Fall 2020 Roundtable Series Insights Paper

Unlocking New Sources of Techno-Security Advantage

In 2015, Senator John McCain sought help from leaders in tech and finance to improve relations between the innovation hub of Silicon Valley and the technology demands of the defense market.

The result: The Silicon Valley Defense Group.

The Silicon Valley Defense Group seeks to ensure the U.S. and its allies achieve a durable advantage in the global techno-security competition. To achieve this goal, we create the nexus of pioneering ideas, people, and capital that will unlock new sources of innovation for national security and power the digital evolution of the defense industrial base. With questions, or for more information, visit www.siliconvalleydefense.org.

With gratitude to our series sponsors:

ANDURIL

Microsoft Raytheon Technologies

Google Cloud MAXAR UBS ForgePoint CAPITAL rebellion

Preface

The series of discussions hosted by the Silicon Valley Defense Group in the fall of 2020 sought to explore the challenges to developing a sustained, durable techno-security advantage in the face of a increasingly competitive environment. We acknowledge at the outset that an enormous amount of research and analysis has already been undertaken to address these themes. This document does not seek to reiterate a comprehensive summary of all ideas that have been expressed on these topics, but to highlight insights generated by the rich dialogues in the series and to suggest novel areas for immediate and future action by those parties able to advance U.S. techno-security.

We recognize that implementing any of these expert recommendations will require public sector leaders, private sector investors, and technologists and innovators in both civilian and military roles to achieve mutual understanding, alignment of incentives, and the resurgence of a robust defense innovation ecosystem. At the same time, trust between the defense and innovation communities has grown brittle. We saw no better way to begin to bridge this gap than by fostering robust dialogue and debate.

Up to now, the U.S. Department of Defense has prioritized maintaining the readiness of its legacy military posture, while making modest investments in innovation. Sustaining this posture has made it challenging to shift DoD's focus to the full range of digital capabilities this moment demands. Now the U.S. government must confront the problematic reality that we are losing -- or have lost -- our global position as an unrivaled military power. We must employ all means necessary to compete technologically, economically, and geopolitically. In order to do so, Congress must consider a bottom-up approach to industrial policy—in which DoD defines target outcomes and serves as a fast follower of technologies developed in the commercial sector. We see no other path to the innovation at speed and scale that would restore a techno-security advantage to America and its allies.

To sustain political support for DoD's investment in and procurement of new commercial technologies, the public needs to understand the nature of the challenge that the United States faces. Public hearings about the pace of China's technological advances and their ethical implications will be vital in helping the American public and its allies understand the magnitude of the threat the U.S. faces. A coordinated public engagement campaign on this topic should inform citizens -- and in some cases, their leaders – of how leadership in strategic technologies will shape the future of allied democracies, free markets, and human rights. Partisan differences between Democrats and Republicans has up to now yielded disagreement on the appropriate U.S. posture towards China, one compounded by the circumstances of the COVID-19 pandemic. Moving forward, it will be vital for political leaders to adopt a "country first" mentality, setting aside their domestic differences to do what it takes to ensure the U.S. retains its global position.

The Silicon Valley Defense Group looks forward to a future in which we serve as allies to policymakers, servicemembers, investors, entrepreneurs, and established industry players, bringing these important partners together around shared complex challenges to develop and execute solutions. Our hope is that this paper will serve as a starting point for discussion, and that robust and substantive actions swiftly follow.

Sam Gray
Executive Director, SVDG

Roundtable Speakers (By order of appearance):

