Paper
06

# The Elusive Promise of Digital Acquisition for Combat Capabilities

**Dr. Ted Harshberger**
*Senior Associate (Non-Resident), Defense-Industrial Initiatives Group,*
*Center for Strategic and International Studies, United States*

**Dr. Cynthia R. Cook**
*Director, Defense-Industrial Initiatives Group,*
*Center for Strategic and International Studies, United States*

## ABSTRACT

Military decision-makers should reexamine their assumptions on the role of digital capabilities and artificial intelligence (AI) in future combat systems. The widely held view that future conflicts will be dominated by information technology, while correct in essence, under-emphasizes the enduring importance of more prosaic military technologies. For AI in particular, decision-makers would be well-served to approach the complex terrain of technology adoption with greater skepticism, recognizing that the complexity of military integration and test processes will place meaningful (and appropriate) limits on the transformative potential of AI for combat systems. A multi-faceted approach is appropriate, one that considers the distinct requirements of combat systems while recognizing the potential benefits of advanced digital tools for other aspects of military operations. Military leaders can and should aggressively leverage the startup and venture-funded sector for end-to-end information system capabilities, including the use of non-standard acquisition approaches. However, attempts to "force fit" the commercial ecosystem into the development of advanced combat capabilities are likely to lead to continued frustration and failure.

## INTRODUCTION

For the past several decades, the capabilities of digital systems have benefited from relentless progress in computational power and storage capacity, accompanied by order-of-magnitude improvements in the size, weight, and power storage capacity. The results have been stunning for both commercial and industrial customers – enormously powerful digital devices are now in the hands of ordinary consumers around the world, and military aircraft and spacecraft systems have simultaneously grown lighter, cheaper, and more powerful, able to connect to, contribute to, and take advantage of significant sources of data. In a meaningful way, digital capabilities – computing, digital processing, and the ability to access, fuse, and present information – are the critical characteristics of modern combat systems.

More recently, data scientists and programmers have used these hardware advances to create impressive breakthroughs in artificial intelligence (AI) – a suite of techniques that support natural language processing, inference, and generative behaviors, and evolving, learning signal and image recognition, among others. These tools require not merely systems with advanced processing capabilities but also access to the data and information that underpin them – a requirement that is becoming better understood with the advent –and limitations of – online tools like Chat.gpt and Google Bard. The military potential of these capabilities seems clear, and the US Department of Defense (DoD) has embraced them as a source of improved performance and, perhaps, competitive advantage (Lipton, 2023). But, the pursuit has led to significant frustration, primarily with the pace of adoption of new approaches and the ability to advance systems beyond the demonstration phase to the field. This paper discusses this challenge and provides, perhaps, a different perspective on the acquisition of digital capabilities.

## A COMMON VIEW AND AN ALTERNATIVE PERSPECTIVE

As militaries have looked with envy at the rapid spread of commercially available digital technologies, a common perspective has emerged based on a set of assumptions with varying degrees of truth. It's worth reexamining some of these "digital truisms" in light of recent experience. They may be leading modernizing militaries down an acquisition pathway that will continue to be frustrating. We can characterize (or perhaps a better word is "caricature") this common view in a simple way. The argument goes thus:

> *The future battlefield will be dominated by information, not kinetics, and AI technologies will bring new and fundamentally different capabilities to combat military systems.*

> *Militaries have been too slow at inserting digital technologies into operating systems, and as a result, they will lag behind potential opponents, particularly "pacing threats." The solution to this challenge is to lean heavily on the commercial tech sector, particularly the defense-focused startup and venture-funded ecosystem, and since these firms are not structured or incentivized to work with the typical acquisition process, defense organizations need to pursue non-standard acquisition approaches.*

Let's unpack and examine the different elements of this view.

## Truism #1: The future battlespace will be dominated by information, not kinetic effects, and AI technologies will bring new and fundamentally different capabilities to combat military systems.

Well, sort of....

It is true that military capabilities are useless without information, and those who can best apply modern digital technologies are likely to have a meaningful advantage in future conflicts. For example, R&D programs like the Joint All-Domain Command and Control System (JADC2) aim to connect the sensors and the shooters to allow for rapid kinetic effects. Future combat system concepts in Europe and elsewhere envision similar systems of systems architectures for sixth-generation air forces, albeit on smaller scales. It is also true that commercially developed, information-heavy technologies like commercial satellite communications and small drones have played a role in the recent conflicts such as Ukraine.

