SPECIAL COMPETITIVE STUDIES PROJECT

Defense Paper Series

Reimagining Military C2 in the Age of AI – Revolution, Regression, or Evolution

Lieutenant General (ret.) John (Jack) N.T. Shanahan
U.S. Air Force

This paper series includes discussion papers written by SCSP advisors to accompany our Defense Panel's 2024 Working Group Meetings. The views and opinions expressed in this newsletter are solely those of the authors and do not necessarily reflect the views or positions of SCSP.

Portions of this paper are adapted from Shanahan's forthcoming paper, Artificial Intelligence and Perception in Crisis and Conflict: Mating 21st Century Technologies with 18th Century Minds, to be published by the Strategic Multilayer Assessment (SMA) program and Air University Press.

Introduction

Command & Control the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.[1]

Historically, multi-domain C2, from the strategic to the tactical level, has been a significant competitive advantage for the U.S. military. Reimagining joint and combined C2 for the all-domain digital age first requires either accepting an existing definition or proposing a new one. For the purposes of this paper, I have chosen to accept the extant definition. However, even if the *definition* of C2 remains unchanged, the disruptive characteristics of AI, robotics and autonomous systems, and other emerging technologies – such as next-gen wireless, quantum computing, and advanced sensing – make it highly likely that how all-domain C2 is *executed* during planning and operations will need to undergo major, perhaps even transformational, changes in the future operational environment. I explore the outlines of these potential changes throughout the paper.

Extending the above doctrinal definition, AI-enhanced C2 should empower humans to make better, more informed decisions, providing decision advantage over adversaries even under the extraordinarily intense and chaotic conditions of high-end combat against a peer adversary. AI-enabled C2 encompasses weapon systems, networks, and the underlying IT architectures that connect sensors, systems, weapons, and personnel, all designed to enhance the orchestration of actions and synchronization of effects across time and space. It will assist commanders, analysts, and warfighters in processing vast amounts of data and unclassified and classified information from all domains and more sources than ever before, offering critical insights for planning, analysis, targeting, execution, and assessment. AI-enhanced C2 should guide, inform, and assess operations, creating shared awareness across all domains to support the achievement of mission, campaign, strategic, and grand strategic objectives.

Stating the obvious, AI-enhanced C2 *is only advantageous if the outcomes in peacetime, crisis, and conflict are significantly better than they would have been under the same circumstances, absent AI.*[2] In other words, the returns on investment must justify the time and money spent integrating AI across all-domain military operations. Investments in AI must also consider the opportunity costs of prioritizing AI over upgrading existing systems or fielding more traditional

[1] While the DoD's official definition of C2 has changed over the years, for the purposes of this paper I use the 2017 version of JP-1.

[2] While this statement may be self-intuitive, it is highly likely that the AI 'gold rush' currently underway will continue to generate pressure to use AI to solve undefined or ill-defined problems, instead of using AI only when a problem cannot be solved using traditional tools.

yet proven C2 technologies. While faster C2 speeds are often critical, in OODA Loop[3] terms, the goal should be for AI to improve tempo and increase agility while generating friction, disruption, and chaos within adversary C2 systems, networks, and decision-making processes – aiming for *relative and temporal*, if not *absolute and enduring*, OODA cycle advantage.

As with all other aspects of military operations, C2 is highly situation- and context-dependent. AI will be most effective when it helps humans gain a rich contextual understanding of a situation – enriching the observation and orientation phases of the OODA Loop – before decisions are made and actions are taken, or before a human approves autonomous systems and AI agents[4] to act on their behalf.

In future conflicts, particularly against peer competitors and when facing large numbers of robotics and autonomous systems on both sides, AI will be essential for enabling U.S. forces – and those of its allies and partners – to maintain their edge. Indeed, the theory of the case today is that U.S. forces will not succeed, especially in a conflict with China or Russia, *without* the widespread adoption of AI-enhanced systems across the joint and combined force. As the National Security Commission on AI cautioned in its 2021 final report, "In the coming decades, the United States will win against technically sophisticated adversaries *only if* it accelerates adoption of AI-enabled sensors and systems for command and control, weapons, and logistics [emphasis added]."

After setting the stage with a more detailed examination of the concept of AI-enhanced C2, I test the theory of the case by presenting three distinct scenarios that illustrate the range of possible outcomes in the future operational environment – revolution, regression, and evolution. I outline the most salient features of each scenario and later explain why one outcome is significantly more likely than the other two. Finally, I conclude with reflections on the enduring nature of C2 and the imperative to reimagine mission command in an AI-enabled future operational environment.

Framing

In his 2016 speech to NATO in Brussels, then-Deputy Secretary of Defense Bob Work placed C2 at the center of the Third Offset Strategy (TOS), a concept he introduced in 2014 with the goal of

[3] For a robust treatment of the OODA Loop as originally envisioned by John Boyd, especially the critical roles of both positive and negative effects of feed-forward and feedback loops throughout all the stages of the decision cycle, see Chuck Spinney, Evolutionary Epistemology: A Personal View of John Boyd's "Destruction and Creation"...and its Centrality to the...OODA Loop, https://www.youtube.com/watch?v=gdK4y6O-lIE. James Johnson provides an excellent, critical examination of the OODA Loop as it pertains to AI-enhanced command and control.