Dr. Eric Schmidt, Former CEO and Executive Chairman, Google // Co-Founder, Schmidt Futures
The Hon. Dr. Will Roper, Assistant Secretary of the Air Force for Acquisition
James Baker, Director, Office of Net Assessment
Lee Dunn, Director of Government Affairs and Public Policy, Google
Dr. Kori Schake, Director of Foreign and Defense Policy, AEI
Tom Keane, Corporate Vice President, Azure Global, Microsoft
VADM Fritz Roegge, President, National Defense University
The Honorable Malcolm Turnbull, Former Prime Minister of Australia
GEN Joseph Votel (ret.) CEO, Business Executives for National Security (BENS)
Mike Brown, Director, the Defense Innovation Unit
Richard Coleman, VP and General Manager, Federal Sector, Axon
Peter Dixon, CEO, Second Front Systems
Meagan Metzger, CEO, Dcode
Rachel Olney, CEO, Geosite.io
Heather Richman, Entrepreneur-in-Residence, BMNT & Co-Founder, Defense Investor Network
Chad Rigetti, CEO, Rigetti Computing
Andrew Rubin, CEO, Illumio
Chris Shaw, CEO, Advanced Navigation
Trae' Stephens, Partner, Founders Fund & Chairman, Anduril
The Hon. Bob Work, the former Deputy Secretary of Defense
The Hon. Hondo Geurts, Assistant Secretary of the Navy for Research, Development & Acquisition
James Cross, Director, Franklin Venture Partners & Founder, SVDG
Orion Hindawi, CEO, Tanium
Nazzic Keene, CEO, SAIC
Wahid Nawabi, CEO, Aerovironment
Brian Schimpf, CEO, Anduril
Mike Petters, CEO, Huntington Ingalls Industries
Kevin Phillips, CEO, Mantech
Myles Walton, Senior Aero-Defense Analyst, UBS
Katie Arrington, Chief Information Security Officer, DoD Office of Acquisition & Sustainment
Matt Bigge, Partner, Crosslink Ventures
Steve Blank, Professor, Stanford University
Jonathan Curtis, Portfolio Manager, Franklin Templeton
Sheila Kahyaoglu, Senior Aero/DefenseAnalyst, Jeffries
Chris Moran, Partner, Lockheed Martin Ventures
Raj Shah, Partner, Shield Capital & former Director of the Defense Innovation Unit Experimental
Alberto Yepez, Managing Director, Forgepoint Capital
Representative Mac Thornberry, (R-TX), House Armed Services Committee
Representative Jim Banks, (R-IN), House Armed Services Committee
Representative Seth Moulton, (D-MA), House Armed Services Committee
Chris Brose, Chief Strategy Officer, Anduril
Bobby Franklin, CEO, National Venture Capital Association
Gayle Tzemach Lemmon, Partner, Chief Marketing Officer, Shield AI
Chris Lynch, CEO, Rebellion & founder of the Defense Digital Service
Tom Mahnken, CEO, CSBA
Joshua Marcuse, Advisor, SVDG & former Executive Director of the Defense Innovation Board (Moderator)

Introduction

In fall 2020, the Silicon Valley Defense Group (SVDG) convened a series of five roundtables that brought together leaders and luminaries from government, industry, and academia with the expertise and authority to respond to the escalating techno-security challenges of this moment. These virtual events were conducted under Chatham House rules, but were open to a broad group of attendees who represented the technology, finance, military, and policy communities. Each of the conversations addressed a specific aspect of the challenge, focusing on five key components of techno-security innovation: the geopolitical context, the challenges of entering the defense market, disruption in the established defense industrial base, incentives for and barriers to capital investment, and the public policy interventions required to address these objectives. The discussions generated clear conclusions on ways to improve the relationship between the Department of Defense (DoD) and industry, the need to evolve the stance of the United States and its allies towards its rivals, and deeper reforms and strategic changes needed to transform DoD.

In 2020, the United States and its allies face a unique set of security challenges. Digitization has transformed industry, bringing digital technology into every aspect of the global economy, and the transformation of industry has changed the nature of power. In the 20th century, the size of a nation's weapons arsenal determined its ability to project power worldwide. Today, technological innovation and geoeconomic dominance are the primary sources of global strength. The defining characteristic of this new era of technological competition is speed, and the U.S. defense ecosystem is not optimized for speed in any respect.

In the last five years, a crescendo of congressional, military, civilian, and academic leaders have sounded the alarm. On September 23, 2020 the House Armed Services Future of Defense Task Force issued an 87-page report on the realignment required to ensure America's strategic competitiveness, which reinforces similar findings by other commissions. While such reports indicate emerging intellectual consensus, the financial resources, political will, and urgency required to achieve the stated objectives are still missing.