But as the conflict in Ukraine dragged on, the biggest lesson is a sad echo of every past war: defeating and displacing surface combat forces is an extraordinarily difficult and violent endeavor. Recent conflicts demonstrate the persevering relevance of trench warfare and extensive mining, tactics developed over a century ago in World War I, and needs to counter these tactics. Lasting combat advantage on the battlefield (where it has existed) has not been created by cutting-edge commercial tech - it has been generated by effective, *highly destructive* military combat systems in large numbers (Insinna, 2022). The promise of advanced technology does not negate the lessons of millennia of warfare: it is a difficult and kinetic business.

Commercial information-heavy technologies *do* have the ability to reshape this calculus. Faster and lighter computing, storage, and electric power have lowered the size, weight, and cost of combat systems for any given level of capability, are enabling more complex and flexible control and feedback within and among these systems, and are easing the information burden for human decisionmakers in the loop (like pilots or spacecraft operators). New concepts *are* being enabled (for example, those

that rely on large numbers of coordinated systems to bring kinetic force together in new and different ways).[1] Nonetheless, reliably capable military combat systems will continue to depend on prosaic technologies (engines, structures, explosives) and, importantly, the systems integration of all needed technological components, including information technologies.

## The Role of AI

What role should AI and other advanced software capabilities play in this picture? With respect to AI for the military in general, it helps to be clear on the part of a large universe of AI capabilities we are discussing. There is a vested stake in the tech venture world to emphasize the world-changing aspects of digital software technologies, both for society and for the military. This is a mixture of reality and hyperbole. A simple taxonomy is useful, and each of the applications below relies to a greater and lesser extent on the process of machine learning – using large databases to train machines to recognize patterns in data (Hinote, 2023).

- **Autonomy in Motion:** Applications in the physical world that act/react according to environmental conditions and mission needs (using on-board or real-time connected computing)
- **Autonomy at Rest:** Applying virtual systems to recognize patterns and take appropriate actions (drawing on large computing and data storage infrastructures)
- **Large Language Models:** Algorithms trained on very large amounts of human language text to generate the "most appropriate" language in response to a prompt
- **Generative AI:** Training algorithms to produce images, music, videos, etc., based on large amounts of similar content

There is a strong argument that these technologies have the potential to have profound and even disruptive impacts on many parts of society. In particular, large language models and generative AI are showing their potential for disruption in entertainment, education, and the workplace, and "autonomy at rest" capabilities are already enabling authoritarian government control of citizenry and even raising existential concerns tied to evolving non-human intelligence (Alison, 2019). Similarly, there is real, immediate value to be gained from the use of these techniques in many areas of military endeavor, including logistics, training and personnel systems, command and control capabilities, and intelligence, surveillance, and reconnaissance applications, to name just a few. Not surprisingly, these tasks within

1 For an example, see Deputy Secretary Kathleen Hick's comments (2023) on the new DoD Replicator initiative.

the military enterprise (inference and pattern recognition from large data sets, standard report generation, language recognition, and image generation) are most closely analogous to those we see being disrupted in civilian society.

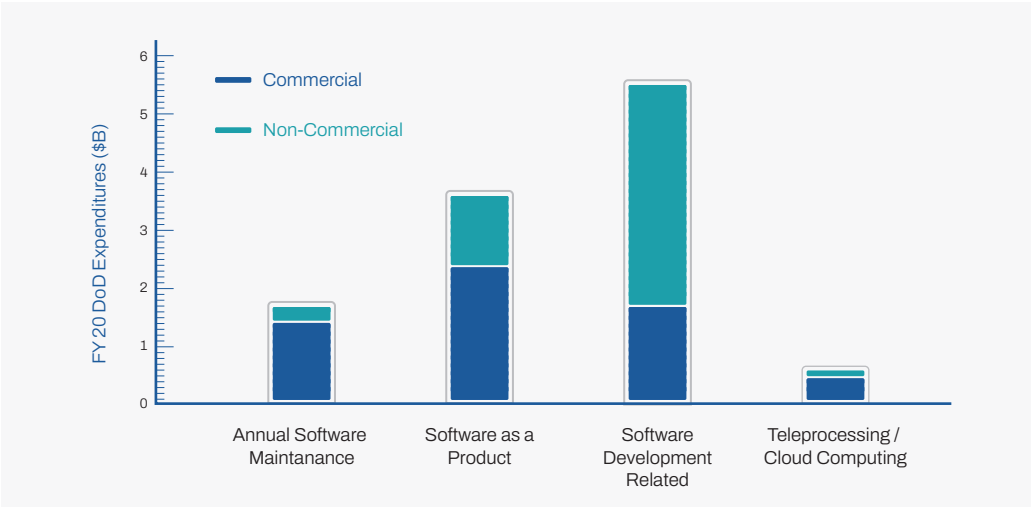


Figure 6.1: United States Department of Defense Software-Related Expenditures in 2020 (Source: United States Federal Procurement Data System)

