Leveraging Commercial Best of Breed Companies to Increase Agility and Lethality For Integrated Deterrence in the Information Age

RESEARCH PAPER

Presented as part of the
Global Space & Defense Program
Price School of Public Policy
Viterbi School of Engineering
University Of Southern California
Los Angeles, CA

24 April 2022

Contents

Introduction

Does China really want to go to war with companies like Amazon and Google? China continues rapidly bolstering its military presence, through increased pace of building and launching counterspace capabilities, significant modernization of its navy and air forces, and proliferation of its presence in the South Pacific. These indicators boost Chinese Communist Party (CCP) confidence in defending the region and amplify the potential threats to Taiwan's sovereignty. Meanwhile, in line with the latest National Security Strategy, the United States is finally shifting its attention and resources away from the Middle East and toward the INDOPACOM area of responsibility. Now more than ever, the U.S. must consider novel elements of deterrence to minimize the risk of major conflict and ensure lasting peace.

To date, deterrence strategies have typically been kinetically focused and hardware-centric, designed for the later "end game" phases of war. Currently, U.S. intercontinental ballistic missile (ICBM) systems are in the middle of a much-needed, long-term upgrade and recapitalization. Additionally, the U.S. also has ongoing programs addressing long-range strategic bombing, ground-based theater defense, and other major investments in hypersonic and under-the-sea systems. These massive enduring programs are an important part of strategic deterrence, relying on the world's best industry partners to design and build the most complex hardware and software systems. When these programs are put out for bid, however, the same rotating handful of prime contractors typically respond, and unfortunately their value can be realized only in the latest stages of war when tensions are likely to escalate to "end game" consequences. These same prime contractors have also evolved to mirror the monolithic and bureaucratic mindset and culture of the Department of Defense (DoD).

When one examines the hardware-centric systems, they tend to suffer from the same old acquisition challenges. Congress incessantly demands faster, better, and cheaper development and delivery of capabilities to the warfighter, while the Pentagon cannot seem to get out of its own way in terms of process and bureaucracy. As these kinetic, late phase-of-war systems are some of the most complex creations the world has ever seen, major cost, schedule, and performance risks are essentially guaranteed during development. Meanwhile, the U.S. Defense Acquisition System (DAS) suffers from significant weaknesses when it comes to development of software and information systems—an area of expertise and policy that could use improved attention and resources. How then can deterrence with China be enhanced by both the acquisition of non-kinetic warfare capabilities to supplement ongoing development and making the best use of the considerably more opportunistic early phases of war?

Tremendous opportunity exists to utilize commercial best of breed information technology (IT) companies to support agile software development, quickly react to emerging threats, embed best practices in our operations, and consistently advise our leaders in the Pentagon and in the field. Companies big and small, such as Google, Amazon, Oracle, Cisco, IBM, GitLab, and many others represent the best and brightest minds in the world, having led prosperous innovations in the software and information technology sectors for decades. Yet, these companies have been largely under-utilized not only by the DoD, but in a deterrence strategy with China. Not that these profitable companies need incentives beyond a well-posed defense program that they might profit from, but the incentive for companies like these to be involved may ultimately be their survival. If the U.S. engages in a “kinetic” battle with China, there is no guarantee that things may not escalate to nuclear means. This unfortunate situation would threaten the very existence of mankind, which clearly includes these companies. If

deterrence means convincing adversaries that the U.S. possesses the muscle to make the cost of conflict too great, why not make commercial best of breed IT a significant and enduring part?

Therefore, this paper proposes a new framework that addresses the challenges with the following primary research question: can the U.S. leverage commercial best of breed IT companies to enhance agility and lethality in deterring China through the largely non-kinetic information domain? In addition, several secondary research questions also come to mind (See Figure 1.) The framework ideally aims to model the best elements of innovation efforts in recent years, address recent traditional acquisition challenges, propose how to fill persistent gaps in software and information domain acquisition processes, and consider lessons learned from past successful warfighter mobilization efforts—all with the goal of complementing and enhancing existing nuclear deterrence capability and strategy. Ultimately, if the DoD makes effective use of commercial best of breed companies, it is doubtful China will want to go to war with the likes of our best commercial IT companies.

- Primary research question:
  - **Can the U.S. craft a framework to leverage best of breed commercial IT partners to enhance agility and lethality in deterring China?**
- Secondary questions:
  - Can an acquisition model exist that leverages commercial best of breed to stay ahead of and quickly react to threats, embed in domestic operations, and constantly advise DoD leaders?
  - Are there other software acquisition tripwires to be avoided?
  - Are there corollary mass mobilization and rapid reaction hardware acquisitions that can be used to learn from and apply to software and information domain acquisition?
  - What can be learned from recent innovative organizations, constructs, and solutions that have failed or delivered less value than expected?

Figure 1. Primary and Secondary Research Questions

Literature Survey

China

"Better to see once than hear a hundred times." – Chinese folk proverb

The United States cannot afford to wait until China overtly attempts to reclaim Taiwan on the world stage, given that this would be a stark pivot point in U.S.-China relations and likely cause a major escalation in tensions that would negatively affect global markets. In many ways, the U.S. remains blind to China's rise to power, their intentions, and their assumptions. China aims to 1) return to being a great world power and 2) never again be humiliated by the West, and they will go to any length, including crafty use of misdirection and deception, to attain these goals. The U.S. continues to misjudge China's mindset, including the thinking that engaging with China equals cooperation, China is on the road to democracy, China is fragile, and China wants to be like us (Pillsbury, 2015). CCP nationalists often cite a set of lasting stratagems, including one held close by Mao Zedong during the Long March in the 1930s, which says, "there cannot be two suns in the sky," alluding to the strongly held Chinese belief that the nature of the world is hierarchy and there can only be one leader at the top.

Thus, Beijing seeks to realign international order in its favor by achieving a "great rejuvenation" no later than 2049, which include the People's Liberation Army (PLA) developing and advancing capabilities in space, counterspace, cyberspace, and nuclear forces (Military and Security Developments, 2021). China has effectively followed templates for three "strategies of displacement," the first two of which recognized the U.S. as a legitimate threat given the Gulf War and Soviet collapse and then emboldened China to be more confident economically after the 2008 global financial crisis. China plans to displace American order through its third strategy of displacement, which they believe already started with events like Brexit and the COVID-19

pandemic. China aims to see a unified Taiwan, U.S. forces withdrawn from Korea and Japan, the removal of the U.S. Navy from the Western Pacific, and resolution of territory disputes in their favor in the South China Seas (Doshi, 2021).

Additionally, the PLA will accelerate "informationization" and "intelligentization" of networked systems of systems by 2027 to help fight and win wars against a "strong enemy" like the U.S. Theories on "grand strategy" in China emphasize first the principle of situation, which includes time, space, and system—both internal and external interactions (Chunqiu, 2002). This emphasis on understanding the whole picture and potential interactions and outcomes directly supports an early phase of war, the information domain, and a systems-thinking mindset for the Chinese military—an area where the U.S. needs work. China further emphasizes this nuance noted by Sun Tzu who said, "the notes do not exceed five, but the changes of five notes can never fully be heard."

China ultimately intends to induce high levels of uncertainty given that the nature of warfare is changing rapidly and focus on safeguarding their interests in space and cyberspace (Cordesman, 2021). Advanced research & development (R&D) in new technology is on the rise in China, as they continue to make significant investment in the same technologies of interest to the DoD—their R&D spending has grown 10 times the rate of that of the United States over the past 20 years (Sargent, 2021). China's military buildup has been overt and significant, especially within space launch, on-orbit capabilities, and power projection at sea. China is clearly not the fragile flower they once were, as they strive for Indo-Pacific hegemony, and they are ready today to stand up to what they perceive to be the greatest threat to prosperity—the United States.

National Security Guidance

"During peace or in war, the Joint Force will deter nuclear and non-nuclear strategic

attacks and defend the homeland. To support these missions, the Joint Force must gain and maintain information superiority…"

– Jim Mattis, former Secretary of Defense (Summary of the NDS, 2018)

Secretary of Defense Lloyd Austin in a March 2021 message to the force has stated that the DoD will "prioritize China as the number one pacing challenge," as they constitute a long-term threat to the U.S. and its allies. Secretary of the U.S. Air Force Frank Kendall has recently stated at a major annual defense conference that the Air Force's three main priorities in order are "China, China, and China", adding that "there is not a moment to lose" (Tirpak, USAF's Three Priorities: China, China, and China, 2021). This direction from senior defense leaders falls in line with the latest National Security Strategy (NSS), which highlights that China is rapidly becoming more assertive and insists the U.S. will shift resources and investments from anachronistic legacy weapon systems to those that support this emerging priority (Interim National Secuirty Guidance, 2021). Furthermore, guidance recognizes that China seeks unfair advantages and regularly undermines "the rules," as the U.S. aspires to ensure that China does not set the international agenda. The NSS prior to this also focused on China and their theft of intellectual property and malicious cyber activities, recognizing that China's rise to power has been at the expense of the sovereignty of others (National Security Strategy, 2017). This strategy also admits that in its dealing with China, the U.S. typically narrow-mindedly views the world as either "at peace or at war," when it is really a continuous spectrum, especially according to China. The rebalance to Asia and the Pacific has been acknowledged for years as our strategy alluded closely to watching China's swift modernization (National Security Strategy, 2015).