Yet, even if the government took decisive action, as it must, it cannot singlehandedly re-orient the United States' defense and aerospace market along with the widening array of related industries (e.g., semiconductors, telecommunications, and information technology) required to achieve its mission. Implementing any of these expert recommendations will require public sector leaders, private sector investors, and technologists and innovators in both civilian and military roles to achieve mutual understanding, alignment of incentives, and the resurgence of a robust defense innovation ecosystem. To this end, this paper recommends three core areas of focus that, taken together, will affect this outcome.

The Relationship Between Government & Industry

> ***"The military needs commercial technology because we're not developing all of what we need in the military these days. Much of what we need is dual-use commercial technology where we can leverage the scale inherent with the success of commercial vendors. We need an answer to China's civil-military fusion. And the nation needs the U.S. and our allies to lead in these game-changing technologies for our economic prosperity and for our national security."***
>
> *– Michael Brown, Director, DIU*

During the Cold War, government investment drove the emergence of Silicon Valley as a hotbed of innovation, fostering close ties between government-funded R&D, private investment, and the adoption of emerging technology. Over the past two decades, as Silicon Valley has led the digitization of industry, the United States

has ceded aspects of its military technological advantage to its rivals. Private sector venture capital and commercial R&D has overtaken government funding as the driver of innovation. Trust between the defense and innovation communities has grown brittle. New commercial technologies have languished in the defense market as the U.S. government has prioritized Lowest Price/Technically Acceptable (LPTA) offerings or focused on legacy programs at the expense of building an investment portfolio of "new bets," producing a risk-averse defense culture that prioritizes sustainment over innovation. The status quo emphasizes capacity and incremental innovation over transformational disruption.

The scope and importance of the government's mission can effectively motivate collaboration and commitment, yet, as the gap between government and industry has grown, eroded trust has dampened the will of industry to advance America's technological dominance. Stringent security protocols and opaque acquisition requirements have made it nearly impossible for commercial companies to serve the innovation needs of the United States. For much of the past decade, the U.S. government has focused on cost-savings over speed, and prioritized legacy platforms over disruptive new digital approaches, yielding a laggard legacy posture against rapidly evolving threats. R&D funding is both too sparse and too slow to invest effectively in technologies as they emerge.

The commercial world always faces the age-old management quandary: cheap, good, or fast—pick two. While DoD claims to prioritize quality and cost, an insistence on bespoke products often means that the final cost of unique solutions far surpasses the original bid price. While the cost of a commercial product may exceed that of a bid price, in final terms, commercial prices are inherently more competitive and affordable while also offering the benefit of being ready to deploy much more quickly. Now is the time for DoD to focus on quality and speed, and seek pathways to deploy the most cutting edge emergent digital technologies as quickly as possible.

> ***"Where I think the DoD has not particularly kept pace with Silicon Valley is broadly around anything software-related. Software development is incredibly complex and we need to find more incentives for the DoD to embrace software and emerging technologies. That was a lot of what we thought about when we started: how can we bring what's working well in Silicon Valley—which is a software-first approach—into DoD?"***
>
> *– Brian Schimpf, CEO, Anduril*

Some successful efforts are underway to address this innovation shortfall. The creation of the Defense Innovation Unit (DIU) in 2015, located in Silicon Valley, has anchored a defense presence within the U.S. hotbed of innovation and has created an early demand signal for high-potential, dual-use technologies. Since then, more than 20 innovation-focused organizations have emerged to address different defense missions, customers, or technologies. Sadly, these organizations are underfunded, under-manned, uncoordinated, and under constant bureaucratic and political attack precisely because they are challenging the status quo. These pathfinders should be venerated for their efforts, but we should not be deluded into believing they will be adequate. The government must double down on these early successes with greater emphasis, investment, and flexibility. Elevating three core priorities could dramatically reshape the relationship between industry and government.

Flexible Funding: Increased government R&D investment can encourage increased investment from industry, who will be an important partner in both developing and deploying the next "moon shot." Congress should allocate a meaningful tranche of money that DoD can responsively invest in promising new technologies and account for that spending retroactively. DoD can also incentivize primes to proactively invest in new capabilities and ventures to disrupt themselves before they are disrupted or antiquated.

Hard Choices: To encourage the development of capabilities that serve its present and future needs, DoD must clearly frame the problems it seeks to solve and the outcomes it hopes to achieve. Intentionally publishing (and de-classifying) operational problem statements will make it possible for new ventures to participate in designing solutions and for primes and new ventures to better collaborate. In turn, contracts should be awarded based on delivering outcomes, rather than on the basis of staffing, cost, or prior performance.

