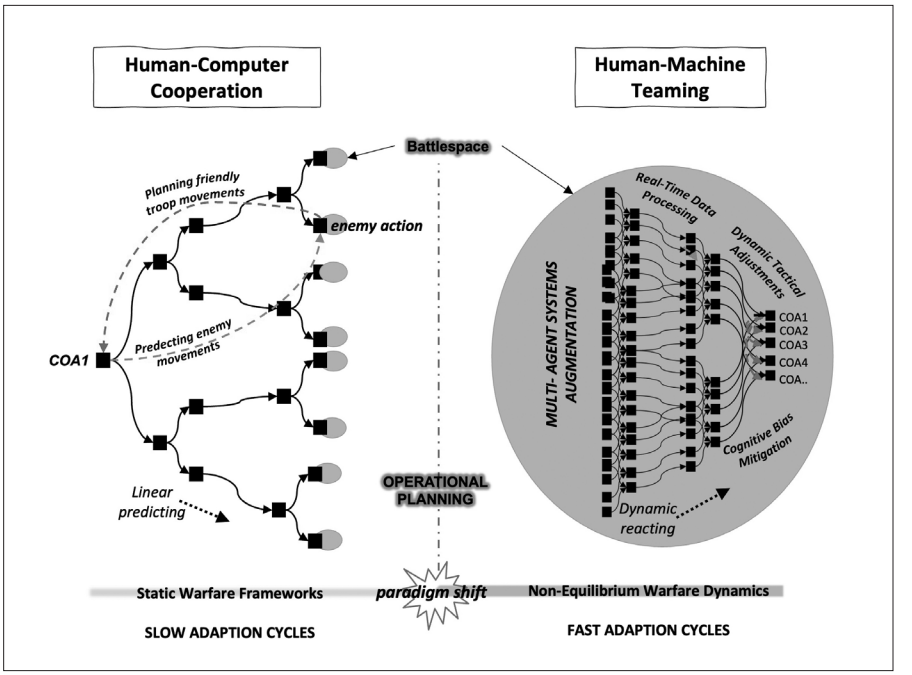
Figure 1 illustrates the tension between linear and complex operational art, where two distinct paradigms can intersect on the future battlefield. The purpose of this depiction is not to argue for the superiority of either approach but to analyze the reality of warfare and military planning from two different perspectives. The traditional linear planning mental model is rooted in reductionist thinking, where complex phenomena are deconstructed into discrete, manageable components. This article, however, posits that AI applications introduce a disruptive dimension to military planning, enabling novel approaches to addressing threats within a dynamic and multifaceted operational environment. In particular, the multiparadigmatic nature of the contemporary battlespace, along with the inherently complex and dynamic character of operational reality, necessitates the continuous evolution of military planning and operational art. The development of AI should be perceived as an opportunity rather than a threat. It is essential to recognize that AI is not merely another "instrument" in the historical progression of military technology, gradually enhancing warfare through incremental advancements, nor just a decision-support system; instead, it can establish a novel operational environment where strategic choices, situational awareness, and operational thought evolve in constant interaction with multidimensional data flows. Thus, AI does not simply provide more efficient means of responding to changes in warfare; rather, it can alter the very conceptualization of warfare itself by generating new situational developments,

enabling emergent strategies and decentralizing operational decision making in ways that challenge traditional command structures and linear planning paradigms. In this sense, AI is not merely a solution to the challenges of modern warfare—it constitutes an entirely new paradigm for understanding, organizing, and executing military operations.

We can first analyze whether AI agents could calculate, model, or simulate the complexity of warfare to a level of rationalist and mechanistic paradigm. This is plausible, as AI systems can filter, structure, and distill vast, multilayered information flows—often surpassing human cognitive capacity—into clear and actionable decision alternatives.[13] However, warfare and even a conflict is always a reciprocal hostile activity. The degree to which AI influences warfare complexity depends on its design and operational application. If AI is used primarily for data reduction and simplification, it risks reestablishing a deterministic, mechanistic approach to military planning, limiting adaptability in emergent, nonlinear conflict environments. Conversely, when AI is integrated within an iterative, emergent, and complexity-embracing operational framework, it can enhance adaptive decision making, deepen situational awareness, and facilitate dynamic actions. Ultimately, the human role remains decisive—military professionals determine whether AI functions merely as an information-reduction tool or as a catalyst for embracing complexity and fostering emergent strategic thinking.

Figure 2 illustrates a paradigm shift that will be driven by multiagent systems. Real-time operational planning becomes feasible through data automation, multiagent network intelligence, and enhanced human-machine integration. In traditional, static operational planning, enemy actions must be predicted well in advance, as dynamic responses during combat situations are severely limited. Historically, predictions relied heavily on extensive manual data management, typically handled via cumbersome spreadsheets emphasizing data entry over cognitive teaming. MAS fundamentally transforms this process by integrating information with unprecedented precision and significantly mitigating cognitive biases inherent in human-centric planning. Rather than eliminating the need for predictive activities, MAS refines and improves prediction accuracy through artificial intelligence. Automated management of information overload, combined with an emergent and dynamic human-machine planning interaction, ensures continuous adaptation. Multiagent coordination further supports decision making, enabling tactical adjustments in real-time combat scenarios, provided sufficient authorization. The introduction of MAS radically compresses both spatial and temporal dimensions within the battlespace. Consequently, operational planning undergoes a profound paradigm shift, adopting a multiparadigmatic approach centered around dynamic human-machine

Figure 2. Static versus nonequilibrium warfare



Source: courtesy of the author, adapted by MCUP.

teaming. This transformation is crucial for addressing the inherent unpredictability and instability of future warfare environments.

Historically, the center of gravity has been perceived as the enemy's critical focal point, the disruption of which would lead to the collapse of the entire system.[14] This perspective is rooted in mechanistic thinking, where the adversary is conceptualized as a hierarchical and predictable system. Operational planning has also been based on the assumption that targeting strategic nodes—such as command centers, logistical networks, and key capabilities—is sufficient to achieve the objectives of warfare.[15] This model has proven effective in traditional conflicts and during battles with superior forces where warfare has been clearly delineated and structured. However, in asymmetric and hybrid operations, the adversary can be a decentralized and adaptive network in which focal points continuously shift.[16] In preparing the abilities to fight near peer enemies, the static and predefined center of gravity no longer provides a viable strategic framework, as modern military operations require continuous situational awareness updates and adaptive decision-making mechanisms. In contemporary warfare, center of gravity should be understood as an evolving and context-dependent phenomenon, emerging in real-time as a result of various factors and environmental changes. Instead of focusing on striking a fixed cen-

ter of gravity, operational planning can leverage multiagent systems and AI to map how an enemy's critical structures evolve dynamically.

Current Research on Human Collaboration with Multiagent Systems

AI research has transitioned toward a paradigm that fuses adaptability with structured planning, reactivity with cognitive modeling, and emergence with self-organization, creating an increasingly seamless and autonomous decision-making framework.[17] This shift represents a departure from deterministic, rule-based systems of the 1950s, which were limited in scope and lacked situational awareness or contextual learning. Today, AI agents have evolved into sophisticated, autonomous systems leveraging deep learning, reinforcement learning, and large language models (LLMs) to address complex, multilayered challenges.[18] Unlike their predecessors, these AI agents are not merely reactive tools; they now engage in higher-order decision making, problem-solving, and dynamic environmental interaction.[19] Their integration into both civilian and military applications is redefining intelligence analysis, operational planning, and command structures, enhancing speed, adaptability, and strategic foresight. Looking ahead, AI agents are poised to transition from digital environments to real-world physical operations, particularly in robotics and autonomous systems where they will navigate, assess, and act independently within dynamic, unpredictable terrains.[20] This evolution requires advanced sensor fusion, real-time data processing, and context-sensitive decision making, ensuring AI systems adapt fluidly to changing operational conditions. As AI's role extends beyond passive computation into active execution, its impact on warfighting, logistics, and battlefield autonomy will become increasingly foundational rather than supplementary.

The defining characteristic of AI agents is their ability to operate autonomously while interacting with their environment. Unlike traditional software systems that follow static, predefined rules, AI agents sense, interpret, and adapt to new situations in real time. They leverage sensors to collect stimuli—such as sound, text, and images—and process this data to support decision making. This capability distinguishes AI agents from conventional software, which lacks the flexibility to adjust to evolving conditions.[21] AI agents can be broadly defined as autonomous entities that function independently yet engage dynamically with other agents and their surroundings. Their core attributes include autonomy, social intelligence, reactivity, and proactivity.[22]

The future of AI agents is closely tied to their increasing autonomy, adaptive learning, and self-organizing capabilities, which are crucial for the evolution of more complex multiagent systems.[23] The key distinction between AI agents and MAS lies in the complexity and scalability of their application do-

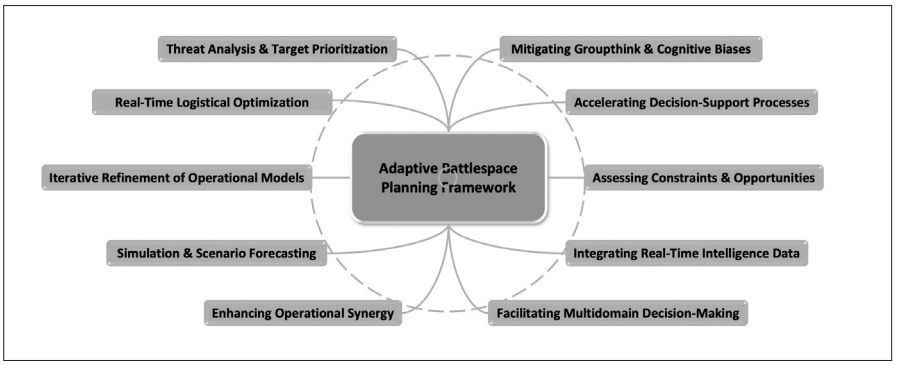
mains. While an individual AI agent can efficiently perform a specific task, MAS enables decentralized decision making, real-time adaptability, and emergent problem-solving, making them particularly valuable in highly dynamic and uncertain environments.[24] MAS consists of autonomous agents that can either collaborate or compete to achieve shared objectives. One of their primary advantages is their ability to decompose complex problems into smaller, manageable subproblems, allowing for parallel computation and real-time decision optimization.[25] MAS systems are uniquely suited for environments requiring both distributed intelligence and dynamic adaptability. By leveraging collective intelligence, swarm behavior, and coordinated learning, MAS can generate synergistic effects that surpass the capabilities of individual agents. This allows them to enhance system-wide efficiency, optimize resources, and increase resilience against disruptions.[26]

Drone swarms are a concrete example of applying multiagent system theory to dynamic combat environments, and their significance in autonomous warfare is growing.[27] Swarming behavior refers to the real-time, coordinated operation of multiple autonomous agents acting as a unified whole. Each agent operates independently but synchronizes its decision making with others without centralized control, enabling faster responses compared to traditional systems.[28] With localized situational awareness and rule-based decision making, the system remains both adaptive and resilient under rapidly changing conditions. Intelligent communication within the swarm allows for real-time data sharing, enabling sensor drones to detect threats or targets and direct armed units accordingly.[29] Drone autonomy enables coordinated collaboration without continuous human intervention, and cooperative methods developed on this basis support effective swarm behavior across various operational environments.[30] Swarm technologies are expected to play a critical role in future armed forces seeking to outpace adversaries in decision-making and operational tempo within complex and fast-evolving combat scenarios.[31] The United States' latest planned Boeing F-47 sixth generation stealth fighter jet exemplifies the integration of swarm intelligence and AI-based agent technology into a single, advanced system.[32]

MAS systems elevate the operational capabilities of AI agents to a new level. Their decentralized architecture enables the efficient and flexible resolution of complex, large-scale problems, making them highly adaptable to dynamic environments.[33] Moreover, MAS systems leverage synergistic effects, where the collective intelligence of individual agents leads to emergent behaviors and solutions that surpass the sum of their individual capabilities.[34] According to recent publications, AI agents are transforming military planning and execution in the following 10 key areas.[35]

The benefits offered by AI agents and multi-agent systems extend broadly

Figure 3. Adaptive battlepace planning framework.



Source: based on ideas from Thom Hawkins, "We Are All Agents: The Future of Human-AI Collaboration," Modern War Institute, 28 August 2024; and J. Caballero Testón, "The Role of Automated Planning in Battle Management Systems for Military Tactics," *Expert Systems with Applications* 297 (2025), https://doi.org/10.1016/j.eswa.2025.129259.

across military planning and operational activities. These technologies can enhance command processes, optimize resource utilization, and support decision making in complex and rapidly evolving environments. Most importantly, AI agents can introduce noninstitutionalized novel alternatives, generating solutions and decisions that are developed interactively—learning from past operations and adversary actions to refine and design future actions. Looking ahead, the advancement of AI agents and MAS systems will unlock new opportunities to merge human and AI capabilities, paving the way for more efficient, adaptive, and innovative operational models. This evolution will inevitably reshape operational art and influence the organization of planning syndicates, driving military strategy toward greater agility and intelligence-driven execution.

At this point it seems already clear that AI agents represent a paradigm-disrupting technology, not a fleeting trend, and their influence extends across tactical, operational, and strategic levels.[36] Organizations increasingly integrate AI agents as virtual team members, leveraging them for knowledge management, workflow coordination, and complex operational execution.[37] As the technology evolves, AI agents transition from simple assistants to autonomous entities capable of decision making, environmental adaptation, and achieving strategic objectives with minimal human oversight.[38] This transformation signals a fundamental shift in both technological and operational paradigms, with far-reaching implications for planning effectiveness, strategic agility, and emergent decision architectures. Military organizations must embrace the dissolution of rigid, deterministic models and move toward fluid, adaptive, and AI-enhanced frameworks that align with the realities of modern conflict.