The old term turned buzz phrase "anti-access and area denial" used to characterize Beijing's efforts to keep the U.S. military out of the western Pacific region has been

acknowledged by the DoD since the mid-2000s (National Defense Strategy, 2008). However, despite the long-known understanding that China is a growing security threat on paper, in practice, the U.S. has only just left Afghanistan late last year, finally signaling a shift and an alignment to this security guidance prioritizing INDOPACOM deterrence.

Integrated Deterrence

"*We affirm that a nuclear war cannot be won and must never be fought.*"

– Joint statement of the Leaders of the Five Nuclear-Weapon States on Preventing Nuclear War and Avoiding Arms Races (The White House, 2022)

The "War on Terror" consumed significant U.S. military leadership, attention, and intellectual bandwidth over the last two decades (Peters, 2018). Thus, the U.S. lacks experience integrating nuclear and non-nuclear planning, as potential adversary nuclear states show themselves to be prepared for deliberate and rapid escalation to the nuclear threshold, even during what the U.S. would formerly consider to be "early" in conflict. These well-documented adversary strategies have been dubbed "nuclear hybrid" strategies for which the U.S. largely does not have an answer.

In the worst-case scenario of escalating conflict in which long-range ICBMs are launched by an adversary nation at any allied nation, it is doubtful that one missile is shot and then one missile is defended, and the U.S. in turn reverts to less serious forms of kinetic or non-kinetic conflict. Such a scenario would almost certainly end up with many ICBMs being launched on both sides, causing innumerable casualties and potentially the end of nations involved, if not the end of the modern world. Mutual destruction between two nations is obviously an unacceptable end game, and therefore attention must be given to the earlier phases of war, to include our ability to defend and fight non-kinetically against great powers like China. This, in turn, means

the U.S. must focus more on the early phases of war and enhancement of non-kinetic capabilities, which will be referred to as the information domain (e.g., information, software, space, cyber, data, command, and control), to reinforce deterrence and supplement existing missile defense capabilities. It is considered a major factor adversely affecting the U.S. strategy that nuclear deterrence is largely absent from consideration as fighting grows more intense, becoming prominent only when necessary to deter nuclear employment by an adversary (Peters, 2018). This narrow view overlooks that adversaries may want to employ nuclear forces at earlier points in conflict and does not consider intra-conflict deterrence. It is quite probable in a major conflict that China and Russia would team up, further complicating warfighting decision science, as the U.S. knows that China and Russia "want to shape a world consistent with their authoritarian model" (Summary of the NDS, 2018). They both look to undermine international order by exploiting its benefits and undermining the rules. Thus, experts claim that the U.S. should make best use of peacetime by preparing to win the next war, while defeating any adversary aggression below the threshold of conflict (Cohen, 2021). But thanks to our inherently digital world, the word "peacetime" can be fuzzy.

The creation of the U.S. Space Force in late 2019 adds emphasis to early phase of war readiness, defense, and offense. "Phase Zero" is an area that will require continued and increased planning and wargaming to enhance awareness, assessment, and attribution within the digital battlefield (Johnson, 2015). Modern wargaming ideally also includes multi-domain operations (MDO), which has the potential to maximize complexity for an adversary. Big Tech can help understand complex adaptive systems (CAS). Recent studies show that applying a CAS lens to warfare is useful in understanding how a planner might create allied advantages, and they suggest that leaders be more fluent in CAS to support joint MDO concept of operations

development (Lingel, 2021). Highly informed scenario and mission planning is a proper goal, but it is one that depends on the information domain systems that are acquired and used.

A new term is taking shape, however, that incorporates all domains, instruments of national power, and phases of war: integrated deterrence (Garamone, 2021). This concept assumes that adversaries like China and Russia will not fight a protracted war with the U.S.; instead, they will act differently than previous conflicts where the U.S. has been involved. Also, this concept is fully tied to strategic nuclear deterrence. Integrated deterrence pulls the thread across phases of war to maximize resilience along the decision chain and best inform the potential use of U.S. "end game" capabilities at its disposal.

Defense Software Acquisition

"We don't have ships, planes and tanks anymore…we have computers that fly, computers that sail, and computers that drive." – Rogan Shimmin, Defense Innovation Unit (Shimmin, 2022)

The future is software-defined everything, as some call it. Starlink is showing this sort of capability currently in the Russia-Ukraine conflict and the DoD may have a lot to learn from it (Losey, 2022). Despite the DoD relying on taxpayer money to acquire new systems, which drives DAS bureaucracy and oversight, technology timescales continue to shrink, while acquisition process timescales remain the same—a problem that only gets worse with time (Johnson, 2016). Thus, the DoD needs increased agility in the way things are acquired to combat new threats. A recent RAND study notes that acquisition agility approaches are dependent on requirements, budgeting, technology, and intelligence activities, and they are unfortunately hard to apply universally, adding that focusing on speed alone could compromise cost or technical performance (Anton, 2020). Additionally, to ensure agility, the DoD must look beyond the traditional model of the warfighter having a problem and then going out to find a solution.

Instead, as suggested by the former head of Air Force Ventures, the DoD should take a platform approach to acquisition by incentivizing solutions to find problems, while problems also look for solutions, which is highly applicable to software in the information domain (Rathje, 2019).

The U.S. especially needs agility in how the DoD acquires software. Members of Congress are taking a hard look at a "software-centric" approach to acquisition in general (Williams, 2021). Hardware-centric approaches worked for a long time, but not anymore—the time has come to recognize that software is likely the core technology of top warfighter needs. Fortunately, as of late 2020, the DAS was updated to include a new software acquisition pathway, which is meant to "facilitate rapid and interactive delivery of software capability to the user" (DoDI 5000.87, 2021). It aims to enhance user engagement, existing enterprise services, and to support "tightly coupled mission-focused government-industry teams" (see Figure 2). This could serve as a basis for a working framework to leverage commercial sector partners to increase information domain lethality and agility.

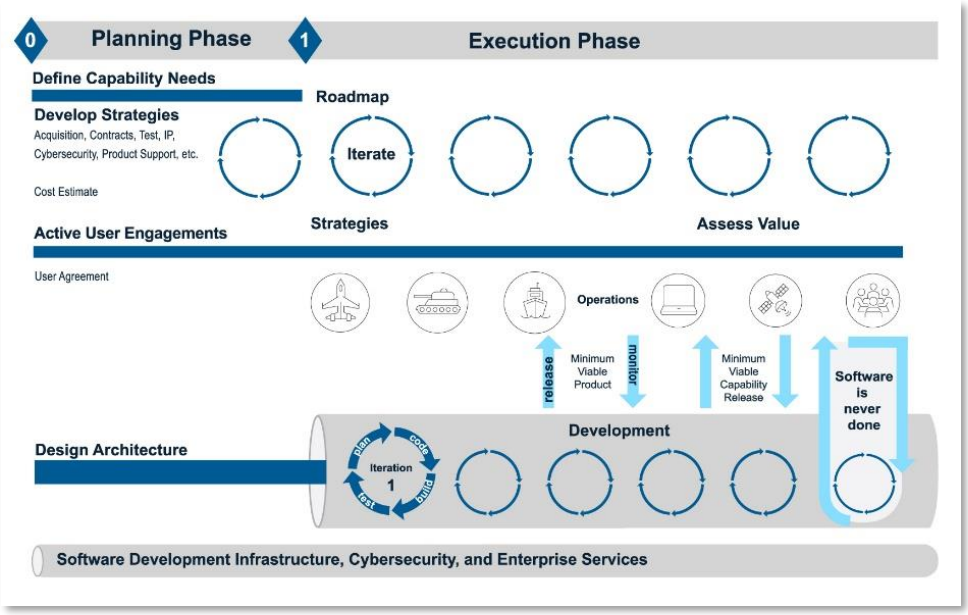


Figure 2 - New DoD Software Acquisition Pathway Lifecycle (DoDI 5000.87, 2021, p. 8)

A well-known publication in the software world mentioned a problem 36 years ago that persists today—that software acquisition often assumes "one can specify a satisfactory system in advance, get bids for its construction, have it built, and install it" (Brooks, 1986, p. 14). Even if this new acquisition pathway was implemented perfectly, the DoD must stop thinking of software and information acquisition as large time-boxed programs. It was principally this thinking that led to the canceling of the Joint Enterprise Defense Infrastructure (JEDI) cloud-computing contract, which was highly disputed since being awarded to Microsoft in 2019 (Nix, 2021). JEDI will be replaced with a three-year multiple awardee, indefinite order, indefinite quantity (IDIQ) contract called the Joint Warfighter Cloud Capability (JWCC)—while the new plan makes no mention of use of the new software acquisition pathway, it may enable additional capability and learning from the best of all the commercial IT giants and their partners by not putting all the proverbial eggs in one basket. Still, JWCC merely supports infrastructure, not modern warfighting in support of deterrence.