Publishing problems and target outcomes can serve as market indicators that encourage private investment in early stage companies and capabilities. Effectively connecting a technology with an intended strategic application, such as the U.S.-China competition in the South China Sea, could help signal to investors a technology's future potential. Ideally, private investors will join the government as co-investors to reduce risks and increase the probability of success.

In recent years, the military services have adapted the Small Business Innovation Research (SBIR) program so that it can better provide small, rapid grants to many early-stage companies. This has forged new collaborations, generated insights, interest, and goodwill, as well as some promising early results. Building on that success, DoD must strategically choose specific technologies that can be of greatest impact or serve the greatest need and then reward those companies with full-scale contracts. DoD must pick winners and losers, aligned with its strategic aims, focusing on providing growth ventures with longer funding runways, rather than one-time small awards.

At the same time, Congress should undertake a systematic assessment—akin to a Base Realignment & Closure (BRAC) processes—of legacy platforms to understand their future use and relevance and reallocate funding away from obsolete platforms to emerging threats and capabilities. According to the analogy, Programs of Record have grown to the size and scale of physical bases and have all the attendant political ramifications for terminating them. As with the volatile and dangerous politics of closing physical bases, only independent commissions are politically capable of euthanizing vast legacy programs consistently.

Access & Information: Past performance and security clearance requirements prevent most new companies from winning prime contracts, constraining the degree of innovation to which DoD has ready access. After demonstrating a prototype's efficacy, it takes Congress two years to approve funding, creating a "valley of death" of uncertainty few startups can survive and risk most investors won't accept. So far, only billionaire-backed ventures have successfully survived to compete with established primes, an unreachable standard. Both DoD and Congress must prioritize equalizing access to sustained investments through programs of record and better democratize security clearance protocols such that new companies can also compete on innovation.

Finally, both industry and government need to improve their relationship and mutual understanding through education, networking, human capital exchanges, and intentional collaboration. Think tanks, universities, public-private partnerships, and civil society associations will be important partners who can curate educational resources and interactive programming that increase the knowledge, spatial awareness, and networked capabilities of civilian innovators and servicemembers alike. Talent must flow more freely between these communities. New military education programs should be initiated that tie the China techno-security threat to concepts of innovation, digital transformation, national security, and geo-economics.

United States Posture Towards Allies & Rivals

"We have to be very, very clear-eyed and hard-headed [with China], and we've got to establish what I would call 'boundaries of trust'—areas in which we are very happy to engage and collaborate and areas in which we are not. And the best way, I think, to explain that to people—including Chinese interlocutors—is to just remind them that a threat is the combination of capability and intent. Capability takes a long time to put in place and intent can change in a heartbeat."

– Malcolm Turnbull, Former Prime Minister of Australia

"The first question I would ask is, 'Can you draw the Chinese industry, military, commercial, and academic innovation system?' Because if you can't, it's kind of hard to have a discussion of what we're competing with. It's what you'd ask your own startup: 'Who's your competitor? Name of company. Well, what's their business model?' I don't think we understand that deeply. Everybody who participates in this discussion, whether in startups, or funding, or DoD, step one is we need to understand: 'Who are we competing with, and how are they moving'?"