The primary challenge of this technological transformation is not merely

the performance capabilities of AI agents but their acceptance within military organizations as integral components of operational planning and decision making. Sarvash Sawant et al. highlight three critical concerns: the transparency of AI-driven decision making, the formal delineation of its role within operational structures, and the trust that military personnel place in autonomous systems' evaluative capacities.[39] Excessive AI autonomy risks obscuring accountability, increasing strategic uncertainty, and diminishing critical human judgment, particularly if AI agents operate beyond the comprehension and oversight of human commanders.[40] Conversely, well-integrated and applied AI agents could enable a novel paradigm of autonomous operational planning, characterized by unprecedented speed, adaptability, and initiative in decision-making. Consequently, the radical adoption of AI-driven military planning necessitates a fundamental redefinition of operational thinking—one that deeply accounts for the capabilities and limitations of these technologies and systematically re-evaluates AI agents' roles within military operations at a foundational level.

As has become clear, MAS consists of autonomous agents, which can be either software- or hardware-based components working collectively to achieve a common objective.[41] The core attributes of these systems include:

- **Decentralized decision making**: MAS agents can operate autonomously and make decisions without reliance on a centralized command structure.
- **Scalability**: The system can adapt to operations of varying scales and types.
- **Adaptability**: MAS can respond to real-time changes in the environment and anticipate emerging threats.

Agents within MAS can be homogeneous (identical in function and capability) or heterogeneous (specialized with different roles and abilities), allowing for efficient execution of complex tasks.[42] While AI offers significant advantages in analytical and administrative tasks, its role as a leader or in fostering social cohesion remains challenging. Military leadership requires not only decision making but also human empathy, social intelligence, and intuitive understanding of complex political and cultural factors. These limitations define the extent to which AI can fully replace human decision making in critical military situations.

AI agents can already offer a decisive advantage in military operations by automating repetitive and high-volume tasks, allowing human operators to focus on complex, strategic, and creative decision making. Beyond task automation, AI agents and MAS can process real-time data streams, detect emerging patterns, and execute high-speed strategic decisions with unmatched precision.[43] This capability is particularly critical in military operations, where fast

data-driven decisions can directly influence mission success. AI agents enhance operational efficiency, reduce cognitive overload on human planners, and provide real-time adaptability in rapidly evolving combat environments.

Paradigmatic Disruptions in Warfare: Lessons of Unconventional Thinking

Future warfare scenarios are likely to become increasingly complex, faster-paced, multiparadigmatic, and conceptually more challenging to comprehend. This is particularly true in conflicts involving near-peer adversaries with highly trained officer corps, who may demonstrate minimal regard for institutionalized rituals or legal constraints on fair warfare. Engaging a near-peer adversary—whether through direct confrontation or proxy conflicts—will inevitably incorporate familiar elements of past military engagements, including established methods, strategies, and operational practices, and these can be augmented by progressively faster adaptation cycles and accelerated deployment of emerging technologies. However, such developments primarily reflect increased efficiency in applying existing methodologies rather than a fundamental shift in the nature of warfare. While adaptation and incremental innovations remain crucial, they are not the primary focus of this article. Beyond simply accelerating existing approaches, strategic advantage may also emerge through entirely novel methods and unconventional means.[44] Additionally, the relatively unexplored operational domains of space and cyberspace introduce further layers of disruption. To contextualize this shift, the concept of paradigmatic surprise is introduced into military theory, illustrated through historical case studies, and linked to the planning process.

Paradigmatic surprise is a cognitive effect imposed on an adversary through actions that cannot be comprehended using existing mental models and conceptual frameworks. In military contexts, surprise is traditionally understood in terms of unexpected force posturing, troop numbers, or unforeseen movement vectors. However, in such cases, the advantage is still gained within the established and mutually understood parameters of warfare. In contrast, paradigmatic surprises arise from actions that fundamentally disrupt the prevailing paradigm, necessitating entirely new indicators to assess their impact. In the realm of technological innovation, radical advancements are often distinguished by whether their capabilities are measured using entirely new performance indicators.[45]

As previously suggested, future warfare may challenge the Newtonian deterministic paradigm that underpins current ontological and epistemological approaches to warfighting and operational planning. This evolution places increasing demands on military organizations to cultivate innovation that transcends institutional rigidity. With AI-enhanced collective cognition, paradigmatic surprises may not only become a recurrent feature of modern warfare

but also an essential element of contingency planning. Although history offers numerous instances of paradigmatic surprise, these events were often incomprehensible at the time they occurred—only later were they fully understood in hindsight. When first encountered, their very nature obscured whether an operation was actively unfolding, often delaying an effective response until it was rendered futile. Even though these surprises seemed unpredictable in the moment, the activities were nevertheless devised within the planning groups of one antagonist—the surpriser's. As such, even MAS-augmented and broad contingency planning might not have prevented the activities, but it could have been extremely helpful in recognizing the disruptive situation as unfolding aggression and in designing timely countermeasures to the new reality. Therefore, the following examples are not intended to predict specific future actions but rather to illustrate how war paradigms have been disrupted in the past and potential superior cognitive capabilities can conceptualize the paradigms again also.

Superiority through Surprise Instead of Mass

The German victory in France in 1940, often characterized by the term *blitzkrieg*, represented an unprecedented development in modern warfare. The assault through the Ardennes began on 10 May 1940.[46] At the time, France was considered the militarily superior power and had spent the previous two decades preparing for a potential conflict.[47] Nevertheless, Germany devised a military solution that bypassed the previously assumed strengths of conventional warfare, achieving a decisive and unexpected success. Several key factors contributed to the German victory and the element of surprise. The concentration of highly mobile panzer divisions, led by bold and aggressive commanders, spearheaded the offensive in a manner without historical precedent.[48] According to Richard Shuster, Germany's success can be attributed to the innovative employment of armored forces, maneuver warfare tactics that disrupted the conventional notion of a linear front, and a novel conceptualization of military command structures.[49] These strategic innovations rendered obsolete the earlier emphasis on numerical superiority and massed formations as the primary determinants of military effectiveness.

During the Falkland Islands War (1982), Argentina achieved operational surprise but failed to effectively respond to Britain's strategic adaptation, leading to the ultimate failure of its campaign. Similarly, during the Yom Kippur War (1973), Syria and Egypt executed a well-coordinated, large-scale offensive against Israel, yet Israel's ability to improvise and rapidly adjust its defensive strategy enabled it to shift the course of the war in its favor. These cases illustrate that surprise alone does not secure strategic success. The decisive factor is not the initial disruption of an opponent's expectations, but rather the capacity

to exploit that moment of shock and sustain a dynamic response to the evolving battlespace. For mechanistic organizations, this underscores the necessity of integrating innovation-seeking behaviors into their structural and cultural dynamics. Adaptation cannot be a reactive measure; it must be an inherent feature of military planning and execution, ensuring forces remain fluid, responsive, and attuned to emergent complexities in warfare.[50]

Separatists or Joint-Level Special Operation Forces of Russia

During the early hours of 27 February 2014, special operations forces from the Russian Special Operations Command (SOC) seized the Crimean parliament building.[51] These SOC troops, described as the special operations unit "most directly at the hands of the political leadership," had only recently been officially established in March 2013 and were modeled after the United States Delta Force and the United Kingdom Special Air Service.[52] The operation diverged significantly from prevailing Western special operations doctrines, particularly those emphasizing military direct action. The soldiers did not wear identifying insignia, as required under international law, and the Russian government denied any involvement. Instead, the operatives were publicly portrayed as local civilians. The operation demonstrated a high degree of coherence across all levels —from tactical execution to strategic communications and political-strategic maneuvering—ultimately achieving its objectives without direct military confrontation.

The operation was executed at the tactical level through covert means and conducted without direct combat. While it did not constitute a disruptive innovation in special operations at the tactical level, its impact at the operational level created a paradigmatic surprise. It challenged the binary distinction between war and peace, contradicted the Western emphasis on the right to peaceful protest, and did not fit conventional definitions of terrorism. The inability to conceptualize or even name the situation led to a disruption in recognizing it as a military operation altogether. Although carried out at the tactical level, this swift and decisive action undermined the cognitive frameworks of the time, achieving a fait accompli before Ukraine could respond effectively. By the time Ukrainian authorities could react, Russian second-echelon forces were already positioned.[53] The tactical maneuver rapidly escalated into strategic-level consequences. More than two weeks later, Western media outlets continued to refer to the Russian operatives as "armed gunmen" and "separatists."[54] Within just 19 days, a rigged referendum had already taken place, leading to the formal annexation of Crimea by Russia. Throughout this period, special operations forces were still publicly labeled as "pro-Russian armed forces," and major Western

news sources, such as BBC, framed the event as the Crimean parliament having "formally applied to join Russia."[55] This cognitive and political disruption persisted among Western governments, as they struggled to categorize an event that defied existing paradigms of warfighting. While this operation redefined the contemporary understanding of military action, the future of warfare may introduce even greater disruptions, as operations increasingly evolve into multidomain engagements that transcend traditional conceptual boundaries.

The historical case study of Russia's operation in Crimea provides valuable insights into contemporary cognitive deficiencies in military planning processes. First, the operation disrupted existing mental models used to conceptualize military situations, thereby significantly delaying the sensemaking phase, which constitutes the first and most critical step of any military planning process. Whether this phase involves intelligence preparation of the operational environment—through mapping, factor analysis sheets, or other methodologies—effective sensemaking requires the appropriate cognitive tools to identify key challenges and fully comprehend the problem.[56] The process of naming plays a fundamental role in framing a given situation.[57] It is conceivable that the disruptive cognitive capabilities of AI-driven multiagent systems could have enhanced defense planning by recognizing the potential risk of a modern-day Trojan horse operation before its execution. Moreover, the ability to challenge institutional rigidity in planning teams, as well as the prevailing ontological and epistemological frameworks of warfare, could have provided a cognitive advantage in understanding the unfolding situation and, consequently, formulating effective responses. It is also possible that a viable countermeasure already exists but remains unrecognized due to cognitive constraints imposed by preexisting mental models.

The conventional temporal construct in military planning is misleading, as it relies on static and spatial assumptions that fragment operational reality into predefined phases. This reductionist approach can restrict adaptability in responding to dynamic and uncertain situations, particularly when planning is anchored in preestablished scenarios that fail to account for the emergent and adaptive nature of modern warfare. The Crimean operation provides a compelling example of how Russia integrated hybrid warfare elements—disinformation, rapid special forces deployment, and political uncertainty—to manufacture strategic surprise. This represents a cognitive bias toward surprise, where the disruption was not merely a result of tactical execution but rather a deliberate exploitation of information saturation and deception. The objective was to distort and disrupt adversarial decision making, which was predisposed to mechanistic, symmetrical warfare constructs.

Toward Novel Military Thought: The Synergy of Human and Multiagent Systems

Within operational art, planning syndicates will become even more pivotal in achieving complex and dynamic objectives and in surpassing more commander-driven approaches. Recent advancements have expanded the concept of teamwork and decision making to incorporate human-machine collaboration.[58] AI agents can integrate advanced artificial intelligence technologies, such as machine learning, to enhance their adaptability, efficiency, and decision-making capabilities.[59] This transformation is particularly valuable in military planning, where adaptive, high-speed solutions are essential to address complex, multidomain operational challenges. AI agents extend the role of generative AI beyond traditional support functions—rather than merely assisting human operators, they can act as independent agents, collaborating or even autonomously executing tasks when required. AI-driven agents operate 24/7, processing vast streams of battlefield intelligence, command center data, and real-time communications. This continuous, high-speed data synthesis improves situational awareness, optimizes strategic responses, and reduces human cognitive burden, reinforcing faster and more precise decision cycles in modern warfare.

The cognitive demands placed on human operators in human-AI collaboration have already undergone a significant transformation. While certain cognitive burdens, such as information gathering, can now be delegated to generative AI, critical tasks—including information verification and cross-referencing—remain intrinsically human responsibilities. This shift has also introduced new cognitive challenges associated with response integration, wherein AI-generated information must be critically assessed for contextual relevance, alignment with intended objectives, and suitability for the target audience. Consequently, the human role is evolving from that of an executor to that of an overseer.[60] Nathan J. McNeese et al. examined human-AI teams in emergency response scenarios and found that teams integrating AI significantly outperformed all-human teams in shared situational awareness and task efficiency, despite a decline in perceived shared cognition.[61] In the context of military planning teams, research has highlighted not only the critical role of internal information-sharing but also the necessity of external coupling—leveraging expertise beyond the immediate team. Effective decision making in novel and dynamic operational environments depends on the ability to access multidisciplinary insights.[62] If AI-generated knowledge can provide reliable and timely access to diverse fields of expertise, AI agents may fundamentally disrupt traditional external networking paradigms.

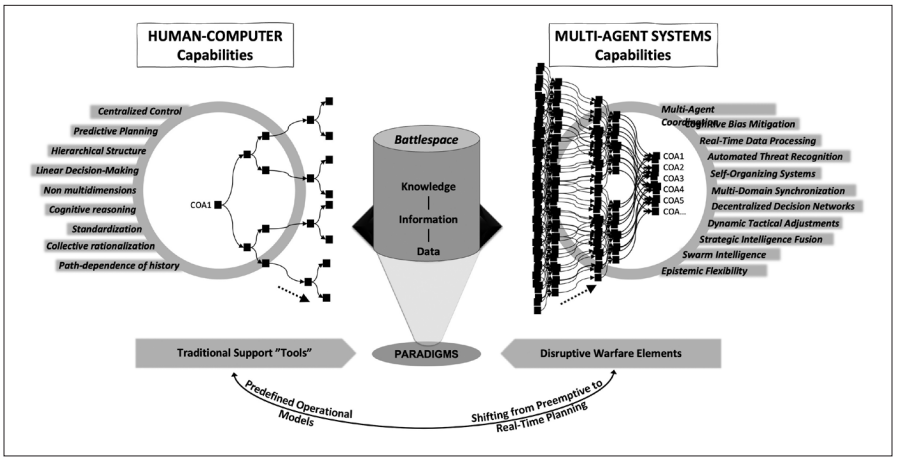
Humans have a natural tendency to oversimplify complex and ambiguous phenomena, perceiving them as more structured and controlled than they truly

are. This cognitive bias limits critical discourse and prevents deeper exploration of alternative perspectives, thereby constraining the recognition, comprehension, and learning of new insights.[63] During the operational planning process, AI agents serve as force multipliers by augmenting human expertise and enhancing the capacity to manage complexity. They can assist in strategic planning by autonomously distributing tasks, integrating external intelligence sources, and continuously refining their own performance. Their role becomes particularly vital during wargaming and scenario analysis, where AI-driven simulations can rapidly generate and assess thousands of alternative courses of action in real time. While human planners rely on cognitive reasoning and experience, AI agents provide a systematic, data-driven approach that significantly accelerates decision cycles and increases strategic foresight. Iterative feedback loops and machine learning mechanisms further refine AI agents' accuracy, adaptability, and responsiveness, making them indispensable tools in modern multidomain operations. Their ability to process vast intelligence streams, optimize dynamic decision making, and function autonomously cements their role as essential components of next-generation operational planning frameworks.[64]

AI agents are no longer passive decision-support tools; they actively engage in the planning process as predictors, critics, advisors, and even leaders. This evolution demands the development of highly adaptive, resilient, and efficient AI agents, capable of navigating complex operational environments, augmenting decision making, anticipating situational shifts, and aligning actions toward shared strategic objectives.[65] This human-AI synergy fosters a nonlinear, emergent approach to decision making, enabling enhanced adaptability in responding to the intricate, rapidly evolving challenges of modern warfare. The integration of decision-making rhizomes—decentralized, non-hierarchical, continuously evolving decision structures—transforms how military organizations perceive and react to complexity.