Looking back at Figure 2, "software is never done," and there is good reason for that. The concept of continuous integration and continuous delivery (CI/CD) ensures that software is always up to date and performing as required since the environment and customer demands continually evolve (McQuade, 2019). The private sector and Big Tech have found ways to master CI/CD to make massive profits and benefit worldwide markets of customers; meanwhile, the DoD struggles to improve software development. Even the Defense Acquisition University (DAU) lacks a foundational understanding of development and operations, also known as DevOps. A recent DAU article notes that DevOps is the feedback loop and relationship between developers and operators, implying that the latter are the military users in the field, which is not entirely correct (Miller, 2022). DevOps is better defined as unification of software development

and information technology (IT), to achieve CI/CD and eliminate functional silos between technical teams (DevOps, 2022). That small distinction, regarding the type of operators that developers interact with in DevOps, is a common misunderstanding in the defense world. Continuous integration and iteration that happens between developers and IT operators helps provide value to customer stakeholders, which in the DoD, are ultimately the military operators and warfighters, who are not necessarily fluent in IT operations.

Recent Government Accounting Office (GAO) and Defense Innovation Board (DIB) recommendations on DoD software acquisition highlight essential areas of improvement:

- GAO-19-58: "…should ensure that the CIO of Defense completes an assessment of all IT investments for suitability for migration to a cloud computing service, in accordance with OMB guidance" (Cloud Computing, 2019, p. 48).
- GAO-19-457: "…should ensure the department implements the pilot program by releasing at least 20 percent of newly custom-developed code as OSS [open-source software]" (Open-Source Software, 2019, p. 14).
- GAO-21-105298: "…programs have yet to implement certain recommended practices associated with modern software development approaches…only six of 36 weapon programs that reported using Agile also reported delivering software to users in less than 3 months" (Status of Challenges, 2021, n. p. [pre-page i after title page]).
- 2019 DIB: "…software development is broken and is a leading source of risk to DoD: it takes too long, is too expensive, and exposes warfighters to unacceptable risk by delaying their access to tools they need to ensure mission success" (McQuade, 2019, p. 1).

According to the GAO website, the DoD has yet to make considerable progress in these areas. The DoD should therefore put commercial best of breed companies to work to continuously

integrate their stellar talent and tacit knowledge from their profitable experience into how the DoD acquires software and improves its proficiency in the information domain battlespace. Furthermore, the DoD needs to make use of individuals from commercial companies with a different background--software people that can change the world (Hadley, 2022).

Mobilization

"Success no longer goes to the country that develops a new technology first, but rather to the one that better integrates it and adapts its way of fighting."

– Summary of the 2018 National Defense Strategy

A primary factor in any modern warfighting strategic deterrence framework depends on the current phase of war, however, many experts say the U.S. is already immersed in a Cold War with China, and a "hot" war is just over the horizon (Beckley, 2021). The Defense Production Act of 1950 built on the success of mobilization in World War II and ensured availability of the nation's resources to meet national security needs by granting executive power to ensure supply and delivery of products and services to military and civilian agencies (Else, 2009). It remains employable today but could stand to be modernized with the implications of modern technology and the information domain in mind. The three titles that remain in effect allude to ordering companies to prioritize defense-related products and the expansion of production capacity, recalling anachronistic images of assembly lines and hardware factories. Of course, today the capabilities are largely software-based. Ideally, the U.S. does not wait until the last minute to use executive powers to employ the commercial sector the way it should; rather, the U.S. should integrate commercial best of breed expertise into its existing work. In any event, the legal means are there to use, as Beijing remains fully determined to make China whole again by "reuniting" Taiwan with the mainland.

From policy, one knows that "Mobilization is the process of assembling and organizing national resources to support national objectives in time of war or other emergencies" (Joint Mobilization Planning, 2018, ix). However, this largely applies to movement of kinetic capabilities. The central problem here is, how are 0s and 1s mobilized? Does the hardware-centric perception of mobilization need to change for the future? For years now, Russia and China have blurred the lines between what is traditionally known as peacetime and war, so why constrict how the U.S. prepares to fight? The tenets of successful mobilization can be applied to the information domain just as well: "objective, timeliness, unity of effort, flexibility, and sustainability" (Joint Mobilization Planning, 2018, p. ix).

New constructs exist to enable rapid acquisition and mobilization in support of information warfare and decision superiority. In recent years, there have been new ways to work with the DoD including Partnership Intermediary Agreements, Commercial Solutions Openings, Pitch Days, Middle-Tier Acquisitions, and Other Transaction Authorities (OTAs) (Mihalisko, 2019). Recent legislation allows for pilot programs to accelerate procurement of innovative technologies and to improve acquisition practices for emerging technologies. In addition, assessments are to be conducted on impediments to acquisition such as "systemic biases in favor of custom solutions," which alludes to the tendency of the defense community to create monolithic programs with complex requirements that might be solved with commercial-off-the-shelf (COTS) products (Rossino, 2021, para. 4). By the time funding is obtained to resource and acquire information domain capabilities, it is often too late because the technology has evolved dramatically, or the adversarial threat has changed. This issue is so pervasive that a new commission has been ordered to address the current timeline-focused DoD budgeting process (Serbu, 2021). These reforms along with incremental value-focused mobilization and budgeting

process could drive increased iteration and agility into U.S. information domain capabilities in support of integrated deterrence.

Employing Commercial Best of Breed

"I don't know what you want to call the conflict we're in with China and Russia, but I'd say we're at war."

– Michael Brown, Director, Defense Innovation Unit (Sullivan, 2021)

Now more than ever, the U.S. military struggles to maintain its technological superiority on the world stage. Recent reports recommend that the DoD seek and embrace technology developed outside of its traditional contractor base, as well as find ways to adapt and leverage commercial technologies for defense applications (Sargent, 2021). These suggestions include modifying organizations and business models to better access technology. The Defense Innovation Unit (DIU) was put in place in 2015 in part to address the need for the United States to more quickly scale commercial technology across the DoD. Despite being focused on one form of contract, OTAs, DIU has set a solid path for identifying and seeding small companies and startups with research funds. This supports future-shaping technology like artificial intelligence (AI), autonomy, integrated network systems of systems, and advanced computing and software, which has been highlighted as competition era priorities (Shyu, 2022). DIU's director, Michael Brown, insists that the U.S. is not shifting enough resources fast enough to the information domain, estimating that commercial best of breed IT companies have been involved in only 1% to 2% of DoD procurement at this point, and much less so on the warfighting side (Sullivan, 2021). As fruitful as these efforts have been to open the doors to Silicon Valley, the U.S. has largely left commercial IT companies out of the warfighting business.

In the recent past, there have been strident arguments against commercial IT companies working with DoD, such as with Project Maven, which is an AI surveillance and classification project, where more than 3,000 Google employees signed a petition to protest involvement with the DoD (Shane, 2018). However, given China's R&D growth rate and the ongoing failures in software acquisition, the DoD may have no choice but to embrace the commercial sector, as even Google has come back around saying they are "firmly committed to serving our public sector customers" (Wakabayashi, 2021). Ultimately, the recent National Security Commission on Artificial Intelligence, chaired by former Google CEO Eric Schmidt, highlighted that despite all the talk about "public-private partnerships" with commercial best of breed companies, there has been little or no action on the part of the DoD, as the Pentagon scrambles to counter the rise of China (Tracy, 2021). The power of the commercial sector lies in its agility, capability, and talent, and the U.S. has yet to take full advantage. According to Silicon Valley, "time is running out" for the DoD to take advantage of tech companies who continue to battle barriers to entry in working with the U.S. government (Insinna, 2021, para. 3). Therefore, the time is ripe to acquire new capabilities with agility.

Summary

"Whatever it takes." – Captain America, The Avengers, Marvel Comics

China's intentions are clear: to emerge from the ashes of previous epochs of humiliation by the West and realign the world order in their favor. Their way of thinking focuses on constant mastery of the situation, which lends itself to their renewed focus on the information domain, as they blur the lines between the phases of war and leverage state-run advances in technology like never before but without any of the bureaucracy the U.S. wrestles with. Our national security guidance has consistently told us to point toward China since the mid-2000s, however in

practice, the U.S. only recently begun to face that direction and address the situation. The U.S. can no longer assume that China or Russia will turn to nuclear means as a last resort nor pretend that it can predict the next move they will make. To support evolving ideas of integrated deterrence and nuclear hybrid warfare, decision superiority is the new holy grail. This requires early phase-of-war planning concepts, new information domain technologies, and consistent value delivery to the warfighter. These, in turn, depend on reliable software, agile acquisition processes, and potentially redefining how "mobilization" in the information age is viewed. To get there though, the U.S. must skillfully employ the help of commercial best of breed companies to enhance lethality in the information domain for mission planners, technology acquirers and user warfighters alike.