[4] As used in this paper, an AI agent refers to autonomous software that is designed to perceive its environment, process information, make decisions, and take actions to achieve specific goals without constant human intervention. They can operate independently, adapting behavior over time based on their experiences and the information they gather.

ensuring the U.S. military would achieve the same decisive advantages as those gained through the First and Second Offset Strategies. He highlighted the historical importance of three interconnected 'grids' that formed a battle network and contributed to England's victory in the Battle of Britain: a sensor grid, a C3I grid, and an effects grid.[5] The latter relied on an 'effects screen,' enabling the British to mass their fighters against German bombers at the right place and time. Work extended this Battle of Britain model to modern-day warfare, emphasizing how the same three types of grids should underpin the TOS. Moreover, he asserted that the "technological sauce of the Third Offset is going to be advances in Artificial Intelligence (AI) and autonomy." He further emphasized the critical role of humans in human-machine battle networks, stating that "AI and autonomy will be used only to empower humans, not make individual or independent decisions on the use of lethal force."

The authors of RAND's 2021 report, A History of the Third Offset, 2014-2018, observed that "AI could be used to augment critical warfighting systems, such as C2, surveillance and reconnaissance, and targeting systems, for speedier effects against an adversary." They noted that Work "argued that understanding the battlespace 'better than the adversary' also would allow for 'more rapid decision making and application of more discriminate effects faster.'" As Work regularly emphasized to those of us on the Algorithmic Warfare Cross-Functional Team (Project Maven), his vision was never for AI to be seen as an end in itself, but rather as a gateway to an 'intelligentized military' – one comprising much greater numbers of autonomous and smart autonomous weapon systems (the effects grid), supported by superior interconnected sensor and C3I grids whose capabilities would continue to improve exponentially over time.

While the terminology around JADC2 differs from what Deputy Secretary Work used when discussing the TOS and AI-enhanced human-machine battle networks, in essence CJADC2 – along with related Service programs[6] and other projects such as DARPA's Assault Breaker II, MOSAIC warfare, and STITCHES – is largely an extension of the Third Offset Strategy. The JADC2 Strategy "provides a vision and an approach for identifying, organizing and delivering improved Joint Force C2 capabilities, and accounts for adversaries who have closed many of the capability and methodology advantages we depend upon for operational success....[It is designed] to deliver information and decision advantage to Joint Force Commanders." The intent is for CJADC2 to enhance all-domain awareness, improve precision and lethality, enable greater battlespace decentralization, and accelerate sensor-to-decision maker, sensor-to-shooter, and sensor-to-effects timelines for policymakers and military leaders.

Similarly, the authors of the 2023 SCSP report, Offset-X: Closing the Deterrence Gap and Building the Future Joint Force, evaluated the changes necessary to optimize C2 for an AI-enhanced future. They concluded that "[t]he U.S. military, its allies, and partners need a new C2

[5] Work attributes in large part the success of this three-grid battle network to RAF Air Chief Marshal Hugh Dowding.
[6] Project Linchpin, Project Convergence, ABMS, and Project Overmatch.

design and architecture that will enable them to be far more tactically flexible, be interchangeable with allies, scale on demand, and adapt dynamically to changing conditions."[7] This redesigned C2 and architecture should facilitate "real-time, informed decisions; generate predictive and proactive insights about their adversaries, their own forces, and the environment; present the PLA with multiple dilemmas; be able to coordinate and command efforts globally; and generate and assess feasible and creative courses of action faster than adversaries."

C2 is most often associated with execution during military operations, but as the SCSP report notes, it is equally critical during the planning process. In fact, given rapid advancements in natural language processing and the growing proliferation of frontier models and generative AI (GenAI), in the near term AI is likely to achieve better and faster results in joint and Service planning than during operations. Such capabilities could improve and accelerate the development and dissemination of national guidance as well as strategic, operational, and tactical orders, enhancing C2 across all echelons.[8] Reinforced by game theory and the extensive use of advanced modeling and simulation, AI will likely expedite collaborative, real-time course of action (COA) development, comparison, and selection. In the medium term, AI could speed up the joint planning process, particularly by accelerating Time-Phased Force and Deployment Data (TPFDD) planning and execution, including continuous real-time updates to the TPFDD database and its interconnected C2 and information systems.[9]

For AI-enhanced C2 to reach its full potential, continuous horizontal and vertical information flows will be essential. Higher headquarters will need timely, constantly-updated campaign assessments to accelerate the development of plan branches and sequels and to issue new guidance to subordinate units.

Paraphrasing Amara's Law, we are likely overestimating AI's short-term impact on C2 while underestimating its long-term effects. The challenge, of course, lies in defining the duration of "short" and "long" terms. With a nod to Yogi Berra,[10] I am not certain whether a 10-year horizon in the digital age qualifies as short, long, or medium term (although I lean towards the latter). Nonetheless, I established 2035 as the outer boundary for the future operational environment and the three scenarios that follow.

---

[7] To make such an architecture function, the report calls for the following capabilities: resilient communications; a common all-domain operational picture (COP); course of action generation and analysis; greater network-based decision-making via distributed, network-based operations; and distributed and localized decision-making and resources. The associated technology solutions include adaptive communications systems; modular C2; human-machine collaboration enabled planning tools; mesh networks; software baselines or architectures to enable communications between systems and militaries; and micro-satellite constellations.

[8] In the form of OPLANs, CONPLANs, Air Tasking Orders, Operations Orders, Maritime OPORDs, PLANORDs, DEPORDs, EXORDs, WARNORDs, PTDOs, ALERTORDs, and so on. See for example https://www.onebrief.com/.

[9] See for example https://www.defconai.com/

[10] "The future ain't what it used to be."

Revolution

By 2035, the DoD's digital modernization is largely complete. Across the Department, data is treated as a strategic asset and data mesh architectures are pervasive. AI capabilities are integrated throughout the military, at all levels from the Pentagon to tactical units. Extensive and frequent experimentation, wargaming, modeling and simulation – to include widespread use of digital engineering – training events, and joint and combined field live-virtual-constructive (LVC) exercises have honed all-domain C2. For C4ISR, the U.S. military adopted many of the same crowd-sourcing techniques[11] that proved instrumental to the success of hyper-scaled commercial tech solutions in the 2020s. Commercial vendors embraced antifragile principles in their software and hardware offerings, which were optimized for operations in denied, degraded, intermittent, and limited bandwidth environments.