Figure 4 presents key terms illustrating the significance and role of MAS in the context of operational planning. AI-driven autonomous agents are not merely auxiliary tools; rather, they can function as independent entities within operational planning, capable of generating, optimizing, and executing complex operational plans in real time. According to Michael Mayer, integrating AI with advanced sensors and autonomous systems enables a self-organizing observe-orient-decide-act (OODA), allowing tasks to be executed without direct human oversight.[66] This advancement could drive a shift toward decision-centric warfare, where AI agents not only support but fundamentally reframe military decision-making processes by continuously generating decision points and courses of action. With AI-driven operational planning, the traditional hierarchical and prescripted planning model can be replaced by a dynamic, decentralized, and self-learning system in which AI agents autonomously

Figure 4. From static frameworks to emergent design



Source: courtesy of the author, adapted by MCUP.

analyze situational awareness, devise adaptive strategies, and coordinate force deployments in real time.[67]

Redefined Operational Understanding

The People's Liberation Army (PLA) perceives the future of warfare not as a continuation of traditional strategic logics but as a contest over the ability to define and reframe the evolving rules of conflict engagement. By integrating artificial intelligence into its strategic calculus, the PLA seeks to anticipate, shape, and dictate the trajectory of military scenarios before adversarial forces can cognitively and structurally adapt to the altered battlespace.[68] However, the assumption that AI can singularly supersede human decision-making complexities ignores a fundamental reality of warfare—its emergent and complex-adaptive nature. Historical military paradigms have repeatedly overestimated technological determinism, neglecting the intricate web of strategic, economic, and sociopolitical entanglements that continuously redefine operational realities. Warfare is not a closed system governed by fixed inputs and predictable outcomes; rather it is an open, recursive, and self-organizing phenomenon, where innovation and adaptation coalesce in unpredictable ways. For instance, the *blitzkrieg* concept has often been mythologized as a linear and mechanistic breakthrough, yet modern historiography suggests that the *Wehrmacht*'s operational artistry was far more nuanced than merely a doctrine of speed and armored maneuver.[69] Similarly, contemporary AI-driven decision architectures including multiagent systems risk becoming cognitively entrapped within rigid epistemological boundaries that fail to capture the ever-evolving nature of military conflict. The critical question, then, is not whether AI can provide superior decision making,

Table 1. The impact of the AI multiagent systems

Zweibelson and Paparone's critiques of contemporary challenges	"Perspectives on Future Operational Art: The Impact of AI MAS"
1. The challenge of the Newtonian paradigm: from determinism to complexity The Newtonian, linear way of thinking emphasizes causality and predictability.	AI multiagent systems' iterative and emergent analyses enhance our understanding of complex operations while deconstructing traditional deterministic warfare models. This shift challenges established planning paradigms and necessitates more adaptive, dynamic mechanisms.
2. The ontology and epistemology of warfare Traditional concepts like centers of gravity and operational levels are outdated and poorly suited for addressing modern complex threats.	AI multiagent systems' adaptive knowledge models promote paradigm diversity, surpassing traditional linear and hierarchical frameworks.
3. Human-machine collaboration: a new division of roles The relationship between humans and machines can no longer be based on a commander-tool model.	AI multiagent systems transform thinking into a collaborative process, where machines generate innovative solutions and continuous learning becomes integral to strategic adaptation.
4. Complexity and emergence in military planning Dynamic and complex models challenge conventional mathematical frameworks, providing alternative perspectives on fluid, nonlinear, and multidimensional operational dynamics.	AI multiagent systems integrate multidisciplinary data sources and dynamically anticipate changes, enabling continuous and adaptive emergent planning.
5. Institutional rigidity versus innovation Institutional inertia perpetuates outdated models, stifling innovative approaches and preventing the assimilation of new paradigms into operational thinking.	AI multiagent systems can disrupt institutionalized thinking by providing alternative, objective perspectives. However, their impact depends on an organization's flexibility and willingness to adapt.

Source: based on Ben Zweibelson, "Breaking the Newtonian Fetish: Conceptualizing War Differently for a Changing World," *Journal of Advanced Military Studies* 15, no. 1 (Spring 2024), https://doi.org/10.21140/mcuj.20231501009; Christopher R. Paparone, "How We Fight: A Critical Exploration of U.S. Military Doctrine," *Organization* 24, no. 4 (2017): 516–33, https://doi.org/10.1177/1350508417693853; Thom Hawkins, "We Are All Agents: The Future of Human-AI Collaboration," Modern War Institute, 28 August 2024; and J. Caballero Testón, "The Role of Automated Planning in Battle Management Systems for Military Tactics," Expert Systems with Applications 297 (2025), https://doi.org/10.1016/j.eswa.2025.129259

but whether it can transcend the human tendency toward rigid doctrinal framing and enable new heuristics for navigating complexity and uncertainty. Could AI, rather than merely optimizing existing military methodologies, act as a catalyst for post-linear operational design thinking, wherein strategy is conceived as an iterative, multidimensional, and nonstatic process rather than a preordained sequence of actions?

In the technological domain, surprise can create new opportunities, particularly when combined with the ability to exploit a rapidly evolving military environment. China's AI strategy appears to place considerable expectations on a single technological solution, a historically common yet often flawed ap-

proach.[70] However, it is crucial to recognize that historical patterns do not repeat in a deterministic manner, and assuming linear progression in military development can be misleading.

The advancement of artificial intelligence and autonomous systems may constitute a military revolution akin to how the atomic bomb diverged from the tank during World War II. The tank enhanced and accelerated traditional warfare, reinforcing mobility and firepower but leaving the fundamental principles of land warfare intact. In contrast, the atomic bomb completely transformed the nature of war, shifting the focus from operational engagements to strategic deterrence and redefining conflict as an existential threat. Similarly, AI and autonomous systems may not merely optimize current military practices but could fundamentally alter the paradigm of warfare, redefining the role of the human on the battlefield and challenging traditional conceptions of conflict.

Discussion

Throughout the history of warfare, technological advancements—such as aircraft, tanks, and siege towers—have been pivotal in securing operational superiority and shaping the evolution of operational art.[71] Traditionally, military tools have been defined by human control and innovation, often leading to rapid and radical shifts in warfare (e.g., the disruptive impact of drones in Ukraine). However, the rise of artificial intelligence fundamentally disrupts this paradigm, as it reconfigures the role of military tools—transforming them from passive, human-operated instruments into partially autonomous agents capable of decision making and dynamic action alongside human operators. This transformation is not merely a technological leap, but a philosophical shift in how military assets are conceptualized and employed. Warfare may no longer be solely an instrumental activity dictated by human actors; instead, it could evolve into an emergent and self-directed process, where AI and other advanced technologies influence—or even establish—operational objectives autonomously.

While Jeremiah Hurley and Morgan Greene emphasize the importance of data-driven thinking, history demonstrates that technological breakthroughs alone have rarely determined the outcomes of wars.[72] For instance, in the twentieth century, mechanized warfare did not single-handedly resolve conflicts; it was most effective when combined with flexible operational planning and the ability to adapt to adversary movements. Similarly, AI and MAS offer unprecedented decision-making capabilities and operational agility, yet they also introduce new vulnerabilities, such as cyber threats, reduced transparency in decision making, and potential dependencies on data analytics, which may be susceptible to manipulation or misinformation. Consequently, the traditional typology of military technology is not merely evolving—strategic decision making must adapt to an increasingly complex and dynamic operational environment.

Table 2. From the MAS dilemma to propositions

Dilemma	AI multiagent system ability	Proposition
Causal reductionism is an inadequate epistemology for explaining a complex world	The ability to continuously discover new ways of representing data, whether visual, narrative, or literary.	AI as an interpreter between diverse participants, bridging epistemological stances.
The enemy deliberately creates complexity, conceals intentions, diverts attention, and remains an active actor.	The ability to continuously evaluate vast data sets and construct representations, models, and visualizations free from institutionalized cognitive biases.	AI continuously generates enemy courses of action (COAs), ranging from the probable to the improbable.
Multidomain environments increasingly require a multiparadigmatic approach.	The ability to assume diverse roles within a syndicate, incorporating multiple perspectives and integrating expertise from various fields.	AI assuming multiple planner roles, introducing new frameworks and perspectives (human-to-AI ratio: 4:2 or 3:3).
Cognitively demanding processes have proven too complex to effectively teach and comprehend for a broad audience.	The ability to engage with theoretical knowledge in metaphysics, develop processes, and design methodologies and methods.	AI as a facilitator within the syndicate/planning team, assisting the leader in selecting contextually appropriate processes and methods.

Source: courtesy of the author, adapted by MCUP.

The operational environment can change rapidly—and historically, an inability to adapt to shifting conditions has resulted in severe losses.[73] The adoption of multiagent systems is a pivotal component in the digitalization of military decision making and the AI revolution. MAS enhances operational capabilities by increasing decision-making speed, optimizing information utilization, enabling decentralized operations, and fostering proactive planning. When effectively implemented, MAS facilitates near-real-time command and control, making it indispensable in contemporary warfare. MAS represents a shift toward a decentralized decision-making approach.

Operational planning cannot be confined to a singular or static paradigm; instead, it must leverage multiple, interwoven theoretical frameworks that dynamically interact with one another. Traditional operational constructs, such as the North Atlantic Treaty Organization's (NATO) long-term NATO Defense Planning Process or short-term Joint Targeting Process, rest on predefined structures and assumptions about the static nature of warfare. However, the modern operational environment fundamentally disrupts these linear approaches, demanding a more fluid, emergent design perspective. Following Bergson's philosophy, the concept of duration resists segmentation into discrete phases, as creativity and temporal continuity unfold as an indivisible, evolving process.[74] Warfare, therefore, is not a linear sequence of events but a dynamic, heteroge-

neous process that does not conform to a predetermined structure.[75] This means that military operations are not isolated stages but continuous, adaptive phenomena that blend into one another. Recognizing and exploiting this continuity is essential for contemporary warfare. War is not an ordered system, nor can it be prescripted through static models—its shape and content emerge through a complex interplay of adversarial actions, environmental shifts, and technological capabilities. As Ben Zweibelson argues, war should be understood as an emergent, multilayered, and dynamically evolving phenomenon, in which conventional static planning models are increasingly insufficient.[76] Instead, adaptive, multiparadigmatic approaches provide the necessary epistemic agility to navigate the inherent unpredictability of modern conflict and prevent decision-making entrapment within outdated doctrinal constraints.

Multiagent systems introduce novel capabilities into operational planning, enabling an accelerated decision-making cycle and a deeper, iteratively evolving situational awareness. MAS transcend the cognitive boundaries of traditional military decision making by integrating real-time analytics, multidimensional data processing, and the ability to dynamically adapt to complex scenarios without the constraints of hierarchical command structures. MAS not only enhances operational planning efficiency but fundamentally alters its core principles, shifting the focus from deterministic, predictive models to real-time, emergent adaptation and context-driven decision making. This transition fosters multiparadigmatic adaptability, where planning is no longer constrained by predefined heuristic models but is instead rooted in self-organizing and adaptive situational analysis. Future military strategies can no longer rely on conventional hierarchical and linear frameworks; rather, they must integrate networked, decentralized, and continuously evolving mechanisms that enable flexible and iterative responses to an increasingly volatile operational environment. This marks a paradigm shift, wherein warfare ceases to be a unidirectional and prescripted process and instead emerges as a self-reflective, self-adaptive system—one in which operational planning and battlefield events coalesce into an interconnected, continuously evolving ecosystem.

Traditional rigid command structures can create bottlenecks in the effective utilization of new technologies and advanced decision-making frameworks.[77] Thus, the integration of multiagent systems is not merely a technological advancement but fundamentally an organizational challenge—one that demands resilience and epistemic agility—the ability to rapidly adapt to fluid operational conditions and leverage new paradigms effectively. MAS can provide alternative analytical frameworks for decision makers, acting as a mechanism that detects strategic blind spots that human cognition might overlook. This fosters multiparadigmatic decision making, where multiple scenarios and interpretations

can be evaluated simultaneously, mitigating the risk of cognitive entrenchment within preordained assumptions.