Given the supporting story told in the literature survey, the research question and hypothesis, as summarized previously, is timely, relevant, and viable. Key elements of the hypothesis touch on innovation, technology, and policy as shown in Table 1:

Technology	**Innovation**	**Policy**
Information Domain (Data, C2, space, cyber)	Leveraging Commercial Best of Breed IT	Defense Software Acquisition Pathway
Enabling Future Tech (AI, automation, etc.)	Persistent Warfighter Value Delivery	Joint Mobilization
Software Platform	Early Phase of War Decision Superiority	Integrated Deterrence

Table 1 - Research Proposal Key Elements

Methodology

The methodology for this work consists primarily of qualitative research, including:

1. A survey of recent and relevant literature as covered above.

2. Interviews with a handful of highly experienced senior defense experts to validate hypotheses, note themes, and fill gaps in our framework.
3. Use of a brief survey to our peer networks to confirm our hypotheses and better understand users, needs, and capabilities, from which a simple Wardley map can be constructed.

Findings from all elements of the research are then used to build a framework to leverage commercial best of breed companies to increase lethality and agility in how the U.S. deters China through our information domain capabilities.

Interviews were conducted with nine individuals from both government organizations and the defense industry. To ensure candor in interview discussion, all interviewees were pre-briefed that all answers to questions were non-attributable. Thus, interviewees are summarized in a generic manner in Table 2. Each interviewee was asked the same five interview questions which closely modeled the secondary research questions to help gather any notable themes (see Appendix A).

Interviewee Duty Title	**Experience**
Senior Executive Service Civilian, Theater Requirements	30+ years in military operations and strategic planning
Senior Executive Service Civilian, Service Requirements Policy	40 years in military operations and strategic planning
Technical Director, Major Defense Contractor	20 years in defense advanced technology development
Director of Requirements, Major Defense Contractor	30+ years in military operations and defense industry
General and Commander, Combatant Command Missile Defense	30 years in military operations and theater combat
General and Director, DoD Innovation	30+ years in military operations

Chief Architect, Missile Defense	30+ years in military space operations
General and Program Executive, Missile Defense	30+ years in air and space acquisition
Highly Qualified Expert, Defense Software	20 years in software development and technology entrepreneurship

Table 2 – Summary of Interviewees

A simple six-question survey was generated and distributed to our peer networks. A total of 33 respondents provided answers to the survey. From the answers, which highlighted existing issues, users, needs, and capabilities, a simple crowd sourced Wardley map can be made. Wardley mapping is a novel way to take a value chain anchored on customer needs and expand it across a map to show where components of a value chain lie, which in turn creates a shared understanding and vocabulary between stakeholders, potentially leading to new opportunities (Leading Edge Forum, 2022). Wardley mapping can be applied in this case to map the value chain for warfighters requiring decision superiority in support of integrated deterrence in the information age. This can be accomplished utilizing conclusions drawn from the literature as well as from interviews. The surveys can potentially induce some objectivity into a typically subjective exercise of creating a Wardley map.

Next, the preceding elements can ultimately inform a useful candidate framework to employ commercial best of breed IT and deliver value to warfighters in the information domain for INDOPACOM. A viable framework also requires assumptions, driving themes from our interviews plus notable elements outlined in Table 1, address identified users, needs and capabilities from the survey, an easy-to-follow model that includes effective outcomes, and a frequent feedback loop. One key assumption addresses stakeholders in the framework, who are as follows:

- Primary: Combatant commands (mission planners), Users/Operators/Warfighters, Information Domain System Acquirers, the DoD Service Branches (bill payers), Big Tech Industry Partners.
- Secondary: The President, Congress, American People (taxpayers), SECDEF, Joint Staff, China, and other adversarial nations.

Another assumption is the problem statement, which should be transparent and widely agreed to within the framework. Here, the research team assess that the problem is: **current technology expertise and acquisition processes are not sufficient to meet the emerging threat in the information age**. A third assumption is the theory of action, or the objectives of the framework; in other words, what will it aim to do? Currently, the objectives will be to accomplish the following:

1. Change the game (strategic level)
2. Gain decision superiority (operational level)
3. Deliver warfighter value (tactical level)

The first objective modernizes the overall way the DoD executes strategic deterrence, the second improves agility over time against an evolving threat, and the third enhances lethality within the mostly non-kinetic information domain. Taken together, the objective is then to gain a shared understanding of the threat in the current competition phase of war to create support of rapid and agile software acquisition processes that help fight the right war.

Results

Interviews

Based on interviews conducted with senior leaders, one the major pivots taken under advisement for the current hypothesis was to shift from Big Tech[1] as a primary player to mobilize and fill potential gaps in information domain capabilities in supporting integrated deterrence to "commercial best of breed IT companies". This was in part because many Big Tech firms have inherent conflicts of interest with the DoD, such as employees with close ties to, and divisions with major business operations in, potential adversarial nations (Anonymous Interviewee #9, personal communication, February 24, 2022). Unfortunately, some commercial companies prefer to support Chinese storefronts rather than work with the DoD. Thus, the authors shifted focus to commercial sector companies of all sizes, new or old, that could bring necessary software development and IT experience and expertise to the DoD.

Additionally, there were other themes that stood out above all. After reviewing notes from interviews and comparing these to the literature survey, the following themes emerged that should be a point of emphasis for an ideal framework:

Increase Clarity for Industry. The first theme echoed by both industry and government interviewees was ensuring enduring clarity for industry. While many commercial companies tend to embrace a purpose-driven business concept, the reality is that this sector of industry, just like companies comprising the defense industry, go into business to make a profit. To do so, they need to have predictability and clarity from their customers to position themselves for the future, recruit and hire the right workforce, scale production to align to demand, and invest in their own

[1] While there is no consensus on which companies comprise "big tech," people generally use the phrase to refer to Google, Apple, Facebook, Amazon, and Microsoft, as they wield significant social and economic power due to their size and market dominance (https://scholar.harvard.edu/files/hongqu/files/bigtechdemocracy.pdf).

innovation processes to meet anticipated future needs. To best enable industry partners, including those in the commercial sector, the DoD must set and stick to strategic priorities (Anonymous Interviewee #3, personal communication, March 19, 2022). In this vein, the use of Strategic Requirements Documents (SRDs) has recently been suggested as an agile process for validating operational needs and requirements which in turn enables iterative development of capabilities (Anonymous Interviewee #2, personal communication, March 23, 2022).

The current DoD acquisition process puts current defense industry companies at a disadvantage—not only cannot predict if the capability gaps, they are currently developing fits within Joint Capabilities Integration and Development Systems requirements, but unpredictable DoD budgets additionally hamper companies' future Independent Research and Development (IRAD) investments (Anonymous Interviewee #2, personal communication, March 23, 2022). This is due in part to the one-off, all-or-nothing, large program nature of acquisitions today, along with a lack of clear strategic roadmaps. There is no longer a guarantee that the DoD will buy technology in development. To make the best use of commercial best of breed IT companies, who tend to suffer from even greater barriers to entry into DoD business than traditional defense industry, they must be embedded earlier in the requirements process which drives future convergence and alignment around intent for future capabilities, increasing innovation, productivity, and decreasing costs in the long run. Industry must be on contract structures that allow them to be in the tent, shoulder-to-shoulder with DoD partners when requirements are developed so they can build collaboratively with continuous user input (Anonymous Interviewee #4, personal communication, March 19, 2022). Concerning clarity for commercial best of breed companies, the DoD does not have a shared understanding with tech

companies as well as the American people working for them, which will be an added obstacle in accelerating change to operate in the information age.

Use More Commercial Off-the-Shelf (COTS). The second theme observed in our research is that the DoD must accelerate adoption of and high Technology Readiness Level (TRL) offerings and COTS, which can increase speed of use and integration. TRL 7 through 9, meaning technology demonstrated in its intended environment up through technology that is mission proven, is abundant among commercial best of breed IT company offerings. This, along with typically higher amounts of IRAD funding on the commercial side can accelerate new technology and capability to implementation and get those into the hands of the warfighter faster. One interviewee noted that Amazon government cloud is two years behind Amazon's best commercial capabilities (Anonymous Interviewee #9, personal communication, February 24, 2022). The more COTS is used, the more benefits and vulnerabilities can be understood to bridge the gap between commercial and DoD capabilities.

The DoD can learn just as much from commercial best of breed technology as they can from their talent and experience. Approaches such as agile methodologies are being used more in the DoD, however not to the fullest extent they could be. Best of breed commercial companies can help embed best practices and train the warfighter, resulting in continuous learning and improvements.

Use Platforms for Information Domain Capability. The third theme observed in multiple discussions with senior leaders is use of software platforms as well as to focus on problems, not prescribed solutions. DoD software platforms are gaining traction recently due to their tendency to increase frequency of value delivery through CI/CD pipelines and how they encourage modularity, discourage vendor-lock, open-source solutions, and enterprise-level systems

thinking. Government leaders recently note that software defined hardware adds agility and drives the DoD away from single-purpose systems. Instead of software within mission systems, the time has come to think of mission systems as the co-stars riding on well-thought-out software platforms (Tirpak, 2022). The DoD can employ frameworks to solve problems directly with commercial speed and scaling instead of being bound by over-specified DOD requirements for custom solutions (Brown, 2022). Given today's procurement model, one small step of progress would be to consider best of breed IT companies as primes while hardware companies are the subcontractors (Anonymous Interviewee #8, personal communication, March 8, 2022). Furthermore, since hardware is more and more becoming a commodity, and waveforms can be change without changing hardware, hardware can be situated, maintained, and updated at the edge, providing more flexibility to warfighters (Anonymous Interview #9, personal communication, February 24, 2022). This also discourages locking into any particular hardware provider over time.