These parts of the defense ecosystem have long been the province of commercial information technology firms. *Figure 6.1* is drawn from the Federal Procurement Data System (FDPS) and shows DoD FY2020 software-related expenditures by the class of activity and the type of contractual relationship. The data demonstrate that the bulk of United States DoD expenditures are commercially based (and, not surprisingly, under fixed-price terms). However, larger, established firms and small businesses focused on lower-end IT support make up the bulk of this spending to date. The startup and venture economy has poured enormous resources into new, relevant capabilities, and the near-term opportunities for the military are clear, most obviously in the "Software Development Related" expenditures, where more typical contracting has, at least until very recently, predominated

But what of combat military systems? There is certainly something to be gained from "autonomy at rest" (for example, training combat systems to recognize and respond to threats). Still, it's worth noting that much (not all) of what might now be called "autonomy in motion" used to be called "decision logic supported by statistics." Many digital information elements of this sort were applied (and even pioneered) in military combat systems long ago. Moreover, military combat systems arguably *shouldn't* involve much (if any) emergent or generative AI behavior. Aside from ethical concerns associated with truly autonomous, evolving combat systems (which some would argue will be set aside by adversaries)

and concerns with the ability to spoof or game these capabilities, the utility of any system in combat, crewed or uncrewed, will rely in no small part on their predictable coordination with other combat elements) (Janelle, 2019).[2] They operate within a broader ecosystem of military capabilities that, for the foreseeable future, will include humans. And happily, some of the digitally driven behaviors that have the most "cool factor" for military combat systems (for example, coordinated drones and crewed/uncrewed teaming) are the most straightforward to implement using traditional software techniques (and are *not – should not be* – "artificial intelligence").

## Truism #2: Militaries are too slow at inserting digital technologies into systems, and as a result, will lag potential opponents in the future.

Well, sort of...

It is an article of faith among many observers that some military powers are advancing proportionately more rapidly in their mastery of digital technologies than others (ASPI, n.d.). Others take a more sanguine view, arguing that measures of impact and employment lessen any perceived advantage those more adaptive militaries may be accruing (Schmid, 2023). What does seem clear is that major military powers view digital technologies as critically important to future force development and possess thriving (albeit different) innovation ecosystems to drive advances in these fields. The strategic competition in this arena is likely to be long-term and fierce and, if history is any judge, largely inconclusive in terms of clear winners and losers.

So, generally, are militaries moving fast enough in terms of implementation? Probably not, especially as military leaders stare enviously at their civilian counterparts. But the solution isn't likely to be driven solely by faster tech development. Pacing factors for the military application of any technology include a much broader suite of integration processes, including operational test and evaluation under realistic conditions. Advance and upgrade/modernization for these systems *can* be accelerated through Modular Open Systems Architecture (MOSA) approaches and thoughtful system design, particularly architectures that effectively segment the software components of the system, but adding AI techniques into the mix

*Pacing factors for the military application of any technology include a much broader suite of integration processes, including operational test and evaluation under realistic conditions.*

2 System operators and test and evaluation personnel view "emergent behavior" as a worrisome feature. However, what the Air Force seems to be seeking is predictable, yet flexible and complex, decision logic in its drone systems, not a truly intelligent autonomous system (Lipton, 2023).

adds a new layer of complexity (Sanders and Holderness, 2021). Many of the most powerful machine learning techniques have been developed in non-adversarial environments. It is disturbingly easy to undermine many of these algorithms, a worrisome feature in the civilian world, but a potentially devastating characteristic under military conditions (Janelle, 2019).[3]

The net result is that such systems will inevitably lag behind the cutting edge of commercial applications, where the stakes of failure are orders of magnitude lower. The IOT&E process is enormously frustrating to a "go-fast, fast-failure" mindset, but it is worth considering what "risk" and "failure" mean when developing combat capabilities. In the normal parlance of the acquisition and commercial business world, "risk" is tied to concepts like cost and schedule – risks worth taking if they generate meaningful capability on faster timelines. But the end result should never involve a meaningful chance that a weapon employed by combat personnel will not perform predictably – such "survival risk" is unacceptable. Development processes have generated meaningful advantage for militaries such as the U.S., when its systems have finally been employed under the stress of combat (witness the conflict in Ukraine, the opening days of Desert Storm, and many others).