Endnotes

1. "What Is a Multiagent System?," IBM, accessed 25 September 2025; and "Magentic-One: A Generalist Multi-Agent System for Solving Complex Tasks," Microsoft, 17 July 2025.
2. Ben Zweibelson, "Breaking the Newtonian Fetish: Conceptualizing War Differently for a Changing World," *Journal of Advanced Military Studies* 15, no. 1 (Spring 2024), https://doi.org/10.21140/mcuj.20231501009.
3. Christopher R. Paparone and George E. Reed, "The Reflective Military Practitioner: How Military Professionals Think in Action," *Journal of Military Learning* no. 88 (October 2017).
4. Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2011).
5. Haridimos Tsoukas and Robert Chia, "On Organizational Becoming: Rethinking Organizational Change," *Organization Science* 13, no. 5 (September–October 2002): 567–82.
6. Robert Chia, "A 'Rhizomic' Model of Organizational Change and Transformation: Perspective from a Metaphysics of Change," *British Journal of Management* no. 10 (1999): 209–27, https://doi.org/10.1111/1467-8551.00128.
7. William S. Lind, *Maneuver Warfare Handbook* (Boulder, CO: Westview Press, 1984), 3–4, 9.
8. *Warfighting*, Fleet Marine Force Manual (FMFM) 1 (Washington, DC: Headquarters Marine Corps, 1989), 29.
9. Zweibelson, "Breaking the Newtonian Fetish."
10. Jani Liikola, "Luovuuden hyödyntäminen sotilasorganisaatiossa" [Harnessing creativity within military organizations], *Tiede ja ase* [Science and arms] no. 75 (2017).
11. Paparone and Reed, "The Reflective Military Practitioner."
12. Ben Zweibelson, "One Piece at a Time: Why Linear Planning and Institutionalisms Promote Military Campaign Failures," *Defence Studies* 15, no. 4 (2015): 360–74, https://doi.org/10.1080/14702436.2015.1113667.
13. Zweibelson, "Breaking the Newtonian Fetish."
14. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976; reprint, 1989).
15. Christopher R. Paparone, "How We Fight: A Critical Exploration of U.S. Military Doctrine," *Organization* 24, no. 4 (2017): 516–33, https://doi.org/10.1177/1350508417693853.
16. Zweibelson, "One Piece at a Time."
17. Cristiano Castelfranchi, "Modeling Social Action for AI Agents," *IJCAI International Joint Conference on Artificial Intelligence* no. 2 (1997): 1567–76.
18. *Navigating the AI Frontier: A Primer on the Evolution and Impact of AI Agents* (Geneva, Switzerland: World Economic Forum, 2024).
19. "What Is a Multiagent System?"
20. *Navigating the AI Frontier*.
21. "What Is a Multiagent System?"
22. W. J. Zhang and S. Q. Xie, "Agent Technology for Collaborative Process Planning: A Review," *International Journal of Advanced Manufacturing Technology* 32 (2007): 315–25, https://doi.org/10.1007/s00170-005-0345-x.
23. *Navigating the AI Frontier*.
24. P. G. Balaji and D. Srinivasan, "An Introduction to Multi-Agent Systems," in *Innovations in Multi-Agent Systems and Applications*, ed. Dipti Srinivasan and Lakhmi C. Jain (Berlin: Springer, 2010), https://doi.org/10.1007/978-3-642-14435-6_1.

25. Khadijah M. Hanga and Yevgeniya Kovalchuk, "Machine Learning and Multi-Agent Systems in Oil and Gas Industry Applications: A Survey," *Computer Science Review* 34 (2019): 100191, https://doi.org/10.1016/j.cosrev.2019.08.002.
26. Eugénio Oliveira, Klaus Fischer, and Olga Stepankova, "Multi-Agent Systems: Which Research for Which Applications," *Robotics and Autonomous Systems* 27, nos. 1–2 (1999): 91–106, https://doi.org/10.1016/S0921-8890(98)00085-2.
27. Gyu Seon Kim et al., "Cooperative Reinforcement Learning for Military Drones over Large-Scale Battlefields," *IEEE Transactions on Intelligent Vehicles* (2024): 1–11.
28. Kim et al., "Cooperative Reinforcement Learning for Military Drones over Large-Scale Battlefields."
29. M. Lehto and W. Hutchinson, "Mini-Drone Swarms: Their Issues and Potential in Conflict Situations," *Journal of Information Warfare* 20, no. 1 (2021): 33–49.
30. Yong-Kun Zhou, Bin Rao, and Wei Wang, "UAV Swarm Intelligence: Recent Advances and Future Trends," *IEEE Access* 20, no. 8 (2020): 1–1, https://doir.org/10.1109/ACCESS.2020.3028865.
31. Kim et al., "Cooperative Reinforcement Learning for Military Drones over Large-Scale Battlefields."
32. George Allison, "What Do We Know About the New F-47 Fighter?," *UK Defence Journal*, 22 March 2025.
33. Hanga and Kovalchuk, "Machine Learning and Multi-Agent Systems."
34. Oliveira et al., "Multi-Agent Systems."
35. Thom Hawkins, "We Are All Agents: The Future of Human-AI Collaboration," Modern War Institute, 28 August 2024; and J. Caballero Testón, "The Role of Automated Planning in Battle Management Systems for Military Tactics," *Expert Systems with Applications* 297 (2025), https://doi.org/10.1016/j.eswa.2025.129259.
36. "What Is a Multiagent System?"; "Introducing Multi-agent Collaboration Capability for Amazon Bedrock," *AWS News Blog*, 3 December 2024; and "Magentic-One: A Generalist Multi-Agent System for Solving Complex Tasks," *AI Frontiers Blog* (Microsoft), 17 July 2025.
37. Alan Dennis, Akshat Lakhiwal, and Agrim Sachdeva, "AI Agents as Team Members: Effects on Satisfaction, Conflict, Trustworthiness, and Willingness to Work With," *Journal of Management Information Systems* 40, no. 2 (2023): 307–37, https://doi.org/10.1080/07421222.2023.2196773.
38. Joseph B. Lyons et al., "Human-Autonomy Teaming: Definitions, Debates, and Directions," *Frontiers in Psychology* 12 (2021): 589585, https://doi.org/10.3389/fpsyg.2021.589585.
39. Sarvesh Sawant et al., "Human-AI Teams in Complex Military Operations: Soldiers' Perception of Intelligent AI Agents as Teammates in Human-AI Teams," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 67, no. 1 (2023): 1122–24, https://doi.org/10.1177/2169506723119242.
40. Sawant et al., "Human-AI Teams in Complex Military Operations."
41. Zhang and Xie, "Agent Technology for Collaborative Process Planning."
42. Pedro Hilario Luzolo et al. "Combining Multi-Agent Systems and Artificial Intelligence of Things: Technical Challenges and Gains," *Internet of Things* 28 (2024): https://doi.org/10.1016/j.iot.2024.101364.
43. Antje Barth, "Introducing Multi-agent Collaboration Capability for Amazon Bedrock," *AWS News Blog*, 3 December 2024.
44. Lucy L. Gilson and Nora Madjar, "Radical and Incremental Creativity: Antecedents and Processes," *Psychology of Aesthetics, Creativity, and the Arts* 5, no. 1 (2011): 21, https://doi.org/10.1037/a0017863.
45. Markus Häyhtiö, Amanda Eklund, and Marko Palokangas, "Innovation and Adaptation in Public–Private Partnerships in the Military Domain under Broad-Spectrum Influencing: Towards a Competence-Based Strategic Approach," *Journal of Military Studies* 13, no. 1 (December 2024): 10, https://doi.org/10.2478/jms-2024-0007.
46. Richard Shuster, "Trying Not to Lose It: The Allied Disaster in France and the Low

Countries, 1940," *Journal of Advanced Military Studies* 14, no. 1 (2023): 272, https://doi.org/10.21140/mcuj.20231401012.
47. Shuster, "Trying Not to Lose It," 272.
48. Shuster, "Trying Not to Lose It," 278.
49. Shuster, "Trying Not to Lose It," 286.
50. Karl E. Weick and Robert E. Quinn, "Organizational Change and Development," *Annual Review of Psychology* 50 (1999): 361–86, https://doi.org/10.1146/annurev.psych.50.1.361.
51. Tor Bukkvoll, "Russian Special Operations Forces in Crimea and Donbas," *Parameters* 46, no. 2 (2016): 14–17, https://doi.org/10.55540/0031-1723.2917.
52. Bukkvoll, "Russian Special Operations Forces in Crimea and Donbas," 14–15.
53. Bukkvoll, "Russian Special Operations Forces in Crimea and Donbas," 16–17.
54. Alissa De Carbonnel, "Insight—How the Separatists Delivered Crimea to Moscow," Reuters, 13 March 2014.
55. "Crimean Parliament Formally Applies to Join Russia," BBC, 17 March 2014.
56. John N. Warfield and George H. Perino Jr., "The Problematique: Evolution of an Idea," *Systems Research and Behavioral Science* 16, no. 3 (May/June 1999): 221–26, https://doi.org/10.1002/(SICI)1099-1743(199905/06)16:3<221::AID-SRES245>3.0.CO;2-G.
57. Stefan Banach and Alex Ryan, "The Art of Design: A Design Methodology," *Military Review* (March–April 2009): 107.
58. Lyons et al., "Human-Autonomy Teaming."
59. Hanga and Kovalchuk, "Machine Learning and Multi-Agent Systems."
60. Hao-Ping (Hank) Lee et al., "The Impact of Generative AI on Critical Thinking: Self-Reported Reductions in Cognitive Effort and Confidence Effects From a Survey of Knowledge Workers," in *CHI '25: Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan: Association for Computing Machinery, 2025), 15, https://doi.org/10.1145/3706598.3713778.
61. Nathan J. McNeese et al., "Who/What Is My Teammate?: Team Composition Considerations in Human–AI Teaming," *IEEE Transactions on Human-Machine Systems* 51, no. 4 (2021): 8–10, https://doi.org/10.48550/arXiv.2105.11000.
62. Petteri Blomvall and Mikko Hirvi, "A Dynamic and Decentralised Headquarters to Thrive in Uncertainty," *Journal of Military Studies* 13, no. 1 (December 2024): 108, https://doi.org/10.2478/jms-2024-0008.
63. Karl E. Weick, *The Social Psychology of Organizing*, 2d ed. (New York: McGraw-Hill, 1979).
64. Peng Lu et al., "Human-AI Collaboration: Unraveling the Effects of User Proficiency and AI Agent Capability in Intelligent Decision Support Systems," *International Journal of Industrial Ergonomics* 103 (September 2024), https://doi.org/10.1016/j.ergon.2024.103629; and "What Is a Multiagent System?"
65. Alan Chan et al., "Visibility into AI Agents," in *FAccT '24: Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency* (New York: Association for Computing Machinery, 2024), 958–73.
66. Michael Mayer, "Trusting Machine Intelligence: Artificial Intelligence and Human-Autonomy Teaming in Military Operations," *Defense & Security Analysis* 39, no. 4 (2023): 521–38, https://doi.org/10.1080/14751798.2023.2264070.
67. Mayer, "Trusting Machine Intelligence."
68. Koichiro Takagi, "Is the PLA Overestimating the Potential of Artificial Intelligence?," *Joint Force Quarterly* 116 (1st Quarter 2025): 71–78.
69. Rolf Hobson, "Blitzkrieg, the Revolution in Military Affairs and Defense Intellectuals," *Journal of Strategic Studies* 33, no. 4 (2010): 625–43, https://doi.org/10.1080/01402390.2010.489717.
70. Takagi, "Is the PLA Overestimating the Potential of Artificial Intelligence?"
71. Zweibelson, "Breaking the Newtonian Fetish."
72. Jeremiah Hurley and Morgan Greene, "Adopting a Data-Centric Mindset for Operational Planning," *Joint Force Quarterly* 116 (1st Quarter 2025): 24–32.

73. Richard Farnell and Kira Coffey, "AI's New Frontier in War Planning: How AI Agents Can Revolutionize Military Decision-Making," Belfer Center for Science and International Affairs, 11 October 2024.
74. Ajit Nayak, "On the Way to Theory: A Processual Approach," *Organization Studies* 29, no. 2 (2008): 173–90, https://doi.org/10.1177/0170840607082227.
75. Martin Wood and Ewan Ferlie, "Journeying from Hippocrates with Bergson and Deleuze," *Organization Studies* 24, no. 1 (2003): 47–68, https://doi.org/10.1177/0170840603024001680.
76. Zweibelson, "Breaking the Newtonian Fetish."
77. Liikola, "Harnessing Creativity within Military Organizations."

Strategic Implications of Emerging Weapon Technologies

Kinetic Bombardment, Antimatter, and Antigravity Technology for U.S. National Security

A.S.M. Ahsan Uddin

Abstract: This article explores the strategic implications of emerging weapon technologies on U.S. national security, focusing specifically on antimatter, kinetic bombardment systems, and antigravity technology. As global military dynamics evolve, it is imperative for the United States to assess and perhaps integrate this emerging technology to maintain its military superiority. This article examines the accuracy and destructive capability of kinetic bombardment, the immense energy potential of antimatter, and the groundbreaking applications of antigravity propulsion in aerial operations. The findings underscore the critical role that these technologies may play in improving U.S. national security and provide a foundation for additional research on their national security applications and implications.

Keywords: kinetic bombardment systems, antimatter-based weapons, next-generation missiles, antigravity propulsion technology, emerging defense capabilities, precision strike systems, future combat and warfare, strategic defense initiatives

The U.S. national security landscape is rapidly changing due to the emergence of new threats. These changes are driven by swift technological breakthroughs, shifting global politics, and the impact of both nations

Ahsan Uddin is an independent academic researcher specializing in U.S. national security, artificial intelligence ethics, and policy and project management. He holds an MBA from the University of North Alabama and professional certifications as an IBM Artificial Intelligence Developer and in Google Data Analytics, and his work centers on the intersection of emerging technologies, governance, and strategic security considerations. He has been recognized by the U.S. government through approval of a National Interest Waiver (EB-2 NIW) petition granted for his exceptional ability and work of national importance. https://orcid.org/0000-0001-6460-5736.

Journal of Advanced Military Studies vol. 16, no. 2
Fall 2025
www.usmcu.edu/mcupress
https://doi.org/10.21140/mcuj.20251602009

and independent entities. Cyberattacks, particularly from state-sponsored entities like China and North Korea, have become more complex, targeting critical U.S. infrastructure and governmental systems. The 2023 *Annual Threat Assessment of the U.S. Intelligence Community* identifies China as the most persistent and aggressive threat in cyber espionage, targeting U.S. government and private sector networks to further its strategic objectives.[1] In addition to these cyber concerns, the United States must be careful to manage diplomatic relations with nations such as Russia, North Korea, and China to ensure they are never given the opportunity to launch nuclear attacks or exploit political vulnerabilities. The 2022 *Nuclear Posture Review* highlights that these developments have increased the danger of regional instability, necessitating the enhancement of U.S. military capabilities to address growing threats and uphold effective deterrence.[2] Maintaining military technological innovation is essential to addressing today's complex threats. Innovations like cyber capabilities, drones, and precision-guided missiles are increasingly important elements of modern defense.