Platforms stacked on a solid Government Reference Architecture (GRA) helps stakeholders accommodate their strategies, vision, objectives, and principles across systems. It enables reuse and interoperability across the platform, reduces technology lock-in, and increases security, functionality, availability, and scalability (Anonymous Interviewee #2, personal communication, March 23, 2022). Industry partners often deal with bespoke sets of standards for every individual program they bid for. With a solid intelligence library and infrastructure, multi-skilled, rapid software application iteration is enabled (Anonymous Interviewee #8, personal communication, March 8, 2022). Purpose-built one-off information systems reduce interoperability and integration of other systems and force workarounds for systems to communicate more effectively or to be able to communicate at all. With a reference architecture

to guide the way, the set of architectural principles, standards, reference models, and best practices ensure that the aligned investments have the greatest possible likelihood of success in both the near term and the long term, resulting in shorter implementation timelines and reduced costs (Anonymous Interviewee #2, personal communication, March 23, 2022).

Interview discussions also highlighted a lack of integration and implementation across the DoD. Rather than think of commercial best of breed as only introducing new technology to become future warfighter capability, they could take an enduring role in implementation, improvement, and sustainment of information domain technology most used today. Additionally, a shift away from over-definition and prescription of requirements by the DoD towards problems to be tackled with commercial best of breed companies in the tent enables their freedom to implement a wider array of solutions for the warfighter (Anonymous Interviewee #7, personal communication, March 9, 2022). In this way, a shared understanding is fostered, in which stakeholders listen to continuous commercial feedback on how software value is being delivered and allow them to understand better how the DoD does business. Platforms done correctly have the power of driving how the DoD does budgets from the current process which poorly attempts to predict the next five years of buying, to a value-driven and objectives-based acquisition process at scale that drives more real-time outcomes (Anonymous Interviewee #6, personal communication, March 9, 2022).

Be More Joint. The last major theme noted by a handful of the senior leaders interviewed is a lack of true "jointness" in our requirements and acquisitions, preventing innovation and adding great inefficiencies that the U.S. cannot afford. DoD acquisitions tend to be service-centric (Anonymous Interviewee #5, personal communication, March 16, 2022). Multiple leaders noted that the DoD is not yet situated to take advantage of the innovative techniques employed by best

of breed commercial companies in part because nothing within the Pentagon is truly joint—no joint money or systems of systems (Anonymous Interviewee #6, personal communication, March 9, 2022). A joint GRA to work with from the start enables industry partners to better model potential new information domain capabilities.

One major contributor to the lack of joint-ness is the over-classification of systems in development, which literally perpetuates stovepipes within the DoD (Capaccio, 2021). Multiple interviewees echoed this sentiment noting that acquisition leaders should tell people what the DoD is working on to reduce barriers and increase commercial interest, get our younger generations excited to help, and show some of our cards to deter adversaries and better communicate our "Sputnik moment" about threats in space or within the information domain with the American people (Anonymous Interviewee #1, personal communication, March 23, 2022). Most importantly, cutting down these stovepipes naturally encourages jointness and reduces redundancies in capability. Commercial best of breed companies could also be used to help communicate across formerly joint boundaries by embedding in joint operations, thinking without bias, and being the voice of user satisfaction. An ideal framework to improve information domain capability delivery to the warfighter is purely joint.

Survey Results

The survey collected inputs from 33 peers from government and industry in the world of defense and space. Full details from the survey, including demographics of respondents, can be found in Appendix B. The first two questions were meant to confirm our hypothesis about under-utilization of commercial best of breed IT companies and the need for modernized acquisition processes and frameworks in support of INDOPACOM deterrence. As seen in Figures 3 and 4, both hypotheses were validated by respondents.

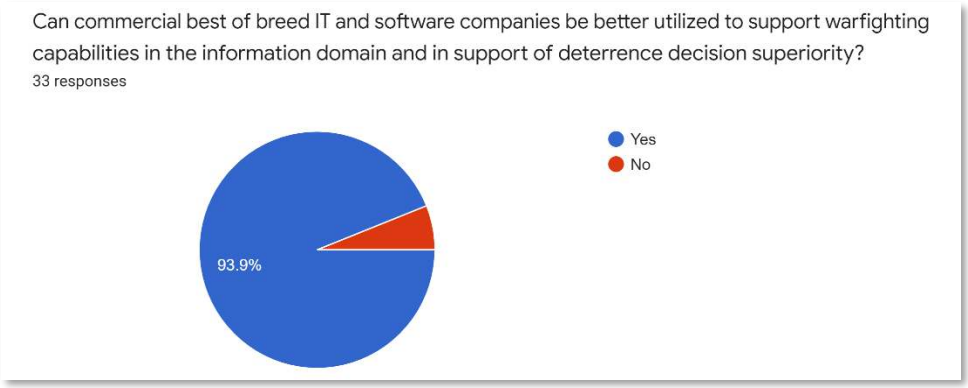


Figure 3 – Survey Responses: Underutilization of Commercial Best of Breed Companies

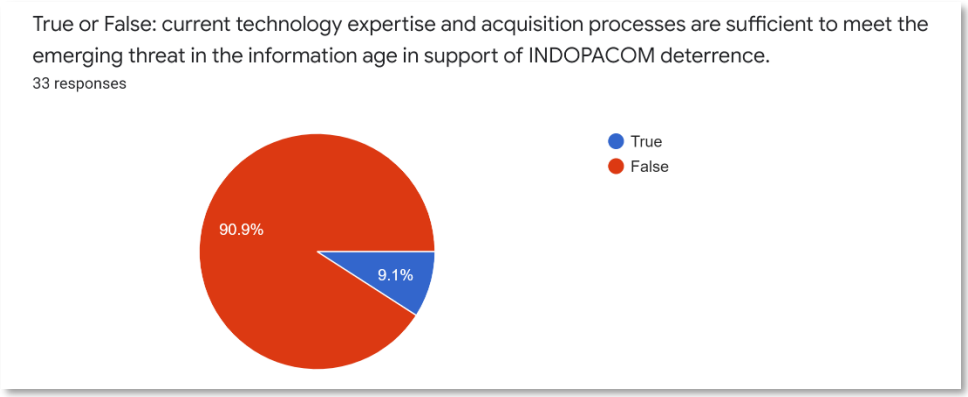


Figure 4 – Survey Responses: Current Acquisition Processes and Expertise

The next question was posed to address what the major information domain related issues might be in the DoD. Respondents could check all issues that apply and then score each on a discrete four-choice scale from "not an issue" to "highly profound issue." The following two issues had the highest frequency of being chosen as highly profound and were selected as highly profound over all other options:

- Outpace shrinking technology timescales with current acquisition law/policy
- Effectively plan and predict missions and scenarios

Respondents assessed that the majority of issues listed were a "definite issue" and the following came out as the top five in terms of highest frequency of selection (in order from the highest):

- Fielding good software
- Supporting deterrence in the information domain
- Achieving warfighter user satisfaction
- Bolstering early phase-of-war capabilities
- Meeting operational needs

Respondents identified the following users (stakeholders), needs, and capabilities as top priority, as shown in the basic Wardley Map in Figure 5. The intent of this map is to begin to show value chains for maturing information domain capabilities in INDOPACOM.