The transformative technology trinity comprising the interaction of uncrewed systems, digital command and control, and meshed civil and military sensors has been achieved, and algorithmic warfare has been institutionalized throughout the military.

The joint planning process accelerated dramatically over the decade, leading to real-time collaborative planning from the strategic to the tactical level. All planning and execution orders are drafted and shared in real-time based on updated permission lists, and are continuously synchronized to ensure all Service, joint, and combined units operate from the same planning guidance. GenAI and AI-enhanced modeling and simulation available on even the smallest fielded tactical devices allows rapid COA development, comparison, selection, and transmission to affected units. Game-theoretic competition combined with advanced AI models that use detailed information about an adversary's strategic, operational, and tactical objectives along with sophisticated network and nodal analysis supports the COA development process, allowing rapid excursion analyses for hundreds of potential COAs.

Operational- and tactical-level commanders and warfighters serve as 'effects brokers,'[12] selecting from and authorizing the execution of myriad options in multiple domains to achieve desired outcomes. AI is integrated throughout all CJADC2 systems, networks, information technology architectures, and weapon systems, resulting in dramatically accelerated sensor-to-decision maker and sensor-to-shooter timelines. Operational- and tactical-level joint and combined commanders gain an unprecedented awareness of the all-domain battlespace, allowing them to select from available air, ground, maritime, space, cyber/electromagnetic

[11] I attribute this phrase to retired Air Force Brigadier General Scott Stapp.
[12] I thank Air Force Major Matt Cook for suggesting this term.

spectrum operations (EMSO), and information operation options – either individually or in combination – to produce the desired effects and achieve mission and campaign objectives.

Battlespace results and changes to unit status to include logistics requirements and force availability are shared with higher headquarters, in accordance with theater and task force commander guidance, resulting in near-real-time adjustments to ongoing operations and generating constantly-updated options to create multiple dilemmas for adversaries.

Warfighters develop and regularly test creative operating concepts to reflect the ubiquity of AI and autonomous and robotics systems, seamlessly integrating remaining legacy hardware and software systems with newly-fielded AI-enhanced systems. These operating concepts are refined constantly, yielding OODA Loop decision advantage over adversaries.

Sequential combat is a relic of the past, replaced by parallel and simultaneous all-domain warfare that achieves the desired mission effects in time and space while generating maximum chaos, friction, and disorientation for the adversary. By 2030, the DoD had adopted the tenets of Mosaic warfare,[13] replacing network-centric and traditional maneuver warfare with a decision-centric approach to warfare "intended to enable faster and more effective decisions by U.S. commanders while also degrading the quality and speed of adversary decision-making." Mosaic warfare addresses the challenges of C2 in a military comprising large numbers of autonomous and intelligent systems.[14] It relies on a combination of *human command* and AI-enabled *machine control*, to include widespread use of multi-modal AI agents, for the "rapid composition and recomposition of a more disaggregated" military force. AI is used throughout the DoD to "empower decision support tools that enable commanders to manage rapid and complex operations," making "military units and platforms more numerous and recomposable."

GenAI and AI agents help accelerate and improve dynamic retasking and retargeting processes, linking tactical units with operational-level headquarters to ensure retasking and retargeting remain congruent with desired campaign and strategic objectives. In conflicts against peer adversaries, this type of agile C2, along with the mission command inherent in and enabled by Mosaic warfare, proves instrumental to success.

AI-powered 'battlespace assistants' prove to be enormously successful, especially at the tactical level, turbocharging capabilities provided previously by highly successful legacy devices such as Android Team Awareness Kit or ATAK. The widespread introduction of multi-modal AI agents

[13] See in particular Figures 1, 2, and 16 on pages viii, 5, and 39, respectively.

[14] Even with the kinds of advanced capabilities postulated here, I expect it will be extremely challenging to keep up with the pace of operations when tens of thousands of small drones, including FPV drones and swarms of AI-enabled drones, populate the battlespace.

and voice capabilities into these battlespace assistants allows fielded forces to shorten decision cycles considerably.

Military units have incorporated large language models with advanced voice capabilities for tactical-level battlespace C2, vastly improved from the early versions of ChatGPT's Advanced Voice Mode (AVM). Each digital assistant is tailored to its owner, the result of highly intuitive UI/UX and a process of continuous training and feedback between human and machine.

The proliferation of AI-enhanced robotics and autonomous systems has resulted in machines assuming from humans the most dangerous, dirty, and dull tasks. The Services endorse a framework for human decision-making through the lifecycle of autonomous and intelligent systems. The senior-level review process mandated by DoD Directive 3000.09, *Autonomy in Weapon Systems*, has been fine-tuned: policy officials and military leaders are comfortable with the C2 processes and procedures that permit autonomous systems in all domains to take actions based on human-defined parameters to include, in some cases, even the integration of AI agents. The risks of lethal autonomous weapon systems are mitigated through technical, policy, and procedural constraints. Along with GenAI and advanced neuro-symbolic techniques, these mitigation measures help warfighters adhere to the law of armed conflict/international humanitarian law, national and theater ROE, and local special instructions. Between DoD leaders specifying in detail when, where, and how humans are involved in the lifecycle of AI-enabled systems and the incorporation of responsible AI and 'ethics by design' principles in the development of AI capabilities, American policymakers and military officials have become more comfortable with the Department's C2 of AI-enhanced weapon systems, including lethal semi-autonomous and autonomous weapon systems (LAWS).