During this digital era, autonomy in military systems could offer significant advantages by facilitating faster responses, improved efficiency, and enhanced adaptability in rapidly changing situations. Paul Scharre and Michael C. Horowitz highlight that the concept of autonomy in military systems can vary greatly based on the system's complexity and the interaction between humans and machines. They specify various tiers of autonomy—from semiautonomous systems necessitating human involvement (human in the loop) to fully autonomous systems functioning independently of human oversight (human out of the loop)—each bearing distinct ramifications for decision making in military operations.[3] This supports the idea that combining autonomous systems and AI will considerably help the U.S. military by allowing for speedier decision making, improving operational precision, and reducing human risk in high-stakes scenarios.

Future space-based military systems will need to be operated at the speed and scale required by strategic competition, which will require automation and artificial intelligence (AI). AI-driven targeting, on-orbit anomaly detection, and autonomous navigation may enable kinetic bombardment platforms or orbital attack capabilities to locate, follow, and engage targets without continual human supervision. In the commercial sector, such capabilities are already being investigated; examples of software-driven efficiency that could be militarized include Planet Labs' automated imagery processing and SpaceX's autonomous docking systems. These same advancements, meanwhile, will also give American enemies more power. In May 2025, the first 12 of a projected 2,800-satellites were launched by Zhejiang Lab and Chinese firm ADA Space.[4] While in space, each satellite is built to process AI in real time. High-speed laser communications connect this constellation, which serves as a prototype for some-

thing revolutionary: the capacity to interpret and act on data in space without the need for ground infrastructure. Following that, real-time threat analysis by surveillance satellites and notifications that can be sent without waiting for confirmation from the ground will soon be available. From a military perspective, it is the origin of orbital decision making. These orbital capabilities are supported by China's expanding domestic computing base, which together comprise an end-to-end, vertically integrated system of AI infrastructure based in both space and on land.

The Western model is not the same as China's. Innovation in AI frequently originates from the bottom up in the United States, propelled by business sector investment and academia. The execution strategy in China is distinctly top-down, coordinating AI infrastructure with a long-term geopolitical stance, military doctrine, and state industrial policy. In 2015, China restructured its military to move beyond land defense and strengthen its ability to project power in space, cyberspace, and distant seas to protect strategic interests.[5] China is probably investigating the use of AI in space operations, including the management of large satellite constellations, the analysis of Earth observation datasets (processing and identifying targets in satellite imagery), and cognitive radio (a "smart" radio that makes space-based communications more efficient by automatically shifting channels to avoid interference and congestion) as well as autonomous satellite operation to compensate for limited communications windows, bandwidth, and long latencies, which lowers the workload of ground satellite operators. The People's Liberation Army (PLA) may find it more difficult to construct decision-support AI systems due to its limited combat experience and the resulting lack of "ground truth" data.[6] In this context, *ground truth* data refers to verified, accurate real-world data used to train and validate AI systems. These developments underscore that U.S. national security depends on ensuring American AI and automation capabilities for space operations remain unmatched, which will require sustained research, rapid development, and deployment of superior AI technologies for space—and on denying technologically ambitious rivals the opportunity to achieve parity or superiority in autonomous space warfare.

Paul Scharre raises a crucial point.[7] Although increasing financing for defense research and development is beneficial, it does not change the fact that most new technological advancements take place outside of the military. The Defense Department's new budget calls for major investments in AI and autonomy, including undersea drones, drone swarms, and autonomous "wingman" aircraft. The U.S. Air Force leads these efforts, requesting $789 million for its Collaborative Combat Aircraft program, which will deploy unmanned fighter drones alongside piloted jets. By 2029, the Air Force plans to invest about $28 billion in the program.[8] Although additional funding for defense research is

undoubtedly beneficial for national security, the military must collaborate with the civilian technology sector to remain informed about the most recent advancements. To remain competitive, the Department of Defense requires Congress's assistance in terms of its ability to adapt, act quickly, and collaborate with nontraditional technological businesses. To address the increasing complexity of catastrophic threats, the United States must prioritize the establishment of comprehensive security frameworks. It is imperative to invest in advanced weapon technologies, including antimatter, antigravity technology, and kinetic bombardment to safeguard national security and preserve global strategic influence in the presence of emerging threats.[9]

Research Objective

This study aims to evaluate cutting-edge weapon systems that could significantly strengthen U.S. defense capabilities. This evaluation is crucial for the U.S. military to sustain its strategic advantage amid rapidly evolving geopolitical challenges. This article reviews pertinent studies on emerging technologies and proposes approaches to improve U.S. national security. The main aim is to assess the strategic implications of kinetic energy weapons, antigravity technology, and antimatter weapons for national security. During the Vietnam War, the United States employed "Lazy Dog" explosives, which were small, fast-falling projectiles that could achieve speeds of up to 500 mph. These kinetic bombardment weapons were capable of penetrating nine inches of concrete when dropped from a height of only 3,000 feet.[10] Daniel C. Sproull states that kinetic energy weapons can create craters about 100 feet deep at Mach 10 and more than 150 feet deep at Mach 50, making them extremely devastating to subsurface infrastructure, surpassing the destructive capacity of certain nuclear weapons.[11] This makes kinetic energy weapons an essential instrument for the deliberate destruction of fortified subterranean facilities during future conflicts.

Despite being primarily theoretical, antimatter possesses an immense potential as a result of the substantial energy released during matter-antimatter annihilation. Recent National Aeronautics and Space Administration (NASA) research indicates that antiproton annihilation with heavier nuclei releases substantial energy, with roughly 10 percent of the annihilation energy converted into kinetic energy for nuclei as heavy as silicon, and up to 20 percent for very heavy nuclei such as uranium.[12] Antigravity technology, although predominantly theoretical, is garnering interest due to its potential to revolutionize military aircraft and space exploration. Some recent studies suggest that a natural antigravity force may exist, although it is not yet fully comprehended.[13] Harnessing such a repulsive force could facilitate the development of advanced propulsion systems, allowing for swift, fuel-efficient, and exceptionally maneuverable aircraft and drones. These developments would provide the U.S. mili-

tary with a substantial advantage in aerospace operations and strategic defense, ensuring a preeminent role in future combat situations. In the end, this article will be instrumental in the advancement and encouragement of future research endeavors in this rapidly evolving discipline.

Kinetic Bombardment (Rods from God) in U.S. Defense Strategy

Kinetic bombardment, commonly referred to as "Rods from God," is a space-based warfare system in which satellites deploy tungsten rods to strike terrestrial targets with significant destructive force. A kinetic energy weapon operates at hypersonic velocities, converting a portion or the entirety of its mass into energy at collision. The concept of deliberately harnessing this effect has been contemplated by the United States since the 1950s, when the Rand Corporation first proposed the deployment of tungsten rods on intercontinental ballistic missiles (ICBMs).[14] This technique, still theoretical, proposes a weapon system of a pair of satellites orbiting hundreds of miles above Earth. One satellite oversees targeting and communication, while the other contains several tungsten rods, each measuring up to 20 feet in length and 1 foot in diameter, prepared for deployment within 15 minutes. On order, the targeting satellite directs its counterpart to deploy a rod, which thereafter descends through the atmosphere at velocities comparable to meteors, reaching 36,000 feet per second, and impacts its target with catastrophic force, even when situated deep underground.[15] Tungsten rods traveling at hypersonic speeds could cause catastrophic damage to a city, but they would not wipe out humanity or necessarily kill everyone within the target area. This concept was part of Jerry Pournelle's argument in favor of such weapons, since unlike nuclear devices, they would not produce radioactive fallout. That said, deploying multiple tungsten projectiles could completely level a city much like several nuclear strikes would. Because they can penetrate hundreds of feet into the ground, they are particularly effective as bunker-busting weapons. Rather than being a traditional weapon of mass destruction, orbital tungsten strikes can be seen as a less extreme alternative to full-scale nuclear warfare.[16]

A tungsten rod–based kinetic energy weapon can be compared to the GBU-43/B Massive Ordnance Air Blast (MOAB), the largest precision-guided conventional munition in the U.S. Air Force arsenal, which has an estimated blast radius of 150 meters. Assuming a tungsten rod with a mass of 169,000 kilograms—approximately 90 percent of the payload capacity of an Ares V rocket—the destructive potential at various reentry velocities is considerable.[17] At Mach 10, the kinetic energy released on impact would be comparable to the detonation of 10 MOABs, or roughly 300,000 pounds of TNT, concentrated at a single point. At Mach 50, the release would approximate the yield of 247 MOABs, equivalent to nearly 4 kilotons of TNT. At impact, much of the

tungsten rod would vaporize, producing vapor and particulates capable of spontaneous combustion at temperatures exceeding 6,000 degrees Fahrenheit. In confined environments such as underground bunkers, this combustion would generate an intense fireball, compounding the destructive effects of the initial strike.[18]

With their high precision, rapid deployment, and global reach, these weapons could be employed to target fortified underground facilities, missile silos, or command centers with minimal warning. A primary benefit of this technology is its capacity to penetrate deeper into the Earth, resulting in significant underground damage. Kinetic bombardment presents a nonnuclear alternative to nuclear weapons, capable of delivering comparable destructive power against fortified targets while minimizing collateral damage and reducing the risk of escalation. There are significant difficulties and technical barriers that prevent kinetic bombardment techniques from being used effectively. A principal barrier is the high expense of deploying and maintaining these systems in orbit, particularly due to the substantial costs associated with bringing massive tungsten rods into space.[19] One additional significant issue is the accumulation of space debris. The deployment of kinetic energy weapons in space could significantly exacerbate the existing issue of orbital debris. For instance, the 2011 antisatellite test that resulted in the destruction of the Fengyun-1C satellite produced 3,037 fragments of trackable debris, underscoring the potential for such systems to exacerbate this issue.[20]

It is important to recognize that efforts to mitigate orbital debris are already underway, with Japan playing a leading role. Such initiatives indicate that the challenge of space debris extends beyond national security concerns and is being addressed through technological and commercial innovation. A key example is the (Active Debris Removal by Astroscale-Japan) mission, operated by Astroscale-Japan, a subsidiary of Astroscale Holdings—the world's first private enterprise dedicated to space debris removal. Founded in 2013, the company has developed collaborative partnerships with organizations including JAXA and the UK Space Agency, with the objective of commercializing debris-removal services by 2030.[21] Through committed research and funding, these difficulties could be overcome.

The United States is now facing the possibility of a space-based missile threat from low-Earth orbit, in addition to the already overwhelming threat posed by China's quickly growing arsenal of conventional and nuclear missiles deployed from the air, land, and sea. China could deploy dozens of orbiting missiles with nuclear warheads within 10 years, according to a 13 May 2025 Defense Intelligence Agency assessment that was reported by Bloomberg.[22] Compared to conventional ICBMs, these systems may strike the mainland United States faster than conventional, Earth-based weapons. Among the sever-

al sophisticated missile threats highlighted, the most significant may be China's potential development of a Fractional Orbital Bombardment System (FOBS). FOBS is defined by the Defense Intelligence Agency as an ICBM that enters a low-altitude orbit before reentry, allowing for significantly shorter flight durations along traditional routes or the choice to approach over the South Pole to avoid missile defenses and early warning systems. The payload is deployed prior to the spacecraft completing an entire orbital revolution. Although such a capacity has significant strategic implications for both conventional and nuclear payloads, no state has yet to fully develop or implement such a system. China may have up to 60 operational FOBS missiles by 2035, while Russia is only expected to have 12.[23] The emergence of the FOBS demands that the U.S. Air Force rapidly intensify its research efforts to design either a resilient countermeasure or a more sophisticated system capable of neutralizing such threats.

At the same time, the United States could pursue a comprehensive sanctions strategy that extends beyond conventional economic measures to directly target the technological underpinnings of adversarial weapons development. This would include restricting access to U.S.-origin semiconductors, satellite components, advanced sensors, precision guidance technologies, and dual-use equipment critical for space and missile programs. Sanctions could also bar American firms, research institutions, and investors from any form of collaboration or knowledge transfer that might indirectly enhance FOBS-related capabilities. Moreover, U.S. policy could be broadened to penalize third-party states that provide material, technological, or logistical support to China or Russia in this domain. Such measures might include secondary sanctions against companies or governments that export restricted components, limit enforcement of export controls, or facilitate financial transactions linked to aerospace or missile research. By leveraging its central role in global technology supply chains and financial systems, the United States could not only weaken the direct development capacity of its rivals but also dissuade partner nations from enabling the proliferation of advanced orbital strike systems.

In modern geopolitical environments, nonnuclear states that are looking for a nuclear-style deterrent or are concerned about the deterioration of security assurances from conventional nuclear partners can theoretically seek orbital kinetic bombardment capabilities, such the so-called "Rods from God." For example, Brazil, which does not possess nuclear weapons but has demonstrated the capability to launch satellites and maintains the resources to expand such programs, represents a compelling case. As a nonnuclear state with a well-developed space agency—the largest in South and Central America—and a history of nuclear research that was pursued under the military regime but later abandoned, Brazil retains the technical foundations necessary to pursue advanced strategic systems if it so chose. It is also one of the largest and wealthiest

countries with minimal nuclear defense capabilities, having forsworn nuclear weapons under the terms of the Nuclear Non-Proliferation Treaty. In a deteriorating security environment, a state such as Brazil might theoretically declare the deployment of a small constellation of satellites equipped with tungsten projectiles—Rods from God—as a retaliatory mechanism against strategic or tactical threats. Such an orbital kinetic bombardment system could provide a novel form of strategic deterrence while technically remaining outside the formal restrictions of nuclear nonproliferation regimes, offering a means of achieving deterrence without the complications of radioactive fallout. A move like that would immediately prompt questions about how the world would react: Would Brazil be subject to export restrictions, diplomatic isolation, or economic sanctions akin to those imposed for nuclear proliferation, or would governments be reluctant to act for fear of legitimizing the capability as a new kind of deterrent?