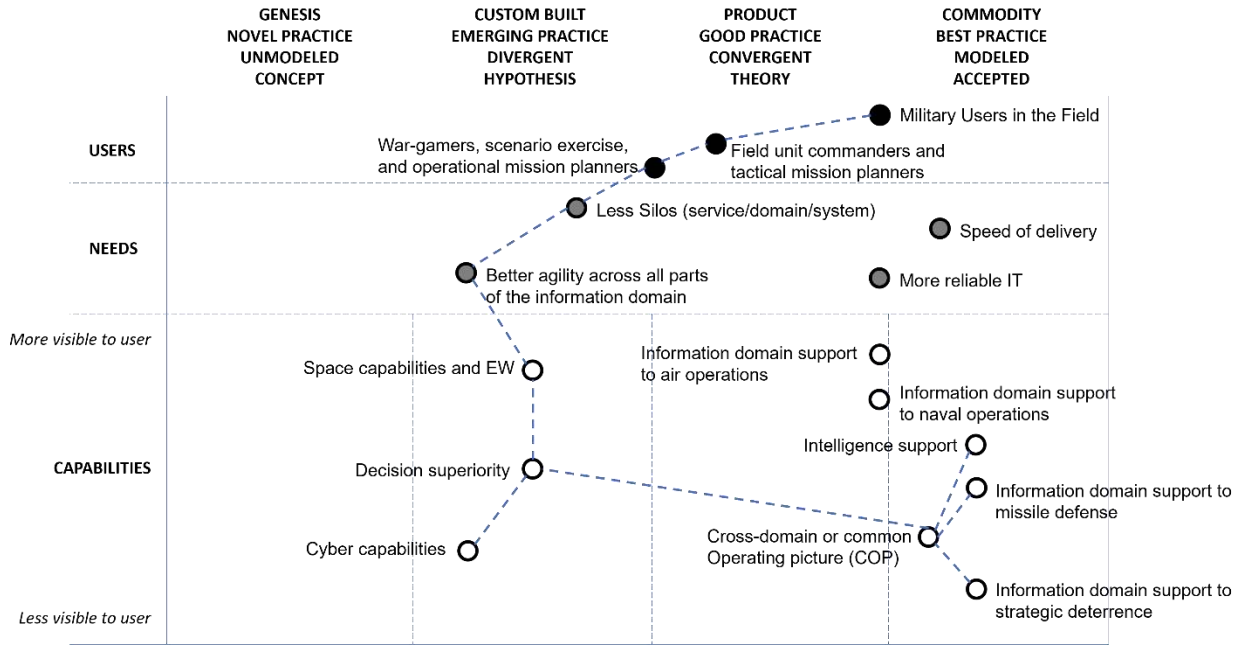


Figure 5 – Basic Wardley Map of INDOPACOM Information Domain Value Chain

Out of all options survey respondents could choose, the users and needs shown in Figure 5 were chosen more often than all others. The nine capabilities are mapped by their maturity, their priority as in how often respondents chose them, as well as by how visible and tangible they are to the user in the value chain. Unsurprisingly, tactical users and their unit commanders were

most often cited as key stakeholders, as well as needs such as less silos, speed of delivery, and reliable IT. The need for better agility in the information domain along with the space, cyber, and decision superiority capabilities that would benefit were reported as less mature and still evolving than other capabilities that were more well understood, such as information domain support to air and naval operations. When it comes to how to approach these challenges, capabilities on the right side of a Wardley map can typically use COTS or be outsourced because they are well understood, while things on the left are more ambiguous and require more agility, attention, and custom solutions. Given the unique expertise of commercial best of breed IT companies and how they might be applied to the current problem, a dotted line has been drawn to show which value chain could reap significant benefits in supporting early phase of war, non-kinetic information domain capabilities. This is also ideally where the focus of a suggested framework should be.

Framework

The framework offered in Figure 6 outlines a number of the elements and findings from the research and results as outlined above. First, the framework is driven by the themes uncovered in our senior leader subject matter expert interviews, including being more joint, using more COTS, providing clarity for industry, and being platform-based while tackling problems and not addressing over-prescribed solutions. Second, the framework also drives towards objectives based on the literature, which are to deliver value to our users, gain decision superiority, and ultimately change the game at the strategic level. Third, given the survey results and the Wardley map, the framework ideally addresses agility, jointness and cutting down silos, and delivers value to decision, space, and cyber superiority within the information domain, ultimately in support of integrated deterrence.

The INDOPACOM Operational Needs & Information Capabilities (IONIC) Framework is a Combatant Command (CCMD) and operationally focused forum for leaders and stakeholders as noted in the Wardley map in all services in theater to continually update operational needs (ONs) and ensure they are delivered to the warfighter. To maintain agility, the model should incentivize INDOPACOM leaders to meet frequently to re-address capabilities in work as well as the evolving threat. The forum, ideally run like a scrum, reviews, prioritizes, resources, scores, completes, and cancels efforts within an evolving and running list of warfighter ONs. These ONs could be small in scope as they are meant to focus on software, IT, and other information domain features. Outcomes of the forum include having the latest idea of tactics to implement, operational plans to integrate, and new strategies to inform. Absolutely key to this framework is the ongoing feedback loop that updates efforts based on the threat, evolving user and warfighter needs, and perhaps most importantly, user and warfighter satisfaction.

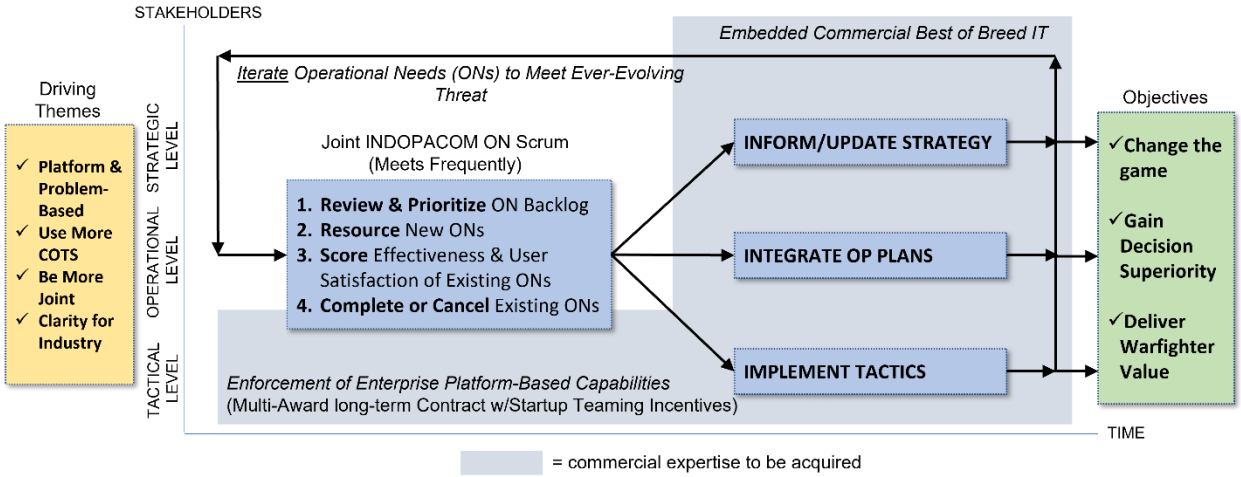


Figure 6 – INDOPACOM Operational Needs & Information Capabilities (IONIC) Framework

The last major element of the IONIC framework gets after the main objective of this hypothesis, which is how the DoD can best use commercial best of breed companies that have been under-utilized for so long to address these very relevant challenges. This framework does

not mean to impede or change existing traditional defense industry efforts working on perhaps more hardware-centric capabilities in any way. It is meant to be built on top of existing efforts to ensure information domain value delivery to the warfighter, which is where commercial best of breed companies can be best employed. The gray area in the framework highlights two main areas where these companies can be used—to drive and manage a joint platform for continuous information domain capability delivery and to advise and teach the DoD at tactical, operational, and strategic levels how we're currently doing it wrong and how to get it right. Ideally, the software expertise being acquired to help operate the framework on an ON delivery platform has the following traits:

- Long-term: "software is never done"
- Multi-awardee: encourages diversity and "best athlete" application of products/services
- Indefinite delivery and quantity structure type: flexibility for orders and contracts by ON
- Incentivizes teaming with non-traditionals and startups: more diversity!

Most of all, DoD regulations may not need to be rewritten if existing acquisitions policy can be used masterfully, such as the use of modular contracts for timely delivery of software applications, encouraging constant engagement with commercial industry, agile work statements, and broad solicitations (McGinn, 2022).

If commercial best of breed companies and their unbiased expertise can better understand what we're trying to deliver, then the DoD can better understand how best to deliver it. This in turn drives quickly evolving best-practice delivery of ONs, greater understanding of agility, and a shared, joint understanding and language of our most important work going forward in the information domain. The suggested framework emphasizes early and frequent collaboration of the right stakeholders, alignment with strategy, transparency, and value-focused oversight, which

is in line with recent thought leadership (McGregor, Modigliani, & Grant, 2022). If this can be scoped at first to a single but highly relevant CCMD, and the acquisition can be administered by that CCMD, then if successful, it could be scaled in other CCMDs or used to update our traditional software acquisition pathway policy.

Conclusion

The DoD must do more to properly incorporate the historically impressive expertise of commercial best of breed companies into an integrated deterrence strategy with China, which includes improving the ability to acquire software and delivering constant value in an agile manner to meet the evolving threat. As a result of research and interviews conducted, the IONIC framework is suggested that drives decision superiority and better informs leaders, planners, and users in the INDOPACOM region. IT and software must no longer be viewed as a cost but as a vital enabler for information domain capabilities, which can be accomplished through acquisition of a modern value delivery platform as well as through collaboration on deployment of tactics, planning, and strategy in a feedback loop that stays ahead of the threat. Interview results highlighted four areas of improvement for the DoD including, being more joint, using more COTS, using platforms to solve problems, and increasing clarity for industry. Surveys identified key stakeholders, needs, and maturity of relevant capabilities. The DoD can leverage commercial companies to support agile software development, quickly react to emerging threats, embed best practices in our operations, and consistently advise our leaders in the Pentagon and in the field. New constructs exist to enable rapid acquisition and mobilization of 0s and 1s in support of information warfare and decision superiority. The U.S must change the way it acquires and delivers these kinds of capabilities, and the IONIC framework may help the DoD finally transition from the industrial age into the information age of warfighting.