The ability to gain and maintain all-domain awareness through AI-enhanced, tailorable all-domain Title 50-Title 10 common intelligence and common operational pictures (CIP/COP) and self-healing, resilient low probability of detection (LPD) mesh networks has led to more decentralization than in any previous conflict, with mission command principles applied to an unprecedented degree. Even the smallest tactical teams and units maintain excellent situational awareness of the immediate and adjacent battlespace, with tight synchronization and alignment within and between military units.

Ongoing improvements to relatively crude augmented and virtual reality (AR/VR) capabilities fielded in the mid-2020s[15] resulted in the deployment of extremely capable AR/VR, MR, and XR[16]

[15] Such as the Integrated Visual Augmentation System or IVAS.
[16] Mixed reality (MR) is a hybrid of AR and VR that blends the physical and digital worlds. Extended reality (XR) encompasses AR, VR, and MR.

systems. These systems include intuitive, commercial gaming-like interfaces that allow rapid and highly effective all-domain C2.

The DoD-wide adoption of the Modular Open System Approach (MOSA), Open Mission Systems (OMS), and Universal Command and Control Interfaces (UCI) results in near-complete interoperability across the Services and with allies and partners; data is shared across C2 networks and weapon systems, based on rules and permissions set by humans and controlled by GenAI and AI agents. Service program offices dedicated sufficient resources to ensure that legacy systems were interoperable with leading-edge AI-enhanced systems. The DoD owns the majority of Application Programming Interfaces (API) to commercial software products, leading to the world's first "API-centric" war. Most APIs are designed for two-way flow: inbound APIs that allow for the control and execution of the system, and outbound ones that provide status capacity, usage statistics, and other crucial information that can be fed back into a C2 orchestration system for planning, dynamic targeting, resupply, and resource management.

The DoD embraces the concept of "field to learn," centered on the accelerated fielding of minimum viable products (MVP) and minimum viable capability release (MVCR), constant end-user involvement during design, development, and testing, and – in close collaboration with commercial vendors – rapid updates to fielded AI models through robust continuous integration/continuous deployment or delivery (CI/CD) processes and continuous ATO (c-ATO).

AI-enhanced cross-domain solutions (CDS) allow the rapid one- and two-way transmission of information at all classification levels, to include to and from special access programs. There is a 'bias toward release' for allies and partners.

All AI-enhanced C2 systems are protected against adversarial attacks through rigorous test and evaluation processes and extensive red-teaming.

Combining human psychological operations and cultural expertise with AI-enhanced information operations placed continuous pressure on adversaries, generating friction and disorientation. The creative use of social media platforms, cyber-attacks, EMSO, traditional psyops materials, data poisoning, and denial and deception attacks against fielded AI models promised new pathways to collapse adversary C2 at all levels.

While the United States' allies and partners are not always able to match the DoD's pace of AI development, new policies allow co-innovation to flourish while data and models are shared rapidly with and by partners, with GenAI and multi-modal agents used to ensure adherence to foreign disclosure rules in near-real-time. Allies and partners participate in the development of new operating concepts during experiments, exercises, and wargames. During military operations, AI enhances C2 interoperability between U.S. military units and those of its allies and partners.

In summary, by 2035 the DoD's digital transformation produced an entirely new decision-centric approach to C2 in the all-domain battlespace. This deep-rooted transformation was only made possible by the wholesale commitment by a series of Department senior leaders, the unbending bipartisan support of Congress, deep collaboration between the DoD, industry, and academia, greater risk acceptance at all levels, and the creativity displayed by a new generation of highly empowered digitally-savvy warfighters committed to out-innovating the adversary. China is deterred from invading Taiwan or directly confronting U.S. military forces anywhere within the First and Second Island Chains.

Regression

The simplistic approach to this section would be to argue that everything that succeeded in the Revolution scenario, failed here. While this perspective is logical, I instead focus on the most significant C2-related breakdowns that collectively resulted in the spectacular failure of the DoD's intended digital transformation. By 2035, the lethargic and lumbering DoD behemoth had regressed from its already-tentative position in 2024 – and is now outgunned, out-C2'd, out-innovated, and outperformed by China.

Over the course of the decade, the following missteps combined to set back the DoD's digital transformation by years:

- lack of urgency from and inconsistent support by a rotating series of OSD and Service senior leaders;
- Service parochialism;
- anemic funding for AI and lack of confidence in, if not outright skepticism about, AI's performance;
- excessive delays in funding critical modernization projects, exacerbated by partisan politics in Congress and Continuing Resolutions year after year;
- lack of enforcement of the DoD data strategy, with data viewed as an afterthought rather than a strategic asset;
- continued atrophy of the Defense Industrial Base's manufacturing capabilities;
- an excessive focus on buying individual leading technologies while neglecting to fund the Department's less alluring yet more important underlying digital modernization requirements;
- failure to hold PEOs responsible and accountable for embracing digital modernization in every new weapon system; and,

- renewed wariness by and lack of incentives for commercial technology companies and academic institutions to work with the U.S. military.

Moreover, encouraging rhetoric by OSD and Service senior leaders about enforcing MOSA/OMS/UCI and mandatory interoperability metrics was belied by the facts on the ground in individual Service program offices. Too many C2 systems throughout the JADC2 family of Service projects relied on proprietary components, left data rights and intellectual property protections unresolved, and were not interoperable without undergoing massive overhauls that would have disrupted ongoing global operations and cost billions of dollars.

Likewise, for myriad reasons and with few exceptions, the DoD's AI projects failed to scale during this decade.