This dynamic is likely to drive the parallel development of antikinetic bombardment defense systems over time. These systems combine electronic warfare, high-power laser dazzling, kinetic- or directed-energy interceptors, and space-based early warning systems to detect, track, and neutralize incoming projectiles prior to atmospheric entry. When developed, such systems would offer some protection to a possible victim state, which would lessen orbital kinetic weapons' strategic coercive value and possibly restore equilibrium in deterrence relationships. It is important that the United States prioritize protective measures for space and prioritize significant investment in kinetic bombardment systems. This strategy is essential for enhancing military capabilities and securing leadership in space operations. By safeguarding space assets and enhancing technology, the United States can attain a strategic advantage in a world where space increasingly impacts global security and defense.

Antimatter's Possibilities for Future Weapons and Space Propulsion

The potential application of antimatter as a weapon remains primarily theoretical, motivated by its distinctive capacity to unleash vast energy through the annihilation of matter, as defined by Albert Einstein's $E=mc^2$ equation.[24] In 1983, the Rand Corporation conducted a study for the U.S. Air Force, examining the feasibility of harnessing matter-antimatter annihilation for its significant energy output. The research sought to examine the viability of using this energy for realistic military purposes.[25] The Antihydrogen Laser Physics Apparatus team at the European Organization for Nuclear Research (a.k.a. CERN) has successfully measured antimatter to the highest precision to date, revealing the spectral details of antihydrogen atoms with extraordinary clarity. This milestone, which was achieved after three decades of dedicated research, marks the beginning of

a new era in the comparison of matter and antimatter.[26] In contrast to armaments, the application of antiprotons as a propulsion propellant is a promising area. The antiproton is more advantageous than the antielectron for propulsion systems. On collision with a proton or neutron, an antiproton generates three to seven pions rather than emitting immediate gamma rays.[27] The charged pions, traveling at 94 percent of the speed of light, persist for approximately 70 nanoseconds, enabling them to cover roughly 21 meters, which facilitates their capture in a magnetic thrust chamber. This framework converts the energy produced by the micro explosion into thrust. As these pions decay, they generate energetic muons that can continue to contribute to propulsion for an extended period.[28] A muon is an unstable lepton, similar to an electron but about 207 times heavier and negatively charged.[29] CERN physicist Rolf Landua clarifies that although antimatter bombs possess considerable theoretical potential, the expense of antimatter production makes them extremely impractical. Landua predicts that the production of a single gram of antimatter may incur costs up to one quintillion dollars, deeming the development of such weapons economically unfeasible currently.[30] It is reasonable to anticipate a future scenario in which associated costs are reduced. Physicists at University of California-Riverside have successfully synthesized molecular positronium, a novel state of matter consisting of two electrons and two positrons bound together. Formed through collisions between positronium atoms—hydrogen-like systems of an electron and positron—this molecule represents a transient yet significant step in the study of matter–antimatter interactions. The work advances fundamental understanding of annihilation processes and offers new methods for generating antimatter ensembles, with potential implications for future scientific and technological developments.[31] China is actively contributing to antimatter research, demonstrating that it is not lagging in this advanced scientific field. An important development in antimatter research was made when a team of Chinese and foreign scientists used a heavy ion collider in the United States to detect a new type of antimatter hypernucleus. In a report published in *Nature*, the researchers, headed by the Chinese Academy of Sciences' Institute of Modern Physics, discovered antihyperhydrogen-4, the most enormous antimatter hypernucleus yet seen in lab studies.[32] Researchers with the STAR Collaboration have detected the antimatter hypernucleus antihyperhydrogen-4—made up of an antihyperon, one antiproton, and two antineutrons—during atomic nucleus collisions at the Relativistic Heavy Ion Collider at the U.S. Department of Energy's Brookhaven National Laboratory.[33] This underscores that the United States cannot remain idle but must undertake intensive research on antimatter technology with the goal of integrating it into military capabilities by 2050.

A Proposal for U.S. Innovation in Antimatter Missile Technology

To provide the United States with significant advantages in both offensive and defensive capabilities, this study suggests the development of advanced antimatter-based missiles. These advanced missiles, which are intended to deliver controlled antimatter explosives, can be manufactured in a variety of configurations, including stealth, high precision, and adaptability to a variety of deployment strategies. The potential game-changing aspect of antimatter technology lies in its ability to unleash vastly greater destructive power from an extremely small quantity of material, making it far more energy-dense and efficient than conventional or even nuclear weapons.[34] The ultimate objective is to avert conflict by demonstrating strength, thereby discouraging potential adversaries from engaging in hostile behavior. A substantial financial investment is essential to make this technology viable and to secure enduring U.S. dominance in this sector. The production and containment of antimatter is presently incredibly costly and poses significant technological obstacles that need to be addressed. It is important to conduct research that concentrates on the production of antimatter at a low cost, as the current methods are both inefficient and costly. Investments should prioritize the expansion of production, the improvement of storage methods, and the strengthening of containment systems to reduce costs without compromising safety. Equally critical are persistent research and financial investment in the integration of antimatter systems with missile technology. This involves the creation of precision autonomous targeting systems and compact containment units to guarantee the safe and precise delivery of antimatter payloads.

In addition, the proposed recommendation also emphasizes the significance of the BASE-STEP device, which was developed by CERN's BASE collaboration. This device is a significant advancement in the safe transportation and containment of antimatter for emerging missile technology. By carefully using electric and magnetic fields to keep antimatter secure, this advanced device—an upgraded version of the Penning trap—ensures safe, regulated transfers by keeping it from contacting regular matter while being transported. A Penning trap uses combined electric and magnetic fields to confine charged particles. BASE-STEP improves this system by including a robust 1-Tesla superconducting magnet to mitigate external disturbances and a liquid helium buffer to maintain the requisite low temperatures for secure transport.[35] However, Penning traps alone are insufficient for neutral antiatoms. In such instances, magnetic bottle traps are employed, leveraging the magnetic fields generated by superconducting magnets to more efficiently confine neutral particles.[36] The difference underscores the complexity of antimatter confinement, as each kind

necessitates specific tools for safe handling. In the case of missiles, integrating antimatter technology poses both significant opportunities and unique technical challenges. Advanced missiles benefit from their larger payload capacity.[37] The extra space in advanced missiles allows for the integration of powerful magnetic fields and containment systems, supporting robust energy sources and stable antimatter storage until detonation. These missiles can also be equipped with advanced guidance systems and remote detonation capabilities, enabling precise targeting and controlled antimatter explosions at critical moments. To initiate antimatter explosions, meticulously controlled procedures are necessary to ensure that antimatter contacts with matter at the exact moment, resulting in annihilation. This can be accomplished by deactivating the magnetic fields that confine the antimatter, bringing matter into the containment, or employing remote signals. To guarantee a controlled detonation, each method necessitates precise control of containment fields and timing. Nevertheless, there are still significant obstacles to overcome, such as the development of energy sources that are both potent and efficient to keep vacuum chambers and strong magnetic fields in compact, advanced missile systems.

To safeguard U.S. national security, it is crucial for the United States to retain complete control over the development of antimatter-based missile technology. To prevent any foreign access, whether from allies or adversaries, all related patents and intellectual property must remain under exclusive U.S. jurisdiction. This technology must be rigorously prohibited from being shared or sold to reduce the risk of proliferation or misuse. Research opportunities in this field should be restricted to U.S. citizens with top secret clearances, thereby mitigating the risk of intellectual property theft or espionage. Additionally, it is vital to prevent technology transfers or collaborations that involve foreign nationals, international students, or foreign governments to maintain security. By limiting antimatter missile development to U.S. territory and restricting access to authorized personnel, the United States can safeguard its strategic superiority and maintain secure control over this revolutionary technology. This strategy is crucial for increasing national security and averting potential misuse that could threaten global stability.

Myth to Reality: The Role of the "Chariot of God" Antigravity Technology and Propellantless Propulsion in the U.S. Air Superiority Strategy

Antigravity is a force that repels two massive objects from one another. The expansion of the universe is believed to be influenced by this repelling force.[38] Antigravity technology and propulsion systems, which are envisioned for advanced aircraft such as the legendary "Chariot of God," feature cutting-edge physics that surpasses conventional physics and propulsion techniques. By using non-

reactive forces, these antigravity systems offer a completely unique method of lift and movement.[39] The Chariot of God is often a symbolic or mythological reference, most famously in the Biblical account of the prophet Ezekiel's vision, where a divine chariot appears to descend from the heavens, moving in ways that defy natural laws. It has sometimes been interpreted in modern thought as a metaphor for advanced or otherworldly technology. The analogy to antigravity derives from the notion that, similar to the chariot's extraordinary and seemingly impossible movements, antigravity technology would enable vehicles to transcend gravitational constraints and operate beyond the boundaries of conventional physics. To detect obvious gravitational effects with a moderate quantity of mass, it is necessary to have matter that is highly dense. This underscores the potential importance of researching degenerate matter, which may provide methods to generate and manipulate gravitation effectively.[40] Degenerate matter arises under conditions of extreme density, where the Pauli exclusion principle governs its behavior. Electrons or other fermions are forced into such proximity that they cannot share identical quantum states, producing a degeneracy pressure that prevents further collapse. In a high-temperature superconductor (HTSD), the minuscule pull of each atom is amplified by the collective effect of the multitude of atoms within the disk. According to Dr. Ning Li, her device could produce a force field that is sufficiently powerful to counteract gravity over a one-foot-wide area, extending from the Earth's surface to outer space, with only approximately one kilowatt of electricity.[41]

In 2001, British electrical engineer Roger Shawyer introduced the concept of a propellantless drive. Known as the EmDrive, this device claimed that it could operate without propellant, thereby challenging the known laws of physics, specifically the law of conservation of momentum. This revolutionary device, the EmDrive, is composed of a conical cavity that is filled with microwaves. As the microwaves bounce around inside, they generate a difference in radiation pressure, which generates thrust toward the narrow end of the cone.[42] This hypothesis challenges known physics by proposing that propulsion can occur within a closed system without the need for external reaction mass. Dr. Charles Buhler's team, comprising specialists from NASA, Blue Origin, and the Air Force, dedicated decades to investigating propellantless motors before redirecting their attention to electrostatics. Their devices initially generated only a negligible amount of thrust; however, each new version demonstrated improvements. By 2023, their "New Force" initiative produced sufficient thrust to offset Earth's gravity.[43] Dr. Franklin Felber posits that a mass traveling at a rate exceeding 57.7 percent of the speed of light generates a gravitational repulsion, or an antigravity beam, that directly affects other masses in its vicinity.[44] This beam intensifies as the object's velocity nears that of light. His findings address how this repelling effect could be leveraged to rapidly accelerate large spacecraft

while minimizing internal tidal forces, so safeguarding the cargo from potential damage.[45] The concept may facilitate revolutionary propulsion technology, transforming not only space exploration but also the defense strategies of the U.S. military on Earth and in space.

Petar K. Anastasovski, in his research on superluminal relativity, suggests the possible existence of elements with atomic numbers (Z) extending up to 145, where Z denotes the number of protons in an element's nucleus. Within this extended range, certain elements—particularly those near $Z = 145$—are hypothesized to exhibit unique properties, including potential antigravitational effects. His study demonstrates that curved space-time, exhibiting both gravitational and antigravitational properties, exists not just surrounding but also within atomic nuclei. He classifies elements into two categories: those with $Z < 64$, possessing nuclei with solely gravitational mass, and those with $63 < Z < 145$, whose nuclei demonstrate both gravitational and antigravitational characteristics in various regions of curved space-time.[46] Anastasovski's theory asserts that antigravity elements have the potential to expand the boundaries of physics, enabling innovative advancements in energy, transportation, and gravity manipulation. If further researched and experimentally advanced, this theory could contribute to significant progress in antigravity technology research. The objective of achieving interstellar travel within a human lifetime remains unattainable using even the most advanced technological implementations grounded in current physics. Constraints such as the exhaust velocity and propellant mass dictated by the rocket equation, or the immense power requirements for photon-based momentum transfer, place this goal in the realm of the seemingly impossible.[47] However, solar sails offer a low-cost way to achieve high-speed exploration of the outer solar system and beyond. By slingshotting close to the Sun (2–5 solar radii), they could push lightweight cubesats to >0.1% of light speed (>300 km/s). This would turn the Sun into a launch pad, enabling missions to outer planets in months, interstellar space in a few years, and 1,000 AU in under 20 years.[48] Nevertheless, history demonstrates that sustained advanced research, coupled with substantial investment, can overcome formidable technical barriers; humanity's successful mission to the Moon serves as a testament to what dedicated effort and innovation can achieve.

To further explore the concept of antigravity technology, this study examines an unidentified anomalous phenomena (UAP) incident which—although often dismissed as pseudoscience—may nonetheless offer insights worthy of scientific consideration. UAPs are inexplicable space or airborne events that occasionally exhibit flight characteristics that seem to violate accepted aerodynamics, such as severe acceleration and silent hovering. Theories regarding cutting-edge technology like propellantless propulsion and antigravity have been stoked by these observations, as they may one day allow for similar maneuvers without the

use of traditional fuel or lift systems. Although UAP sightings are frequently reported, no definitive data currently confirms their existence as extraterrestrial in origin; however, one such observed object was described as exhibiting apparent antigravity characteristics and a propellantless propulsion system. Retired U.S. Navy commander David Fravor testified before a U.S. House Representatives subcommittee on UAP about his experience commanding a Boeing F/A-18F Super Hornet squadron onboard the USS *Nimitz* (CVN 68) on 14 November 2004, when he encountered an unidentified object off the coast of Southern California. Fravor said radar equipment on board the USS *Princeton* (CVL 23) spotted several anomalous aerial vehicles that descended from about 80,000 feet in less than a second. Redirected from training activities, Fravor and Lieutenant Commander Alex Dietrich saw one such thing, about the size of an F/A-18F, with no wings, markings, or exhaust, making quick movements, including an acceleration that made it disappear from view. In less than a minute, the object was claimed to have been reacquired on radar approximately 60 miles away.[49]

It is important to note that while the extent of China's progress in antigravity research and development remains unclear, evidence suggests that some crucial work in this area is actively underway. Closely monitoring China's progress in this area is crucial to safeguarding U.S. national interests and ensuring strategic advantage. A hypergravity facility known as the Centrifugal Hypergravity and Interdisciplinary Experiment Facility (CHIEF) was recently opened in China. It can generate 1,900 g-t, or a gravity that is 1,900 times greater than that found at the surface of the Earth. By surpassing the U.S. Army Corps of Engineers' 1,200 g-t facility, CHIEF is now the most potent hypergravity research station in the world. CHIEF is ranked among the top 10 national scientific and technology infrastructure projects in China. In 2020, the facility's development started in Hangzhou, Zhejiang province. Hypergravity, however, is a costly endeavor. For example, the Chinese will have to pay an astounding $276.5 million (2 billion yuan) for CHIEF before it is even operational. Currently, the facility currently houses three giant centrifuges—large radial arms that rotate at high speeds to generate an outward-pushing effect known as centrifugal force. In rotating systems, this force can mimic the effects of gravity and is therefore referred to as artificial gravity.[50] In rotating systems, this force functions similarly to gravity and is called artificial gravity. In contrast to natural gravity, which diminishes with increasing distance from the Earth's center, centrifugal force is dependent on both radius and rotational velocity. Although there is currently no method to augment Earth's natural gravitational pull, scientists can generate artificial gravity that is significantly stronger than natural gravity by greatly increasing centrifugal force simply by adjusting the spinning arm's radius and rotational speed.[51] Even while China's advancements seem remarkable, the U.S. Air Force's persistent and rigorous study in this area

may result in unmatched antigravity technology that can repel enemies on a never-before-seen scale.