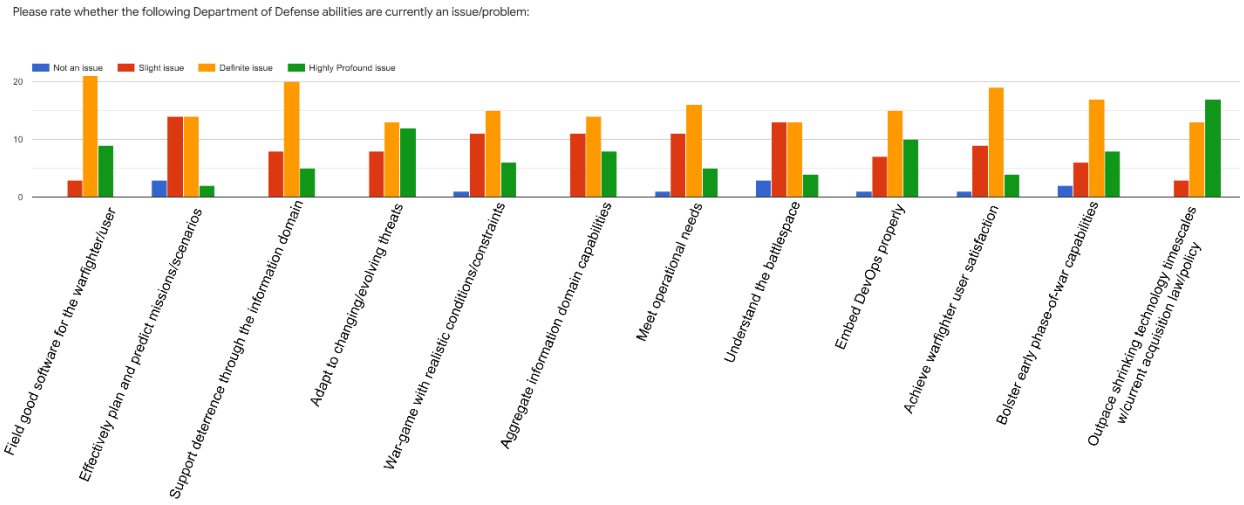
Appendix A

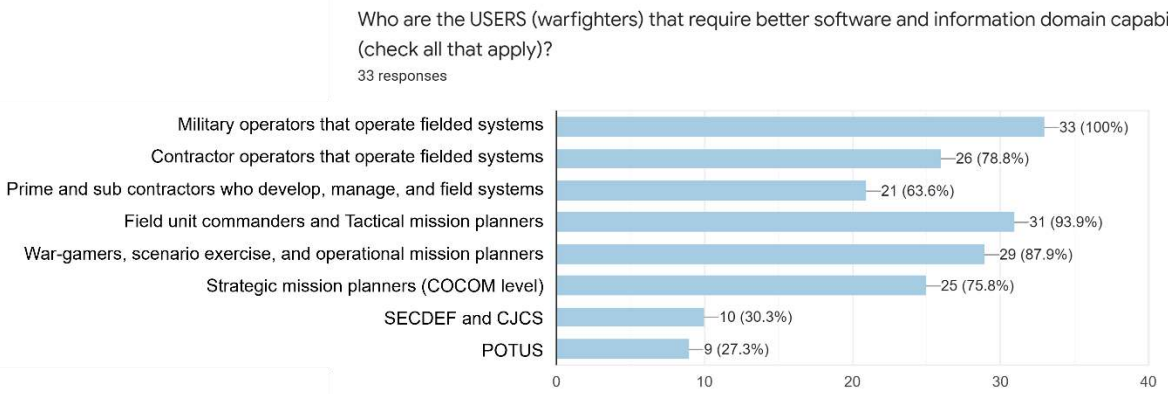
Based on the primary and secondary research questions in the introduction, the following questions were asked during interviews for the current research:

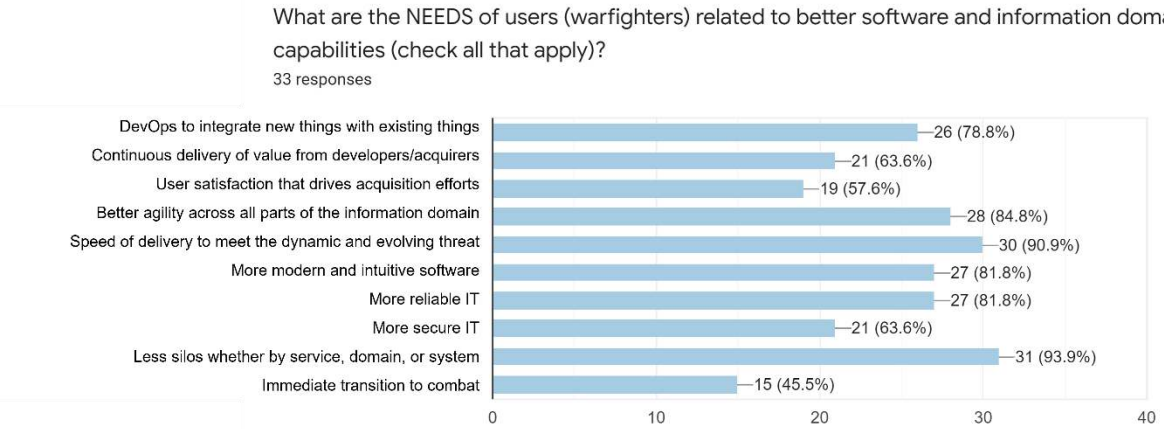
1. In the 40s and 50s we mobilized domestic companies to help fight our wars. To evolve from the industrial age to the information age, what can Commercial Best of Breed IT companies do that advance military capabilities within the information domain and help achieve decision superiority?
2. What incentives or improvements to the DoD software acquisition process could field information domain capabilities (space, cyber, C2, data, etc.) with more agility and warfighter utility in the face of an ever-evolving threat? Are there software acquisition tripwires to be avoided?
3. What do you think we can do to create a better shared understanding between DoD and Commercial best of breed software and IT companies? Can an acquisition and warfighter value delivery model exist that leverages commercial best of breed to:
    a. stay ahead of and quickly react to threats, (Tactical)
    b. embed in our operations, (Operational)
    c. and constantly advise DoD leaders? (Strategic)
4. Are there corollary mass mobilization and rapid-reaction hardware acquisitions we can learn from and apply to software and information domain acquisition? How do we effectively mobilize 0s and 1s?
5. What can we learn from recent innovative organizations, constructs, and solutions that have failed or delivered less value than expected? Are there current innovation entities and efforts delivering sufficient value to warfighters? How do we reap the benefits of software in a way that traditional methods cannot?

Appendix B

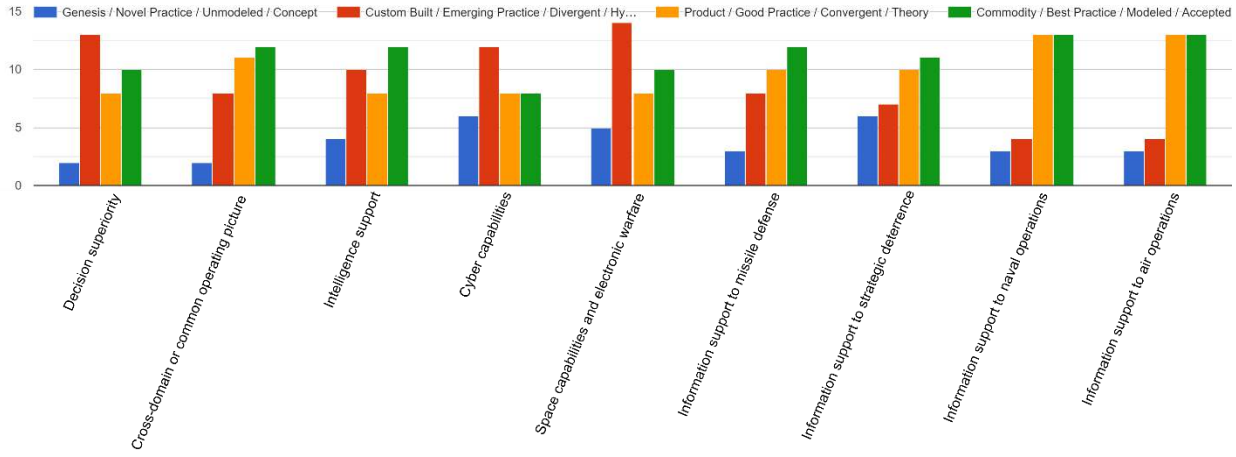
The following graphs outline the full results of the survey with 33 respondents.





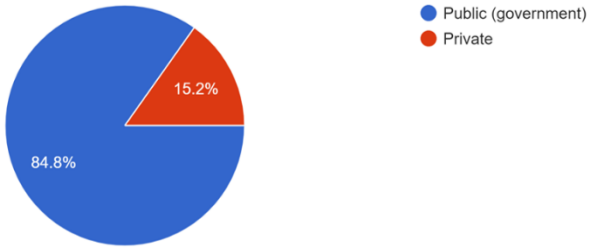


What CAPABILITIES (tools/software) do users (warfighters) require related software and information domain capabilities? Only check rows that apply. Then, for each capability, check ONE column that best describes the capability.