– Steve Blank, Professor, Stanford University

CIVIL-MILITARY INTEGRATION [MILITARY-CIVIL FUSION] COORDINATION AND IMPLEMENTATION SYSTEM, 2018

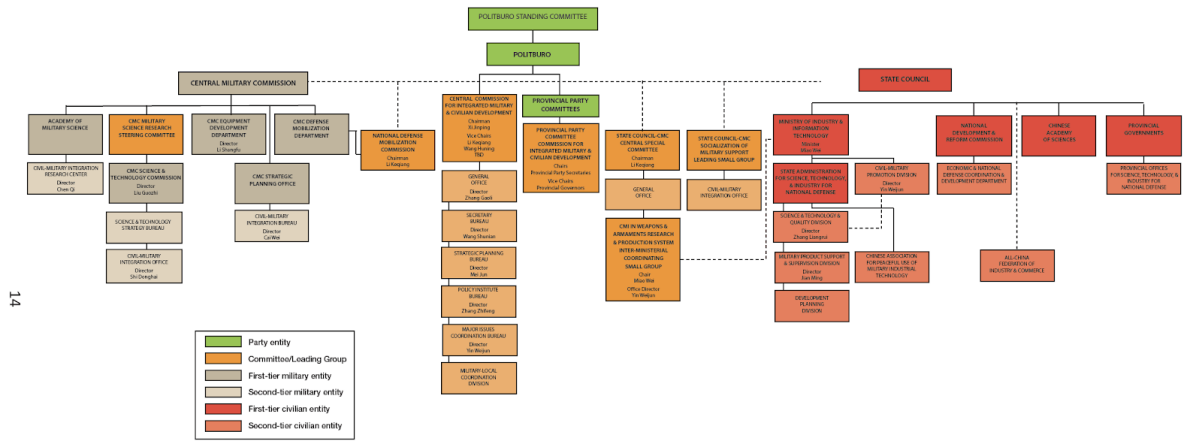


Diagram Source: Tai Ming Cheung. *Innovate to Dominate: The Making of the Chinese Techno-Security State under Xi Jinping*. Forthcoming.

Since the Cold War, the United States has assumed a significant technological overmatch against its adversaries; however, DoD's focus on conventional platform sustainment and cost-cutting has created openings for other great powers to rise. For thirty years, the United States pursued a strategy of engagement, encouraging China's rise with the expectation that it would become a "responsible stakeholder" in its foreign policy and less authoritarian in its domestic policy. That expectation has recently given way to pessimism, however, as China has grown more authoritarian at home and consistently sought to overshadow America's strategic geo-political advantage abroad, especially in the Indo-Pacific region and through China's broader Belt and Road initiative. In response, the United States' strategy has shifted from engagement to competition, heightening tensions.

In 2005, China began a series of economic plans designed to shape the development of its economy, including industrial policies to enhance its competitiveness in emerging technologies. China's ability to consistently fund, develop, and deploy emerging technologies with civil-military fusion rarely seen in the United States has granted China the power to lead in defining international norms as to how these technologies are deployed and ultimately weaponized. 5G should serve as an early warning: Huawei and ZTE are leading the global 5G market, with only Nokia and Ericsson offering viable alternatives, forcing the United States to pursue rearguard action to compete, pressuring other countries not to use equipment from Huawei and ZTE even though doing so may make the most commercial sense. Asking allies and partners to prioritize their security over the advantages of a rapid 5G rollout puts them in a dilemma, making the task of developing a coordinated strategy toward China's rise that much more challenging.

In a pessimistic scenario for allied democracies, China's ascendance in emergent technology could lead to a future in which China greatly expands its ability to project authoritarian power around the world. The lack of political will due to ideological factionalism undermines America's ability to effectively face its geopolitical rival. The United States must respond to China's strategy of civil-military fusion in a way that is consistent with its support for democratic values and free markets and in so doing, build political will and global partnerships that ensure allied democracies retain a global advantage in the world order.

> ***"You must have a strategy to win. And it turns out that there's a set of technologies which are strategic which China has indicated they want to dominate and that we have either not focused on or we're losing on and so forth. We have to agree on that list and then we have to do whatever it takes to catch up."***
>
> *– Eric Schmidt, Former CEO & Executive Chairman, Google // Co-Founder, Schmidt Futures*

Sustaining long-term strategic competition with China demands consistency and unity of purpose—at home, in our alliances, and in our international partnerships—that enables a "virtuous, democratic" response to China's strategy of civil-military fusion. Systematic improvements in the relationship between industry and DoD outlined above will go a long way towards improving the U.S. strategic posture towards its rivals. In addition, the United States should consider more aggressive industrial policy and coordinated efforts to build political will.

Industrial Policy: The top-down model of economic planning that China has adopted is most effective when a country is trying to catch up in its economic development: benchmarks can be identified, and targets can be established, when a country is trying to absorb technologies that have already been created and proven elsewhere. When competing on the technological frontier, a bottom-up approach to industrial policy—in which DoD defines target outcomes and serves as a fast follower of technologies developed in the commercial sector—is more appropriate.