The lack of interoperability – to include incompatible encryption capabilities – across Services or with allies and partners, when combined with data that could not be shared across C2 networks and weapon systems, proved to be disastrous during conflict. The problems were aggravated further by two long-standing practices: over-reliance on bolting-on AI to legacy systems rather than baking it in during new system design and development, and limited interoperability between fielded legacy systems and leading-edge AI-enhanced systems.

Further compounding the problems, in the quest for ubiquitous automation and simplification, over time military personnel who lacked sufficient training began to place excessive and unwarranted confidence in autonomous and AI-enhanced systems. The insidious effects of this automation bias – the well-documented human propensity to favor outputs from machines over humans – along with over-reliance on generative AI whose results, however seemingly sophisticated on the surface, continued to prove highly fallible in military settings, proved to be disastrous in conflict. James Johnson's cautionary words from 2022 proved prophetic during war against China: "AI enabled capabilities cannot effectively, reliably, or safely complement – let alone replace – humans in understanding and apprehending the strategic environment to make predictions and judgments to inform and shape command-and-control (C2) decision-making…."[17] Over the intervening decade, unduly favoring the science side of the art-science equation governing warfare had calamitous consequences once the conflict with China began, and autonomous and AI-enabled systems began to fail.

Adding to the automation bias problem, 'competing' AI models that relied on different datasets at the tactical and operational levels generated contradictory guidance to users in the field and

[17] Also see Johnson's latest book on the same topic: *The AI Commander: Centaur Teaming, Command, and Ethical Dilemmas* (Oxford: Oxford University Press, 2024).

at headquarters, creating unexpected and often debilitating friction at the execution level – ceding decision advantage to the adversary.

The stated goals of maximum decentralization and greater reliance on the principles of mission command did not materialize. The unprecedented ability for everyone at all levels to see the same AI-enhanced CIP/COP led unexpectedly to dangerous over-centralization, as policy and military officials in Washington and at operational-level headquarters interfered regularly with ongoing operations. At the same time, the ability for personnel in tactical units to view the entire battlespace led to a false sense of confidence in their ability to understand broader operational and strategic campaign and national objectives. The push and pull between smothering over-centralization and excessive over-decentralization led to frequent bouts of C2 paralysis during the conflict with China.

Projecting James Johnson's words from 2022 into 2035 illustrates the novel challenges military forces faced in crisis and conflict: "Misunderstanding the human-machine relationship during fast-moving, dynamic, complex battlefield scenarios [undermined] the critical symbiosis between senior commanders and tactical units (or "mission command"), which [increased] the risk of mismatches accidents, and inadvertent escalation. *In extremis*, the rise of "tactical generals" (empowered with AI tools making tactical decisions from afar) and the concomitant atrophy of "strategic corporals" (junior officers exercising judgment, leadership, and restraint) [created] highly centralized and tight-coupled systems that [made] accidents more probable and less predictable."

In the rush to match the perceived – if not always actual – speed of the PLA's AI fielding, the DoD rushed the deployment of some AI technologies that in many cases were untested, unproven, and even unsafe. When combined with the lack of rigorous test and evaluation, fielded AI models did not perform as advertised and degraded rapidly. Battlespace C2 was vitiated significantly, compounded by intense electronic warfare, with few backups available for under- or non-performing AI-enabled C2.

In spite of multiple attempts over two decades to reform the DoD acquisition system, the combination of intrusive oversight; unpredictable budgets and a series of continuing resolutions; risk aversion; overly prescriptive and inflexible requirements during system design and development; and the Services' failure to take advantage of the flexibility allowed by the adaptive acquisition framework – especially the software acquisition pathway – made it impossible for the Defense Industrial Base and Defense Innovation Network to meet the demands of a protracted conflict with China.

U.S. military personnel began to rely on ensembled generative AI models that, while sounding convincing in their peacetime outputs, were developed with insufficient data – especially in the original mandarin – regarding China's military forces and its grand strategic, strategic, operational, and tactical objectives, and limited understanding of Chinese culture and leaders' decision-making processes. Over-reliance on immature models led to a series of poor decisions in the all-domain battlespace, further compounding problems with C2 at the tactical and operational levels.

AI models, once fielded, were not updated fast enough to account for model drift, changes in the operational environment, and the PLA's repeated denial, deception, and corruption attacks. The DoD failed to establish systematic CI/CD process, while the lack of standardized c-ATO processes excessively delayed updates to fielded models.

Insufficient cybersecurity resulted in unfettered adversary access to the military data used to train AI models. In too many cases, the Services allowed their data to be transferred to commercial vendor networks. Sophisticated attacks by China and Russia corrupted critical data, but the poisoning was not discovered until AI models failed after fielding. The absence of real-time sensors on fielded systems, and lack of training on dealing with reversion to legacy systems, generated widespread confusion and ineffective C2 as soon as most AI models began to fail or act erratically during conflict.

The DoD was unable to meet its planned timelines for fielding autonomous and AI-enhanced autonomous systems, largely because of risk aversion, widespread belief by policy officials that such systems would never work as planned, and an intense decade-long international anti-LAWS information operations campaign by Russia and China. The senior-level reviews required by DoDD 3000.09 were continually delayed or halted. Once the conflict with China began, the DoD was forced to place more people at risk and ceded battlespace advantage due to the PLA's extensive deployment of highly capable intelligentized autonomous maritime and air systems.

Due to overly restrictive policies, once conflict began commercial technology companies were unable to help warfighters at forward-deployed locations at the speed of operational relevance. Military personnel attempted to develop and sustain software via in-house platforms, but could not match the speed, expertise, and enormous investments of the leading-edge commercial technology companies, resulting in cascading failures of fielded software and continual degradation in all-domain C2.