Strategic Superiority through Next-Generation Antigravity Aircraft and Humanoid Robotic Warfare Systems

The author of this article recommends the United States should invest in the development of advanced antigravity aircraft to gain a substantial strategic advantage in air and space operation. Should antigravity technology develop, these aircraft may attain unprecedented speed and agility, enabling rapid, unpredictable maneuvers that would be exceedingly difficult to track or counteract.

This study also suggests the development of silicone-based humanoid robots and specialized vehicles, each having superior antigravity propulsion, to strengthen the United States' military capabilities beyond antigravity aircraft. Because of silicon's advantageous qualities—lightweight yet durable structure, thermal resistance, and the ability to integrate seamlessly with advanced sensors and electronics—silicon-based humanoid robots and specialized vehicles, each equipped with advanced antigravity propulsion, could offer unique advantages.[52] The soft robot can be safely handled while in operation, and its silicone body is naturally durable, withstanding harsh conditions such as snow, water, brief exposure to flames, and even the pressure of being run over by a car.[53] The successful development and integration of advanced antigravity technology would be a prerequisite for the creation of a fully operational, flyable humanoid robotic combat system. In theory, a system like this may replace some of the strategic deterrents that nuclear weapons have historically provided, providing a similar strategic impact without the radioactive fallout. With enhanced propellantless maneuverability, these robots could navigate through dangerous areas, hit specific targets with accuracy, and avoid defenses, assuring their survival. In contrast to traditional large-scale weapon systems, their accuracy and mobility could reduce or even eliminate civilian casualties while still accomplishing important military goals. These proposed robots and vehicles, presumably launched from warships in warfare, would be engineered for multifaceted combat missions, competent in engaging on land and in the air with exceptional precision. Antigravity propulsion systems would make the robots exceedingly challenging to target and defeat, as their exceptional maneuverability would enable them to make rapid, multidirectional movements, evade enemy fire, and effortlessly navigate intricate terrains. The robots would rely on nonnuclear weaponry for targeted engagements, while the carrier vehicle could be equipped with a reserved nuclear device for critical situations. To address emerging threats, this approach would substantially improve strategic response capabilities by emphasizing precision, flexibility, and survivability.

The robots and their vehicles would be remotely controlled from U.S.-based command centers via a secure satellite communication system, facilitating real-time tactical updates and preserving control even in hostile circumstances when alternative connections may be compromised. The satellite connection ensures reliable and consistent command, facilitating rapid reactions. Even while the ideas presented in this proposal might seem futuristic at first, it is essential to remember that three centuries ago, modern propulsion technologies and conventional airplanes would have been considered unrealistic. Past experiences show that persistent, well-funded research can turn seemingly imaginary concepts into practical realities, speeding up technical advancement and producing significant strategic advantages. China might have completely autonomous military weaponry on the battlefield in as little as two years. According to defense analyst Francis Tusa, China is not hampered by ethical concerns over so-called killer robots and is developing autonomous weapons systems faster than any other country.[54] Although China has shown a significant investment in robotics and propulsion research, there is no public evidence that it has pursued this particular silicon-based, antigravity-integrated platform, possibly due to technological barriers, material supply constraints, or strategic prioritization of other defense technologies. Attaining this innovative technology in the near future necessitates intensive scientific research and more financing. As global threats escalate and other nations progress, prioritizing this innovation will enable the United States to maintain its competitive edge. To safeguard national security and preserve exclusive strategic advantages, it is essential that this technology is not traded, shared, or transferred to any foreign nations, including allied countries and NATO-allied countries, after it has been developed. The United States must ensure that only U.S. citizens possessing top-secret clearance participate in antigravity research and development. This additional security measure would serve to safeguard against potential intrusions and bolster the nation's position as a leader in advanced defense technologies.

Proposal for Advancing UAV Propulsion Systems through Antigravity Technology

This article proposes the development of drones using an antigravity propulsion system, potentially representing a significant advancement in aerospace technology, transforming airborne mobility with remarkable efficiency and agility for defense and surveillance operations. Although antigravity technology has yet to be discovered, its future developments could transform drones into a powerful asset for military operations. An antigravity technology-powered drone could provide an innovative alternative to the limitations of traditional propulsion systems that depend on rotor blades, fuel, or batteries for thrust.[55] This innovation has the potential to improve the maneuverability and stability

of drones, allowing them to operate in challenging environments such as urban areas, adverse weather, and high altitude. The effective use of antigravity propulsion in drones has the potential to revolutionize the fields of logistics, surveillance, emergency response, and even interplanetary exploration, thereby expanding the limits of drone and propulsion technology. It is crucial to participate in further scientific research on the incorporation of antigravity propulsion systems into drones to enhance U.S. national security.

Ensuring Accountability and Oversight in Advanced Weapons Development

As next-generation weaponry technology progresses, it is imperative to regulate it carefully to mitigate any potential risks. It is important to prioritize global safety and ethical standards as the United States contemplates pursuing powerful technologies such as antimatter weapons, kinetic bombardment, and antigravity technology. The implementation of oversight can serve to prevent unintentional escalations, safeguard against the widespread distribution of these technologies, and ensure compliance with international regulations. The Massachusetts Air National Guardsman alleged to have leaked top-secret military documents is a concerning example of a vulnerability in the way the United States protects sensitive information.[56] This incident underscores the dire need for increased cybersecurity and supervision in military and intelligence environments, as it emphasizes actual concerns regarding the potential security risks associated with new technologies and digital platforms. These types of disclosures not only undermine public confidence but also pose a threat to critical operations and national security. It is important to establish specific responsibilities among the government, defense contractors, and research institutions to prevent the misuse of advanced weapons technology and ensure that it is consistent with U.S. security objectives. Effective oversight and frequent audits are crucial for preventing unintended damage and ensuring accountability. To avoid transferring sensitive technology overseas, defense contractors must also adhere to rigorous standards, face stringent audits, and follow strict guidelines. By achieving a balance between accountability and innovation, it will be possible to maintain stability and security. Without comprehensive governance, these potent technologies could pose significant risks, which could affect national security in unpredictable ways.

Conclusion: Preparing for the Next Era of Warfare

Kinetic bombardment is the most instantly practical and strategically disruptive of the new space technologies. Orbital tungsten Rods from God might be used immediately, delivering devastating precision hits without radioactive fallout, in contrast to antimatter systems or sophisticated propellantless propulsion, both

of which are still decades away from being fully developed. Such a capability could destabilize current deterrence architectures and encourage wider adoption by allowing a nonnuclear state to achieve a nuclear-level deterrent effect while technically avoiding violations of current nonproliferation agreements, as demonstrated in the hypothetical Brazil scenario.

Although still more distant from practical implementation, antigravity technology and propellantless propulsion, along with antimatter weapons, hold even greater transformative potential: the former could enable rapid, unpredictable, and sustained maneuvering throughout the battlespace, while the latter promises an unmatched energy density. As observed in this study, China is making significant strides in the fields of antimatter and hypergravity research, as well as the development of a FOBS. It is worth noting that a United States committed to long-term, well-funded research through the Air Force Research Laboratory, DARPA, and the national laboratories could attain operational leadership in all three areas by 2050, thereby influencing the strategic landscape rather than merely reacting to enemy developments. It is also important to develop advanced antikinetic bombardment defense systems in parallel, incorporating directed-energy systems, rapid interceptors, and space-based surveillance to ensure the comprehensive defense of the homeland against potential enemy deployments.

While the development of an advanced kinetic bombardment system should be the first priority for the United States, the creation of an antikinetic bombardment defense system should also be pursued, with the goal of achieving operational capability by 2030 through intensive research and sustained funding. The United States may use severe economic sanctions and other coercive measures against nations that attempt to abuse such capabilities until a strong antikinetic bombardment defense system is completely developed and put into place to defend the American homeland from any enemy strikes. It is also critical to reiterate that, once operational maturity is reached, no advanced kinetic bombardment or antikinetic bombardment defense system, antimatter technology, or antigravity and propellantless propulsion technology developed by the United States should be traded, shared, or transferred to any foreign country, including allied and NATO member states—to protect national security and maintain exclusive strategic advantages. Furthermore, it is imperative that no foreign nationals be allowed to work on the research, development, or testing of these systems because there is a considerable chance that technical expertise, design processes, or operational ideas will be transferred—directly or indirectly—for use in other nation-states' defense programs.

Moreover, while strategic inaction in these areas could lead to the loss of U.S. technological supremacy, sufficient investment could lead to long-term dominance of the United States and the potential to establish standards for

these potent technologies well into the second half of the twenty-first century. As other nations continue to enhance their capabilities, the United States must seriously contemplate the development of these technologies to guarantee an everlasting military superiority. History has consistently shown that those who invent and develop a technology first secure a decisive first-mover advantage. In China, for example, "The PLA also aims to surpass the U.S. in modernization, capabilities, and power projection capacity by 2049."[57] This aligns with other People's Republic of China's strategies to leapfrog other major powers technologically, using the United States as a benchmark: "The plan involves a 'leapfrog development' strategy, integrating mechanization, informatization, and 'intelligentization' (AI) to achieve dominance in weaponry, training, and military theory, ensuring it can win wars and safeguard peace."[58] This article advocates leapfrogging Chinese technologies to overcome current and future developments by planning and funding for technologies that enable the United States to maintain technological superiority over its most powerful competitor.

Achieving these new capacities is not merely an issue of innovation but an essential strategic priority in an age where technology supremacy is crucial to national defense, as evidenced by the strategic priorities of the People's Liberation Army. By implementing proactive planning, oversight, and innovation, the United States can maintain its position as a leader in military power in a global landscape that is becoming increasingly complex and competitive.

Endnotes

1. *Annual Threat Assessment of the U.S. Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, 2023), 10.
2. *Nuclear Posture Review* (Washington, DC: Department of Defense, 2022), 10.
3. Paul Scharre and Michael C. Horowitz, *An Introduction to Autonomy in Weapon Systems* (Washington, DC: Center for a New American Security, 2015), 6.
4. Andrew Jones, "China Launches First of 2,800 Satellites for AI Space Computing Constellation," *SpaceNews*, 14 May 2025.
5. Amy J. Nelson and Gerald L. Epstein, "The PLA's Strategic Support Force and AI Innovation," Brookings Institution, 23 December 2022.
6. Nelson and Epstein, "The PLA's Strategic Support Force and AI Innovation."
7. Paul Scharre, *Preserving U.S. Military Advantage Amid Rapid Technological Change* (Washington, DC: Center for a New American Security, 2024).
8. Patrick Tucker, "Defense Department Budget Request Goes Hard on AI, Autonomy," *Defense One*, 1 July 2025.
9. Antimatter is matter composed of antiparticles that release immense energy when interacting with normal matter; antigravity technology refers to a theoretical means of counteracting gravity for propulsion or levitation without conventional thrust; and kinetic bombardment describes the proposed use of high-velocity projectiles, such as orbital "Rods from God," to deliver destructive force through sheer kinetic energy rather than explosives.
10. Blake Stilwell, "These Air Force 'Rods from God' Could Hit with the Force of a Nuclear Weapon," Military.com, 22 December 2020.