Its civil-military fusion enables China to quickly and effectively develop and deploy new technology. The U.S. should evaluate how to employ industrial policy to achieve a similar result. Adopting an industrial policy, however, need not mean becoming less democratic or less American. Democratic capitalism enhances not only U.S. prestige and leadership in the world, but also its ability to adapt to new challenges. This would not be the first time the U.S. has employed industrial policy to address strategic concerns. The United States practiced economic planning during the New Deal, during wartime mobilization, and during the Marshall Plan; these efforts employed considerable cooperation between the military, the private sector, and academia for much of the Cold War. DoD already practices some degree of industrial preference in how it relates to prime contractors. By formalizing a strategic vision for the technological capability of the United States as a great power, Congress can provide DoD with much greater flexibility to invest in and deploy strategic capabilities that have not yet been developed.

Political Will: To sustain political support for DoD's investment in and procurement of new commercial technologies, the public needs to understand the nature of the challenge that the United States faces. Public hearings about the pace of China's technological advances and their ethical implications will be vital in helping U.S. and allied citizens understand the degree of the threat the U.S. faces. A coordinated public engagement campaign on this topic should effectively employ events, multimedia, and op-eds about how leadership in strategic technologies will shape the future of global leadership for allied democracies. Partisan differences between Democrats and Republicans has up to now yielded disagreement on the appropriate U.S. posture towards China, one compounded by the circumstances of the COVID-19 pandemic. Moving forward, it will be vital for political leaders to adopt a "country first" mentality, setting aside their domestic differences in order to do what it takes to ensure the U.S. retains its global position.

Global Partnerships: The digital revolution has accelerated global interconnectedness that affects U.S. dependence on our allies and partners. Instead of treating all foreign powers equally, the United States would benefit from strategic global partnerships with democratic allies and international corporations. While industry has a critical role to play in these partnerships, DoD and the U.S. government have a natural leadership role. Defined outcomes and priorities along with industrial policy can and should be used to focus these efforts.

DoD must also clarify its position on international collaboration especially when it comes to "trusted capital," where it has so far failed to define the far limits to international participation on defense-focused investments. The U.S. is the largest capital market by several orders of magnitude. With clearer market signals from Congress and DoD, this resource can be directed to solving national security problems for not only U.S. companies but also for our allies and partners. The unique relationship across defense, academia, capital markets, and governments make the "Five Eyes" an obvious starting point for these efforts. Any efforts DoD makes to leverage private capital should include a path to open collaboration with these countries. Quantum computing, 5G, space, and autonomy are among the vital technology areas that would benefit the most from allied collaboration.

Evolving Defense Personnel, Platforms, and Processes

> ***"The Department of Defense is actually moving fast; it just doesn't move at the speed you're used to. And we have to convince the Department of Defense that they can move faster."***
>
> *– Bob Work, Former Deputy Secretary of Defense*

DoD is the largest employer in the world with nearly 1.3 million servicemembers, some 800,000 National Guard and reservists, and more than 700,000 civilians. The U.S. Navy boasts 11 of the largest aircraft carriers in the world, each housing 80 fighter jets. The U.S. Air Force retains more than 2,400 combat aircraft, in addition to hundreds more support, reconnaissance, and training aircraft. The U.S. Army sustains close to 6,400 tanks for ready deployment. This conventional force position is unmatched by any other country in the world, yet comes at a hefty price, not only in terms of the cost to sustain it, but the opportunity cost of considering new operational concepts and technologies. Retaining such a dominant legacy posture has made it challenging to fully shift DoD's focus to the full range of digital capabilities this moment demands. Not only does this legacy force absorb all our budgetary resources, it also consumes most of our intellectual energy and imagination.

Most experts agree that the gravest threats of the 21st century will be digital rather than conventional, challenges for which this legacy force is underprepared. While the U.S. government seeks to improve and streamline its relationship with industry and realign its strategic posture towards allies and rivals, DoD itself must undertake a series of transformations to position the organization and its workforce for new threats and a fundamentally altered business context. DoD must fundamentally rethink talent management and training;

platform development and deployment; and the processes for requirements, acquisition, budgeting, and testing.