The proliferation of 'off the books' commercial social media applications such as WhatsApp and Signal, which offered excellent encrypted real-time C2 capabilities at the tactical edge, led to a breakdown in all-domain C2. These apps, unrecognized as official DoD C2 systems, were used inconsistently, lacked integration with CJADC2 networks and platforms, and were not standardized. Their use also raised unresolved questions about accountability and responsibility.

The reward optimization function inherent in AI resulted in developing battlespace assistants that introduced significant cognitive risks, *reinforcing* instead of *countering* their users' biases and blind spots. These smart assistants became increasingly biased over time, even failing to present pieces of information about China's plans or actions that, if revealed, would have been critical to mission outcomes.

Military personnel did not consider or account for the consequences of cascading effects and emergent behavior in fielded AI models. Cascading effects stemmed from inherent AI model deficiencies and intentional adversarial attacks. Lacking sufficient human oversight or intervention, significant errors propagated throughout the DoD's networks and systems. When joined with the PLA's widespread use of sophisticated AI-informed information operations, EMSO, and cyber attacks – the DoD's three "exposed flanks"[18] – these undetected errors and ripple effects created destructive self-reinforcing, tightly-coupled feedback and feed-forward loops, adversely impacting C2 and decision-making processes at all levels.

Similarly, the widespread deployment of diverse, advanced AI models within some elements of the national security enterprise over the decade heightened the risks of emergent behavior. Ensembles of advanced AI models operating in dynamic, non-linear ways began to yield unpredictable and unexpected results, without sufficient transparency. By 2035, former Secretary of the Navy Richard Danzig's 2018 warning proved to be prescient: "the introduction of complex, opaque, novel, and interactive technologies will produce accidents, emergent effects, and sabotage."

By 2035, when conflict began, the cumulative effect was that the DoD faced the worst of both worlds: a purgatory in which it was neither fully digitally modernized and prepared for algorithmic warfare against China, nor capable of falling back to rely on fielded, proven legacy C2 systems. Consequently, in late 2035 the U.S. lost the Second Battle of the South China Sea, a previously-unimaginable result, while China began overt and unimpeded preparations to blockade and invade Taiwan.

Evolution

As tantalizing as it might be to imagine otherwise, there was no wormhole to transport the DoD instantly from its state in 2024 to the fully digitally-modernized outcome described in the first scenario. Nor was there any single event over the decade that yielded a revolutionary change to the character of warfare. Moreover, the most consequential decisions and actions during this period did not revolve around any single technology.

[18] A term I attribute to retired Army Lieutenant General Mike Nagata.

Instead, they resulted from the combination of the following human decisions:

- fully funding and closely overseeing implementation of the DoD Digital Modernization Strategy;
- implementing and enforcing the DoD Data Strategy;
- placing senior and mid-level officers and civilian executives in OSD, the Services, and Combatant Commands who were committed to accepting more risk, accelerating acquisition and budget reform, and embracing the tenets of software-defined warfare;
- bipartisan support from Congress for digital modernization, acquisition and budget reform, adoption of commercial software best practices, organizational adaptation, rapid experimentation, greater risk acceptance, and robust public-private partnerships between the DoD, the Defense Industrial Base and Defense Innovation Network, and academia;
- dedicated efforts to bolster the manufacturing capabilities of the defense industrial base;
- establishing a combined OSD-Joint Staff joint and combined futures organization (or command) dedicated to assimilating emerging and disruptive technologies and developing new joint and combined warfighting concepts;
- implementing and overseeing the recommendations of the CNAS Defense Technology Task Force final report and the Atlantic Council's Commission on Defense Innovation Adoption and Software-Defined Warfare Commission final reports;
- incentivizing Service program offices to follow digital engineering best practices and bake-in AI during system design and development;
- creative initiatives by the Services and Combatant Commands along with allies and partners to successfully integrate legacy hardware and software with leading-edge AI, next-gen wireless, and quantum capabilities;
- empowering warfighters through maximum decentralized and distributed C2 and mission command;
- initiating creative new personnel programs designed not only to offer career-long education and training on emerging technologies, but also to match Service and Combatant Command talent needs with talent skills from the National Guard, Reserves, and tech industry; and, most importantly,
- continuing a series of CJADC2-focused joint and combined experiments, wargames, and exercises designed to explore novel approaches to battlespace C2 and improve all-domain combat effectiveness. These progressed over time from small-scale single-Service events, through distributed large-scale joint and combined live-virtual-constructive (LVC) exercises and wargames.[19]

[19] Including events, such as Future Flag, that are not part of the official DoD series of exercises. Future Flag is an especially innovative all-Service field exercise held in upstate New York, with multi-domain C2 as an area of emphasis. https://www.afrl.af.mil/News/Article-Display/Article/3775961/afrl-future-flag-series-grows-in-scope-size-with-new-funding-alliances/

Despite a relatively slow start, in the mid-2020s DoD leaders directed accelerating the pace of these events. Initial projects included the OSD CDAO's Global Information Dominance Experiment (GIDE) and Task Force Lima; the Army's Project Linchpin and TITAN; Navy Forge; AF CCA; the Navy's Project Automatic Target Recognition using Machine Learning Operations (MLOps) for Maritime Operations (AMMO); CENTCOM's Task Force 59 and Task Force 99; the XVIII Airborne Corp's Project Maven; Replicator and Replicator 2; the Joint Fires Network (JFN); the U.S. Indo-PACOM Pacific Multi-Domain Training and Experimentation Capability Program Office (PMTEC); Maven Smart System; OSD R&E's Rapid Defense Experimentation Reserve (RDER) and Accelerate the Procurement and Fielding of Innovative Technologies (APFIT) programs; and the Small Business Investment Company Critical Technology (SBICCT) Initiative.