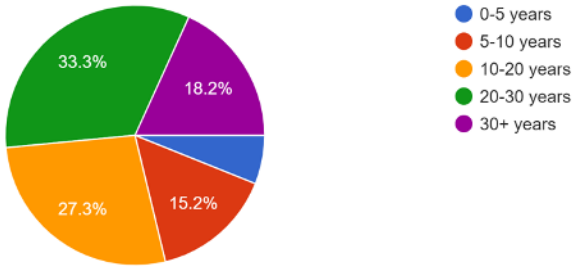
What sector do you currently work in?

33 responses



What is your level of expertise related to IT and/or defense?

33 responses



Which of the following best describes your subject matter expertise?

33 responses

References

Anton, P. S. (2020). *Strategies for Acquisition Agility: Approaches for Speeding Delivery of Defense Capabilities.* Santa Monica, Calif.: RAND Corporation.

Beckley, M. B. (2021, November 1). What Will Drive China to War? *The Atlantic*.

Brooks, F. P. (1986). No Silver Bullet--Essence and Accident in Software Engineering. *Proceedings of the IFIP Tenth World Computing Conference*, (pp. 1069-1076).

Brown, M. (2022, February 5). Reigniting the Pentagon and Silicon Valley Partnership. *TechCrunch*.

Capaccio, A. (2021, October 28). No. 2 Military Officer Bemoans Pentagon's Excess Classification. *Bloomberg*.

Chunqiu, W. (2002). *Dialectics and the Study of Grand Strategy: A Chinese View.* China Aerospace Studies Institute.

(2019). *Cloud Computing: Agencies Have Increaed Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked.* Washington, D. C.: U.S. Government Accountability Office.

Cohen, R. S. (2021, May 18). It's Time to Drop 'Competition' in the National Defense Strategy. *The RAND Blog*.

Cordesman, A. H. (2021). *Chinese Strategy and Military Forces in 2021: A Graphic Net Assessment.* Washington, D. C.: Center for Strategic and International Studies.

DoD Instruction 5000.87, Operation of the Acquisition Pathway. (2021, October 2). Retrieved from https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500087p.PDF

(2021). *DoD Software Acquisition: Status of Challenges Related to Reform Efforts.* Washington, D. C.: U.S. Government Accoiuntability Office.

Doshi, R. (2021). *The long game: China's grand strategy to displace American order.* New York: Oxford University Press.

Else, D. H. (2009). *Defense Production Act: Purpose and Scope.* Congressional Research Service.

Garamone, J. (2021, December 8). *Concept of Integrated Deterrence Will Be Key to National Defense Strategy*. Retrieved from DoD News: https://www.defense.gov/News/News-Stories/Article/Article/2866963/concept-of-integrated-deterrence-will-be-key-to-national-defense-strategy-dod-o/

Hadley, G. (2022, March 4). Former Google CEO: AI Will Be 'Force Multiplier Like You've Never Seen Before'. *Air Force Magazine*.

(2019). *Information Technology: DoD Needs to Fully Implement Program for Piloting Open Source Software.* Washington, D.C.: U.S. Government Accountability Office.

Insinna, V. (2021, December 23). *Silicon Valley warns the Pentagon: 'Time is running out'*. Retrieved from Breaking Defense: https://breakingdefense.com/2021/12/silicon-valley-warns-the-pentagon-time-is-running-out/

(2021). *Interim National Secuirty Guidance.* Washington, D. C.: The White House.

Johnson, J. J. (2015, September 8). *Phase Zero and the unique parallels of space and cyber*. Retrieved from The Space Review by Space News: https://thespacereview.com/article/2820/1

Johnson, J. J. (2016, June 9). Turning Words Into Action: Confronting Acquisition Challenges. *Defense AT&L Magazine*, p. 43.

(2018). *Joint Mobilization Planning.* Washington, D. C.: Department of Defense.

Leading Edge Forum. (2022). Retrieved from Wardley Mapping: Accelerator Workshop: https://leadingedgeforum.turtl.co/story/wardley-mapping-accelerator-workshop/page/2

Lingel, S. S. (2021). *Leveraging Complexity in Great Power Competition and Warfare: Volume I, An Initial Exploration of How Complex Adaptive Systems Thinking Can Frame Opportunities and Challenges.* Santa Monica, Calif.: RAND Corporation.

Losey, S. (2022, April 20). SpaceX shut down a Russian electromagnetic warfare attack in Ukraine last month — and the Pentagon is taking notes. *C4ISRNet*.

McGinn, J. (2022, March 2). You don’t need to rewrite acquisition regulations to improve DoD buying. *DefenseNews*.

McGregor, M., Modigliani, P., & Grant, G. (2022, March 7). Pentagon needs a six-pillar foundation. *The Hill*.

McQuade, M. J. (2019). *Software is Never Done: Refactoring Acquisition Code for Competitive Advantage.* Defense Innovation Board.

Mihalisko, S. (2019, May 30). *'Rapid Contracting': A Quick Review of OTAs and Other Methods to Acquire Innovation*. Retrieved from GovWin: https://iq.govwin.com/neo/marketAnalysis/view/Rapid-Contracting-A-Quick-Review-of-OTAs-and-Other-Methods-to-Acquire-Innovation/

Miller, A. W. (2022). Challenges of Adopting DevOps for the Combat Systems Development Enviornment. *Defense Acquisition Research Journal #99*, 25.

(2021). *Miltary and Security Developments Involving the People's Republic of China.* Office of the Secretary of Defense.

(2008). *National Defense Strategy.* Washington, D. C.: Department of Defense.

(2015). *National Security Strategy.* Washington, D. C.: The White House.

(2017). *National Security Strategy of the United States of America.* Washington, D. C.: The White House.

Nix, N. C. (2021, July 6). Pentagon Moves to Split Cloud Deal Between Microsoft, Amazon. *Bloomberg*.

Osborn, K. (2021, September 25). *The National Interest*. Retrieved from https://nationalinterest.org/blog/buzz/why-air-force%E2%80%99s-icbm-infrastructure-needs-upgrade-194487

Peters, R. A. (2018). Deterrence in the 21st Century: Integrating Nuclear and Conventional Force. *Strategic Studies Quarterly*, 15-26.

Pillsbury, M. (2015). *The Hundred Year Marathon: China's Secret Strategy to Replace America as the Global Superpower.* New York: St. Martin's Griffin.

Rathje, J. (2019, November 18). Solutions, Garbage Cans, and Platforms: How to Drive Commerical Solutions into the Military. *War On The Rocks*.

Rossino, A. (2021, December 15). *Select Acquisition Provisions in the FY 2022 National Defense Authorization Act*. Retrieved from GovWin: https://iq.govwin.com/neo/marketAnalysis/view/Select-Acquisition-Provisions-in-the-FY-2022-National-Defense-Authorization-Act/

Sargent, J. F. (2021). *The Global Research and Development Landscape and Implications for the Department of Defense.* Congressional Research Service.

Serbu, J. (2021, December 29). *Pentagon's ponderous budget process is next target for Congressional reform*. Retrieved from Federal News Network: https://federalnewsnetwork.com/defense-main/2021/12/pentagons-ponderous-budget-process-is-next-target-for-congressional-reform/

Shane, S. W. (2018, April 4). 'The Business of War': Google Employees Protest Work for the Pentagon. *The New York Times*.

Shimmin, R. (2022, January 5). *#PowerebyTalent--Rogan Shimmin*. Retrieved from Linkedin.com: https://www.linkedin.com/pulse/poweredbytalent-rogan-shimmin-diux/

Shyu, H. (2022, Fenruary 1). USD(R&E) Tehcnology Vision for an Era of Competition. *Official Memo*. Washington, D.C.: Department of Defense.

Software Acquisition. (2021, Jan 6). Retrieved from Defense Acqusition University: https://aaf.dau.edu/aaf/software/

Sullivan, M. (2021, November 1). Silicon Valley Wants to power the U.S. war machine. *Fast Company*.

(2018). *Summary of the 2018 National Defense Strategy of The United States of America.* Washington, D.C.: Department of Defense.

The White House. (2022, January 3). Retrieved from whitehouse.gov: https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/03/p5-statement-on-preventing-nuclear-war-and-avoiding-arms-races/

Tirpak, J. A. (2021, October 8). USAF's Three Priorities: China, China, and China. *Air Force Magazine*.

Tirpak, J. A. (2022, March 11). 5 Changes to Acquisition Focusing on Threat, Talent, and Tech. *Air Force Magazine*.

Tracy, R. (2021, September 7). As Google, Microsoft and Amazon Seek Bigger Defense Role, Some Are Leery. *The Wall Street Journal*.

Wakabayashi, D. C. (2021, November 3). Google Wants to Work With the Pentagon Again, Despite Employee Concerns. *The New York Times*.

What is DevOps? (2022). Retrieved from about.gitlab.com/topics/devops

Williams, L. C. (2021, November 8). *Why the DOD is so bad at buying software*. Retrieved from FCW: The Business of Federal Technology: https://fcw.com/acquisition/2021/11/why-dod-is-so-bad-at-buying-software/259180/