11. Daniel C. Sproull, "Kinetic Energy Weapons: The Beginning of an Interagency Challenge," *InterAgency Journal* 8, no. 2 (2017): 65.
12. Mike LaPointe, *Antimatter Propulsion* (Washington, DC: Marshall Space Flight Center, National Aeronautics and Space Administration, 2020), 12.
13. John G. Cramer, "Antigravity II: A Fifth Force?," *Analog Science Fiction & Fact Magazine*, 1 February 1986.
14. Sproull, "Kinetic Energy Weapons," 62.
15. Eric Adams, "Rods from God," *Popular Science*, 1 June 2004.
16. Jeff Edwards, "Rods from God: Unleashing Orbital Kinetic Bombardment as a Theoretical Defense System," *MIRA Safety* (blog), 21 August 2025.
17. Sproull, "Kinetic Energy Weapons," 63–66.
18. Sproull, "Kinetic Energy Weapons," 63–66.
19. Jonathan Shainin, "Rods from God," *New York Times Magazine*, 10 December 2006.
20. Anelí Bongers and José L. Torres, "Orbital Debris and the Market for Satellites," *Ecological Economics* 209 (July 2023): 6, https://doi.org/10.1016/j.ecolecon.2023.107831.
21. Takanori Isshiki, "Japanese Space Cleaner's First Mission a Success," *Jstories*, 2 May 2024.
22. Anthony Capaccio, "U.S. Warns of Missile Threats That Trump's Golden Dome May Face," Bloomberg, 13 May 2025.
23. Sakshi Tiwari, "China's 'Orbital' Nuclear Missiles that Could Hit the U.S. from Space Rattles Pentagon; Why U.S. Fears FOBS?," *Eurasian Times*, 22 August 2025.
24. "Collisions of Light Produce Matter/Antimatter from Pure Energy," Brookhaven National Laboratory, 28 July 2021.
25. Bruno Augenstein, *Concepts, Problems, and Opportunities for Use of Annihilation Energy: An Annotated Briefing on Near-Term RDT&E to Assess Feasibility* (Santa Monica, CA: Rand, 1985), 48.
26. Ana Lopes, "A New Era of Precision for Antimatter Research," CERN, 4 April 2018.
27. Pions, the lightest mesons, are the easiest to produce in annihilation; thus, proton–antiproton annihilation mainly yields multiple pions.
28. Robert Forward, "Antiproton Annihilation Propulsion," *Journal of Propulsion and Power* 1, no. 5 (1985): 370, https://doi.org/10.2514/3.22811.
29. A muon is an unstable elementary particle, similar to the electron but about 207 times heavier, carrying a negative charge, and belonging to the lepton family of fundamental particles.
30. Amanda Gefter, "What About Antimatter Bombs?," *New Scientist*, 22 April 2009.
31. "Molecules of Positronium Observed in the Laboratory for the First Time," EurekAlert!, 12 September 2007.
32. "Chinese, Foreign Physicists Make New Discovery in Antimatter," Chinese Academy of Sciences, 22 August 2024.
33. "New Heaviest Exotic Antimatter Nucleus," Brookhaven National Laboratory, 21 August 2024.
34. Manoj Lakhan, "Antimatter Fuel," *International Journal of Innovative Research in Science, Engineering and Technology* 7, no. 4 (April 2018), https://doi.org/10.15680/IJIRSET.2018.0704140.
35. BASE-STEP refers to Baryon Antibaryon Symmetry Experiment- Symmetry Tests in Experiments with Portable Antiprotons. Michael Irving, "CERN Scientists Design Trap to Transport Antimatter Between Facilities," *New Atlas*, 3 November 2020.
36. William Bertsche, "Antimatter: We Cracked How Gravity Affects It—Here's What It Means for Our Understanding of the Universe," *Conversation*, 27 September 2023.
37. Michael Sirak, "Air Force Envisions Mid-Term, Prompt Global Strike Missile," *Defense Daily*, 7 July 2006.
38. Leandros Perivolaropoulos, "Dark Energy Antigravity" (presentation, 2d Hellenic Cosmology Meeting, National Observatory of Athens, Penteli, Greece, 19–20 April 2001).
39. Alexander Gromov, "Antigravity Based Propulsion Systems—A New Era in Astronautics and Aeronautics" (7th European Conference for Aeronautics and Space Sciences, Milan, Italy, 3–6 July 2017).

40. S. Anandaraj and S. R. Arun, "Design and Analysis of Anti-Gravity Propulsion for Aerodynamic Lift," *South Asian Journal of Engineering and Technology* 8, no. 2 (2019): 289–92.
41. Noah Logan, "Solving the Mystery of Huntsville's Brilliant Anti-Gravity Scientist," *Huntsville Business Journal*, 30 July 2023, 6–8.
42. Eric Ralls, "NASA Engineer Creates Propulsion System that Defies the Laws of Physics," Earth.com, 5 February 2024.
43. Ralls, "NASA Engineer Creates Propulsion System That Defies the Laws of Physics."
44. Bill Christensen, " 'Antigravity' Propulsion System Proposed," Space.com, 15 February 2006.
45. Christensen, " 'Antigravity' Propulsion System Proposed."
46. Petar K. Anastasovski, "The Superheavy Elements and Anti-Gravity," *AIP Conference Proceedings* 699, no. 1 (2004): 1230–37, https://doi.org/10.1063/1.1649695.
47. Marc G. Millis and Eric W. Davis, eds., *Frontiers of Propulsion Science* (Reston, VA: American Institute of Aeronautics and Astronautics, 2009).
48. Artur Davoyan, "Extreme Solar Sailing for Breakthrough Space Exploration," NASA, 8 April 2021.
49. Aliza Chasan, "The Story behind the 'Tic Tac' UFO Sighting by Navy Pilots in 2004," CBS News, 26 July 2023.
50. Rupendra Brahambhatt, "China Builds the World's Most Powerful Hypergravity Facility. It Can Simulate Gravity 1,900 Times Stronger than Earth's," ZME Science, 27 November 2024.
51. Brahambhatt, "China Builds the World's Most Powerful Hypergravity Facility."
52. Enrique, "Silicone vs. Other Materials—The Ultimate Showdown for Manufacturing Superiority," *Newtop Silicone* (blog), 15 March 2023.
53. Rajesh Uppal, "Soft Robotics Transforming Military Soft Exosuits in Reducing Injuries to Explosive Ordnance Disposal," International Defense, Security, and Technology, 30 May 2023.
54. "AI Arms Race: China Could Have Killer Robots on the Battlefield in Two Years," National Security News, 25 June 2024.
55. Bowen Zhang et al., "Overview of Propulsion Systems for Unmanned Aerial Vehicles," *Energies* 15, no. 2 (2022): 455, https://doi.org/10.3390/en15020455.
56. "Suspect in Military Documents Leak Appears in Court as U.S. Reveals Case Against Him," PBS News, 14 April 2023.
57. Reuben Johnson, "China Just Announced Its Plan to Beat the U.S. Military by 2049," *National Security Journal*, 11 August 2025.
58. Johnson, "China Just Announced Its Plan to Beat the U.S. Military by 2049."

Bradley Martin

How Drones Fight: How Small Drones Are Revolutionizing Warfare. By Lars Celander. Havertown, PA: Casemate Publishers, 2024. Pp. 208. $24.95 (paperback); $14.95 (ebook).

Cyber Wargaming: Research and Education for Security in a Dangerous Digital World. Edited by Frank L. Smith III, Nina A. Kollars, and Benjamin H. Schecter. Washington, DC: Georgetown University Press, 2023. Pp. 240. $164.95 (hardcover); $54.95 (paperback and ebook).

Author Lars Celander and editors Frank L. Smith III, Nina A. Kollars, and Benjamin H. Schecter compiled two distinct works that both consider the impact of emerging disruptive technologies on battlefields and national security. Both books provide valuable content in a condensed form. However, the book and edited volume take fundamentally different approaches. Lars Celander describes his book as "only about how things actually work, offering no recommendations on policy, acquisition, training, or organizational matters. Suitable conclusions are left to the reader" (p. ix). Celander is a former Swedish military systems engineer with a master of science in physics. In contrast, *Cyber Wargaming* comprises contributors and editors from multiple backgrounds and recognized experts, "whereas many cyber experts do not interact with wargamers, this book brings together innovative voices from across professional military education, civilian agencies, private industry, think tanks, and academia" (p. 3). Editors Frank L. Smith III, Nina A. Kollars, and Benjamin H. Schecter all have current or previous affiliation with the U.S. Naval War College and are recognized experts in the cyber domain.

How Drones Fight is organized into three distinct parts. The first part pres-

Bradley Martin is an intelligence analyst within the U.S. Intelligence Community. His research interests include emerging technologies, structured analytic techniques, and the use of wargaming as an analytic tool. The views expressed in this review are solely those of the author. They do not necessarily reflect the opinions of the organizations for which they work, Marine Corps University, the U.S. Marine Corps, the Department of the Navy, or the U.S. government.

ents an overview of the engineering and technical knowledge associated with drones. The second part examines the current and historical applications of drones in warfare. In the third part, the discussion shifts to the future of drone technology in conflict. Additionally, the book features a preface, glossary, introduction, 16 chapters, three appendices, a bibliography, and an index to provide a comprehensive resource.

The chapters in the book follow a logical progression, beginning with concise technical information. They cover various topics, including types of drones, navigation methods, drone sensors, and communication systems. The second part delves into weapons, drone tactics, antidrone strategies, and combined arms operations. Chapter 7 stands out as a particularly impactful section, where Celander delves into countering drones through the concept of "soft kill" (p. 59). Despite its brevity, spanning only two and a half pages, this chapter effectively tackles essential topics such as disrupting navigation, interfering with communications, and eavesdropping.

In the final one-third of the book, the author effectively connects technical information from earlier chapters to modern situations. Chapter 12 covers the use of drones in the Global War on Terrorism in just seven pages. Chapters 13 and 14 focus on the 2020 Armenia-Azerbaijan conflict and the 2022 Russia-Ukraine conflict, respectively, and are the highlights of the book. Chapter 14 is the longest and features maps, images from both conflicts, insights into command-and-control dynamics, and evolving drone tactics. While the practical applications are a significant strength, the narrative could benefit from more examples. Overall, the content and writing style are accessible, but inconsistencies in chapter length and subheadings may frustrate readers. Some subheadings include only a few sentences, creating a disjointed reading experience.

The bibliography includes sources, but the book lacks traditional citations apart from a few photographs. Celander downplays the necessity of source listings, stating, "Much of what is said in this book is based on various engineering textbooks. They are not listed as sources here as they all say the same thing. Ultimately, everything is just physics" (p. 175). While some photographs mention citations, many diagrams do not have corresponding references. The absence of a thorough conclusion addressing the potential impact of drones on the future of warfare presents the most significant challenge for readers. In the concluding chapter, Celander remarks that "the book is reluctant to draw conclusions. It is not its purpose. The purpose is to provide the reader with an understanding of how drone warfare works; the reader is expected to draw his or her conclusions" (p. 153).

Cyber Wargaming is a unique book; it focuses on cyber wargaming, not on specifics of cyber warfare technical knowledge, "contrary to popular belief, cybersecurity is also about human decision making: not just hardware, software,

network, and data" (p. 2). The authors divide the book into thirds. The book begins with an introduction, followed by the first one-third of the book discussing research games, the second one-third on educational games, and a final conclusion. While *How Drones Fight* builds on each chapter, leading to a disappointing conclusion, *Cyber Wargaming* takes an independent chapter approach. Readers can navigate much easier between chapters and only read chapters they find of interest.

As *Cyber Wargaming* illustrates, wargaming is a technique used for both research and education in a wide variety of environments: "Fortunately, as a general-purpose tool, wargaming is interdisciplinary. When used correctly, cyber wargaming can bridge the gaps between social and technical knowledge in university classrooms, corporate boardrooms, and military headquarters" (p. 3). The editors note in the introduction that, while wargaming is expanding as a technique, most cyber wargames remain shrouded in mystery.

After the introduction, the book's first one-third concentrates on research games or analytical games. Chapter 2 on cyber wargames as synthetic data is an excellent supplement to the introductory chapter. While the introductory chapter explains why cyber wargaming is a valuable technique, chapter 2 provides more information on cyber wargames as a tool to generate data and provides examples of wargames with alternative approaches to generate research data. The chapter concludes by stating, "It is our hope that the library of cyber wargames and the new knowledge they can create will continue to grow" (p. 34). Chapter topics in the book's first one-third include cyber and nuclear crises, wargaming international and domestic crises, imperfect information games, cyber kill chains, and games within games and critical infrastructure.

The most innovative chapter in the book is chapter 5, which discusses the topic of imperfect information in games. Many wargames assume near-perfect information processing and retrieval, which is a flawed method, as the editors explain: "In this chapter, we argue that the role of information—specifically imperfect information and the means to degrade information—is foundational to any realistic wargame. Imperfect information has always been important to real life" (p. 67). Specifically, in a wargame, the authors used videoconferencing, voice chat, text messaging, and maps, and those capabilities could be degraded based on various cyber or kinetic actions.

The second one-third of *Cyber Wargaming* focuses on educational wargames. It covers topics such as creating enjoyable cybersecurity games, the Cyber 9/12 Strategy Challenge, the North American Electric Reliability Corporation Grid Security Exercise (GridEx), private sector cyber wargames, prototyping virtual cyber wargames, military doctrine, and using matrix games for strategic cyber and information warfare.[1] This section offers numerous examples of lessons learned from various cyber wargames. It includes several graphics de-

picting mock gameboards, cards, and capabilities. The standout chapters in this part are chapter 13, which discusses military doctrine and cyber gameplay and chapter 14, which explores matrix-style games for strategic cyber and information warfare. In chapter 13, Colonel Benjamin C. Leitzel from the U.S. Army War College designed a cyber wargame to help students grasp cyber concepts. He notes that "even for officers who are familiar with the domain, this type of game can encourage creative and critical thinking about the strengths and weaknesses of current doctrine—doctrine they may one day help to update and improve" (p. 188). Chapter 14 highlights the wargame *Pinnacle Protagonist*, a capstone project from the National Defense University. The authors developed an adjudication tool called the National Strategic Program (NSP) framework to enhance cyber wargaming. Based on commercial board game designs, the NSP incentivized players to think carefully about their cyber capabilities. It required players to prepare specific courses of action in advance and limited their resources during gameplay, creating an atmosphere of uncertainty and anonymity (p. 200).

The final concluding chapter of *Cyber Wargaming* discusses the insights gained by using cyber wargames to spur thinking about emerging technology and innovation: "wargames that explore emerging technologies have the potential to influence not only our understanding of these technologies but also their subsequent development and application" (p. 211). To put it directly, "wargaming emerging technologies can affect technological innovation" (p. 212). The chapter concludes with a call for more wargames: "reading a book about riding bicycles is one thing, but riding a bike yourself is a very different experience. More practice playing wargames is good, regardless of your experience and expertise. This is true now, and we suspect the same for wargaming in the future" (p. 213).

Both books contribute to readers' understanding of emerging technologies that will likely remain important to the national security community during future conflicts across the conflict continuum. In summary, Lars Celander's book, *How Drones Fight*, is an excellent practical, tactical overview of drones on the battlefield. Analysts and researchers looking for a deep treatise on drones or those familiar with the technical exploitation of drones will find the information too basic. Readers will likely appreciate the concise nature, making it an excellent desk reference for nonengineers or scientists. This book is recommend as an introductory guide for intelligence and military personnel new to working drones. *Cyber Wargaming* is a different and more scholarly anthology. It is an excellent guide for those interested in wargaming, building, and designing cyber wargames and for scholars researching cyber concepts. The content targets individuals interested in wargaming and is more of a niche advanced text.

Endnote

1. "Cyber 9/12 Strategy Challenge," Atlantic Council, accessed 18 November 2025; and "GridEx," North American Electric Reliability Corporation, accessed 18 November 2025.