## Truism #3: The solution to this challenge is to lean heavily on the commercial tech sector, particularly the defense-focused, startup, and venture-funded ecosystem, and since these firms are not structured or incentivized to work with typical acquisition process, defense organizations need to pursue non-standard acquisition approaches.

Accessing the venture ecosystem *does* come with real benefits for defense organizations (most notably, the chance to leverage private venture investments to advance capabilities and the ability to gain access to top-notch workforces).[4] There are also real risks inherent to the endeavor. In an era of low-interest rates and the rise of SPAC routes to monetization, many defense-oriented firms were initiated, and substantial capital flowed to them, but there is a boom-and-bust cycle to this part of our economy, and we are arguably entering a bust cycle (Jin, 2023). Defense organizations will need to be alert and agile as they engage with the sector.

We've already noted the many opportunities to leverage venture and startup capabilities (including AI capabilities) in the many parts of the defense enterprise (logistics, training, and personnel systems, command and control capabilities, and intelligence, surveillance, and reconnaissance applications,

3 "Officials estimate that it could take five to 10 years to develop a functioning A.I.-based system for air combat. Air Force commanders are pushing to accelerate the effort — but recognize that speed cannot be the only objective" (Lipton, 2019).

4 The United States Department of Defense has recognized these advantages with the formation of the Office of Strategic Capital.

etc.). However, the arguments above would suggest that defense should be turning selectively to this ecosystem when it comes to combat capabilities. The ability to package and produce hardware rapidly and at lower costs is clearly a strength, but if opportunities for applying cutting-edge commercial AI techniques are relatively limited and the timelines for development will remain relatively long, this part of the venture startup ecosystem appears relatively less attractive for combat systems. That may be one explanation for why the many ways that, for example, DoD has tried to accelerate these pursuits – Other Transactions Authorities, capabilities-as-a-service approaches, and FAR Part 12 commercial approaches, to name a few – have faced challenges in trying to transition emerging innovations into funded "programs of record." It isn't a great match.

## What's Actually Happening?

While each of these truisms contains some elements of truth, the real challenge for assessing their validity is that the defense ecosystem has not been postured to collect and assess data on these capabilities and investments. In particular, while the Federal Procurement Data System (FDPS) does grant visibility into business systems and other stand-alone software, it is largely silent on the wide range of embedded software within combat systems. For example, the F-35 has been termed a "flying computer," yet its tens of millions of lines of code are not traceable as investments in information technology in a way that separates those investments from hardware.

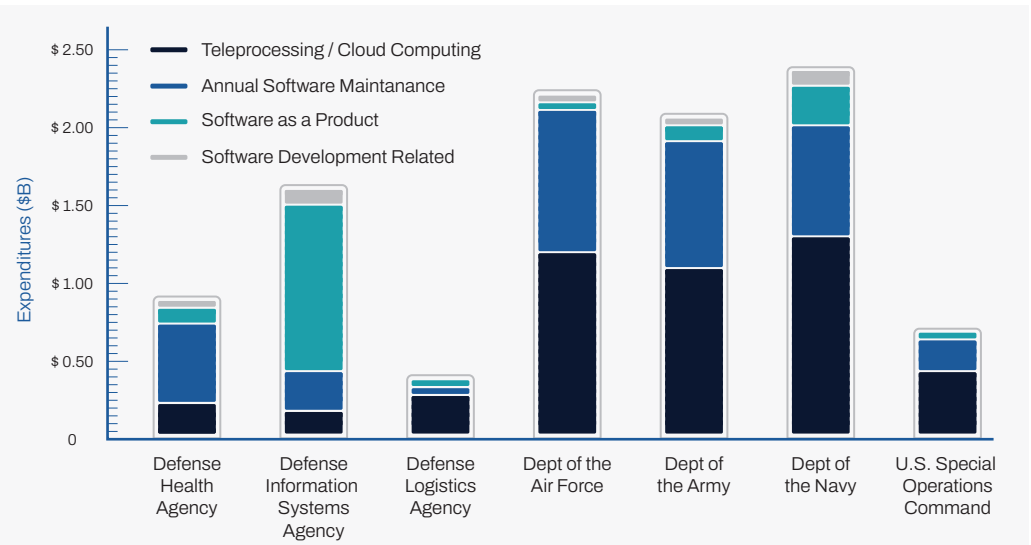


Figure 6.2: United States Department of Defense Software-Related Expenditures in 2020
(Source: United States Federal Procurement Data System)

*Figure 6.2* shows those data elements within the FDPS that were tied to software in FY2020, organized this time by the DoD component or agency that made the purchases and the broad activity these resources funded. While each of the military services (and USSOCOM) is clearly spending money on software, the amounts captured here are very modest (a total of roughly $10B) when compared to DoD's overall acquisition budgets. Combat systems-related software spending is clearly not captured here (or, holistically, anywhere). By inference, software-heavy hardware systems are managed using acquisition approaches designed for hardware, not software.