At the same time, OSD CDAO, the Joint Staff, and the Services committed to building the data backbone for JADC2, while OSD CDAO's Open Data and Applications Government-owned Interoperable Repositories or Open DAGIR Challenge began to put in place the enablers critical to successful DoD-wide implementation of CJADC2.

While some events were more successful than others, and some experiments even failed, the cumulative impact of these ongoing CJADC2-related efforts was significant. Progress was often halting, hindered by bureaucratic inertia and occasional active resistance within the Pentagon and partisan opposition in Congress. Nevertheless, these events proved invaluable for advancing C2 capabilities and refining doctrine. They enabled – and even encouraged – units to take greater risks, explore and refine concepts like Mosaic/decision-centric warfare, and find the optimal balance between centralized direction and decentralized execution throughout the all-domain battlespace.[20] Additionally, they facilitated the rapid and iterative fielding of AI and multi-modal generative AI capabilities, establishing agile processes to deploy, employ, and update software – including AI models – faster than adversaries, leading to consistent decision cycle advantage.

By 2035, the military's capabilities were still well short of revolutionary. However, the decade-long commitment to defense reform, coupled with the cumulative impact of dozens of JADC2 initiatives, led to significant improvements in C2 doctrine and the development and refinement of a more effective form of mission command. The PLA tested its forces in its first conflict in decades, but ultimately were defeated by the United States in the Second Battle of the South China Sea. Subsequent intelligence reporting indicated that this defeat deterred CCP leaders from attempting an invasion or blockade of Taiwan.

[20] In 2023, Andrey Liscovich, CEO of the Ukraine Defense Fund, noted the challenges of striking the right balance in the war with Russia. He stated that everything was decentralized in the hectic early days after Russia invaded, but over time Ukrainian military leaders acknowledged the need for a more centralized operational-level headquarters to C2 the disparate tactical activities throughout the battlespace.

Enablers

Most discussions about the future of an AI-enabled U.S. military gravitate towards theoretical outcomes that depend on a series of consecutive miracles unfolding in a short amount of time – which are exceedingly unlikely to occur in the DoD institutional bureaucracy. These putative success stories frequently fail to consider the critical importance of the underlying enabling functions, such as information technology architectures, networks, and elements of the AI stack. There are exceptions, most notably the National Security Commission on AI Final Report; the Atlantic Council Software-Defined Warfare Commission and Commission on Defense Innovation Adoption; the CNAS Defense Technology Task Force Final Report; the DoD Digital Modernization Strategy; the DoD Data Strategy; the DoD Data, Analytics, and Artificial Intelligence Adoption Strategy; the National Academy of Sciences, Engineering, and Medicine (NASEM) report on Test and Evaluation Challenges in Artificial Intelligence-Enabled Systems for the Department of the Air Force; the DoD Responsible AI Strategy and Implementation Pathway; and the CSIS report Software-Defined Warfare: Architecting the DoD's Transition to the Digital Age.

All these reports share the same overarching theme; namely, that the DoD remains a hardware organization born and raised in the industrial age, when it needs to be retooled rapidly to convert to a software-centric organization in the digital age. Mosaic/decision-centric warfare, greater decentralization, improved mission command, and CJADC2 all depend on implementing the structural and systematic changes called for in these reports.

Military C2 is human-centric and tech-enabled. Neither humans nor machines are perfect. Valid concerns about the risks of automation bias in the AI-enabled battlespace of the future must be balanced by the indisputable evidence of human biases throughout military history. Biases that are manifested in the form of disregarding or dismissing the contributions of machines in favor of human judgment, heuristics, or gut instinct. We should never underestimate the risks and consequences of human fallibility, fear, ego, and hubris on the physical battlefield or in the virtual battlespace.

For this reason, getting the best out of human and machine means that future C2-related initiatives must place renewed emphasis on user-centered User Interface/User Experience (UI/UX). Optimizing the integration of humans and AI-enhanced machines, which in turn depends on redesigning the interfaces between humans and machines and recalibrating human and machine roles and responsibilities, will be one of the most important and defining features of future military and intelligence operations in the digital age. As described in the 2024 SCSP-RUSI report, Leveraging Human-Machine Teaming,"…advances in human-machine teaming will be crucial to delivering effective offsets to adversary advantages."

The DoD will have to change how systems are designed and developed, how humans are trained to work with 'smart' machines that are unlike any previous military systems, and how AI-enhanced systems adapt to human interaction and intervention. The future environment will be characterized by AI-enhanced systems whose maximum benefits can only be achieved through superior human-machine collaboration (HMC) and human-machine combat teaming (HMT).

In an AI-enabled digital future, military users will have to train smart assistants in such a way that systems adapt to an individual's preferences, the pace of their cognitive development, and even their past behaviors. As technology continues to advance rapidly, the concept of highly-tailored human-machine interaction and interdependence is an achievable goal. Humans and AI-enhanced machines need to establish a long-term "partnership," established through career-long education and training, and repeated use under operational conditions, such that human operators gain sufficiently high confidence in a system's outputs before using it for the first time in crisis or conflict. The implications for all-domain C2 will be enormous.

Conclusion

For the past 35 years, the DoD's ability to C2 its own forces, as well as those of its allies and partners, has been its 'secret sauce.' We must reject any assertion or even implication that this key competitive advantage is immutable. It is fragile and perishable. As states – and even non-state actors – gain equal access to emerging and disruptive technologies like AI, competitive advantage and overmatch in future crises and conflicts will derive less from the technology itself than on four critical factors: the ability to "out C2" the adversary; the ability to deploy, employ, and update software and AI models faster than the adversary; the proliferation of intelligent all-domain robotics and autonomous systems; and highly effective and adaptive human-machine teaming.

History demonstrates that no single technology, no matter how impressive, is by itself ever truly transformative in war. Rather, what matters most is how disruptive technologies diffuse across societies and militaries, stimulate innovative operational concepts, integrate with legacy systems, and drive organizational reform and adaptation. AI, despite its unique and likely long-term transformational potential, is no different. For the DoD, there will be more continuity than discontinuity. There will be individual advancements along the way that change military C2 in substantive ways. However, the likelihood of discovering in any given ten-year period a single revolutionary "Black Swan" AI capability that revolutionizes C2 remains low – no *deus ex machina* will rescue the DoD.

For these reasons, the third scenario is the one most likely to unfold by 2035. We should not dismiss the likelihood of the other two scenarios. Based on historical precedent, however, "evolution" is the most probable path. Even this outcome, however, relies on a consecutive series of proactive, even visionary decisions by military leaders and policy officials over the next decade.

It is easy to overstate the speed at which AI-enhanced capabilities will be adopted by the U.S. military, let alone other militaries worldwide. I expect that the adoption rate will be slower and more gradual than expected.[21] This slower pace will be essential for enabling military personnel to adapt effectively. The mantra should be "tactical urgency, strategic patience." For the next several years, we will predominantly see narrow AI – single-use, specialized applications –with broader and more complex capabilities not becoming widespread for some time. Throughout this period, a thorough and ongoing analysis of worst-case outcomes, such as the Regression scenario, will be invaluable in identifying specific actions that humans can take during system design, development, fielding, and sustainment to alter those anticipated outcomes.

The most successful militaries will be those that, *ceteris paribus*, optimize the roles, responsibilities, and interdependencies between humans and smart machines – maximizing the benefits of emerging technologies without becoming subordinate to them. Future warfighters will learn to be as creative in the use of AI-enhanced systems to improve C2 as their predecessors have been with past technologies. While this creativity may likely take a different form than it did in the past, it will be creative nonetheless – likely sparking a rebirth of operational art. Indeed, in 2035, the proverbial military genius who uses AI effectively is likely to defeat the proverbial military genius who does not.

The author of Mission (Command) Complete: Implications of JADC2 questions whether the widespread introduction of AI/ML across the DoD means that "the potential loss of relevance for mission command as a C2 paradigm for the future of combat must be assessed."[22] He also cautions that the "largest implication for implementing JADC2 is the decreased reliance on intermediary command nodes." He offers an excellent argument, but I take a different stance: mission command remains relevant as ever, but how it is executed must evolve in the digital future. On the other hand, I agree with the authors of The Trouble with Mission Command, who observe that "[w]e need a command philosophy that acknowledges the historical constraints of warfare but also leaves room to exploit the emerging capabilities of modern technology." They also ask the essential question: "Given the tactical, operational, and strategic context, how should I command?"[23]

[21] For example, the National Security Commission on AI final report called for the DoD and IC to be "AI Ready by 2025." Neither the DoD nor the IC will meet that mandate.

[22] The author notes that "the degree of efficacy of that mission command could achieve was contingent on seven principles": competence, mutual trust, shared understanding, commander's intent, mission orders, disciplined initiative, and risk acceptance.

[23] The authors propose the concept of *flexive command* as "a more appropriate way to think about command and control."

We must be cautious in assuming that the remarkable capabilities anticipated with AI will automatically lead to unprecedented all-domain situational awareness at the tactical or even operational level – especially when facing an equally adaptive adversary committed to AI-enhanced disruption, denial, and deception. We should also not assume that maximum decentralization is the sole solution. Tactical effects can – and often will – have operational and even strategic consequences, particularly in the era of algorithmic warfare and the ubiquitous use of smart autonomous systems by all sides. As human intervention decreases during certain stages of employing these systems, especially with LAWS, the need for responsive, omni-directional C2 between tactical units, operational headquarters, and even Washington D.C. becomes increasingly critical.

Throughout this paper I described steps needed to accelerate the DoD's digital modernization. I highlight five that are required to enhance AI-enhanced C2, all underpinned by a culture of senior leader support, agility, empowerment, and risk acceptance:

- increased, accelerated, stable, and flexible funding for AI and DoD-wide digital modernization;
- rapid acquisition of commercial C2-related software/hardware;
- embracing field to learn principles;
- enforcing MOSA/OMS/UCI and interoperability across the Services and with allies and partners; and,
- repurposing existing – and increasing the number of – warfighter-focused experiments, wargames, exercises, and modeling and simulation to evaluate C2 tools and develop new C2 concepts such as Mosaic warfare, and to find the appropriate balance between centralized direction and decentralized, distributed execution.

As we accelerate into the AI era, senior policymakers and military leaders will need to confront the implications of a boundaryless all-domain C2 environment where information propagates instantaneously – often without human intervention – and individual tactical units, even when disconnected from higher headquarters, can generate global effects. At the tactical level, junior warfighters will be instrumental in shaping C2's future by pioneering and refining innovative concepts that balance human command with AI-driven machine control.

Paradoxically, human agency will become even more critical in the age of AI-enhanced C2 and a more autonomous, intelligentized military force. The critical challenge lies not merely in defining the future *role* of human input, but in determining *where* and *how* it is most effectively applied compared to current practice. This evolving landscape demands a reimagining of traditional C2 structures, emphasizing flexibility, empowerment, resilience, and rapid adaptation. As AI capabilities continue to advance, military leaders must foster a culture of continuous learning and innovation, ensuring that human judgment remains at the core of decision-making while leveraging AI's enormous potential to enhance operational effectiveness and responsiveness across all domains. The future of all-domain C2 will not depend solely on human-machine Centaurs, but instead on adaptive, context- and situation-dependent combinations of human-only, machine-only, and integrated human-machine teams.