## IMPLICATIONS

This paper paints a different and intentionally provocative picture with several implications for decision-makers. First, approach this set of technologies with more nuance and skepticism than has been recently evident, especially within the popular press. AI and other cutting-edge digital technologies can play a role within military combat systems, but that role is likely to be more limited than commonly argued. Second, carefully segregate the approach to operationally oriented military *information* systems (e.g., logistics, command and control, etc.) from that of combat systems. For information systems, pursuing and deploying advanced digital techniques can and should proceed more aggressively. This could include buying end-to-end information capabilities from the venture and startup world using non-standard acquisition techniques (although these systems can also be pursued by more standard commercial approaches currently prevalent). Third, stop seeking end-to-end solutions from the startup world for complex military combat systems. Instead, consider these capabilities as more typical military subsystems that must be integrated *and tested* within a larger system to create military capabilities.

*AI and other cutting-edge digital technologies can play a role within military combat systems, but that role is likely to be more limited than commonly argued.*

- Consider carving out explicit elements of existing programs of record to attract and utilize non-standard companies.
- Lean on and incentivize prime contractors to develop explicit pathways and models for venture participation
- Measure and incentivize venture and startup participation (beyond typical small business set-asides) on prime combat system contract vehicles.

These may appear to be "business as usual" recommendations, and to a certain extent, they *are* – but that does not mean they are irrelevant. Many elements of the defense enterprise can and should

benefit from a faster, more flexible approach to using cutting-edge commercial digital technologies, but attempting to "force fit" these approaches to developing combat systems will likely lead to continued frustration and failure.

## REFERENCES

Allison, G., (2019) "Is China Beating America to AI Supremacy?" The National Interest, 22 Dec.
Available at: www.nationalinterest.org/feature/china-beating-america-ai-supremacy-106861.

ASPI, Critical Technology Tracker.
Available at: https://techtracker.aspi.org.au2

Hick, K., (2023) "Deputy Secretary of Defense Kathleen Hicks' Remarks: "Unpacking the Replicator Initiative." U.S. Department of Defense, 6 Sept.
Available at: www.defense.gov/News/Speeches/Speech/Article/3517213/deputy-secretary-of-defense-kathleen-hicks-remarks-unpacking-the-replicator-ini/. Accessed 8 Sept. 2023.

Insinna, V., (2022) "LaPlante Pokes Silicon Valley "Tech Bros," Calls for Increased Munitions Production for Ukraine." Breaking Defense, 8 Nov.
Available at: www.breakingdefense.com/2022/11/laplante-pokes-silicon-valley-tech-bros-calls-for-increased-munitions-production-for-ukraine/.

Janelle, S. (2019) Is That a Giraffe or a Cockroach?, Slate, November 5.
Available at: https://slate.com/technology/2019/11/image-recognition-systems-adversarial-attacks.html.

Jin, B., (2023) "Startups Are Dying, and Venture Investors Aren't Saving Them." Wall Street Journal, 11 Aug
Available at: www.wsj.com/articles/startups-are-dying-amid-drought-in-venture-funding-a9005ad2.

Lipton, E. (2023). A.I. Brings the Robot Wingman to Aerial Combat. The New York Times. [online] 27 Aug.
Available at: www.nytimes.com/2023/08/27/us/politics/ai-air-force.html.

Sanders, G., and Holderness, A. (2021) "Readiness for Open Systems: How Prepared Are the Pentagon and the Defense Industry to Coordinate?" www.csis.org, 15 Nov.
Available at: www.csis.org/analysis/readiness-open-systems-how-prepared-are-pentagon-and-defense-industry-coordinate.

Schmid, J. (2023) "Rethinking Who's Winning the US-China Tech Competition." Defense News, 15 Aug.
Available at: www.defensenews.com/opinion/2023/08/15/rethinking-whos-winning-the-us-china-tech-competition/.