> ***"SOCOM has additional authorities, but for the most part, they live under the same federal acquisition regulations that everybody else does. The real difference is the culture that permeates SOCOM and the ability to make decisions at their level. It is a very innovative and mission-oriented culture. There is a huge focus on bottom-up development. One of the areas where SOCOM was very successful was linking technologists with operators and closing the loop on development and technology employment."***
>
> *– GEN Joseph Votel, Former CENTCOM and SOCOM Commander // CEO, BENS*

Adaptive Human Capital: Over the last decade, DoD has permitted a culture of risk-aversion and cost-sensitivity, encouraged by the sequestration of 2013, which has rewarded choices perceived as safe. The myopic focus on preserving program stability in legacy programs with hyperspecific – and often obsolete – requirements blinded DoD to the digital revolutions unfolding in industry such as agile software development, cloud computing, enterprise scale data, automation, AI and machine learning, and 5G. To address this deficit, DoD must invest in educational programs that instruct personnel in experimental and innovative mindsets, adoption and adaptation of commercial technology, and effective frameworks for assessing and accepting risk more holistically. While the U.S. military has long prided itself on fielding a force of generalists who can be trained for any mission, service members must be empowered to specialize in fields of emerging technology, and the military must expand its community of highly qualified experts who bring extensive technical experience and expertise. Of the 700,000 civilians DoD employs, only about 20% are in STEM occupations. To meet the digital threat posed by its rivals, DoD will need to expand significantly its computer engineering workforce. In order to afford these investments in human capital, DoD should consider the full power of automation to improve outcomes and reduce headcounts allocated to mundane tasks. People drive system change. To accelerate the cultural changes required, DoD should ensure its workforce is equipped with the education and technical training they need to meet the challenge, in addition to a clear understanding of industry trends.

Intelligent Platforms: Since the Cold War, DoD has grown accustomed to bespoke platform development. During that time, the digitization of industry has allowed market-driven technologies to surpass bespoke solutions in both functionality and affordability, yet DoD has continued to favor custom solutions. Often, only lawsuits by industry disruptors forcing DoD to comply with the law, which requires the U.S. government to prefer existing commercial solutions to bespoke tools, has been able to shift this entrenched behavior. Instead of using requirements to define the parameters of acquisition, DoD could incentivize teams to find, test, and deploy existing market solutions. To make room for new, disruptive technology, defense leadership and legislators must divest themselves of legacy programs. In 2019, the U.S. Army instituted a review process informally called "Night Court" that allows for a strategic view of the current programs. This process should be expanded across DoD. The savings made can then be applied in more agile methods inside of the traditional budget cycle.

Simultaneously, DoD must prioritize the development of digital capabilities in critical technologies, both within and beyond its legacy conventional platforms. It must speed the process by which an emerging technology can become a program of record, and must ensure its capabilities are not only centralized but also distributed. DoD must create transparent pathways for technology testing and deployment that ensure their integration into centralized systems and their utilization based on the specific needs of certain segments of the ecosystem, moving rapidly and reliably from pilot to scaled utilization.

Responsive Acquisition & Development: The DoD requirement-based acquisition system is antiquated and is no longer competitive in the digital age; it is based on requirements that assume DoD can outline the solution

to problems two, five, or ten years in advance.This system must be updated to incentivize outcomes over requirements, capabilities over platforms, and solutions over “manpower for the problem.” In favoring bespoke solutions, DoD has habituated “linear” procurement cycles: requirements are defined, a platform is produced, and DoD supports the costs of sustainment. Yet, over the last decade, lean, cyclical methods of development have disrupted industry, allowing the private sector to continuously iterate and evolve the solution it offers its customer, especially its digital tools. To achieve a competitive advantage, DoD must integrate such cyclical, adaptive approaches into its cycles of development, ensuring that any platform developed today can be effectively updated on an on-going basis to deliver best-in-class digital capability. Such an approach can begin with a resolution by DoD to securely “publish the problems” it needs to address and offer incentives for companies to develop holistic solutions.

Finally, DoD should remove or deprioritize the prior performance metric that gives outweighed credit to DoD’s prior contractors. This metric gives companies with long contracting histories an advantage over disruptive tech companies, regardless of the legacy performers experience in a new technology area. By eliminating prior performance on technology-centric bids, DoD will open itself to greater access to innovation and capability.

Conclusions

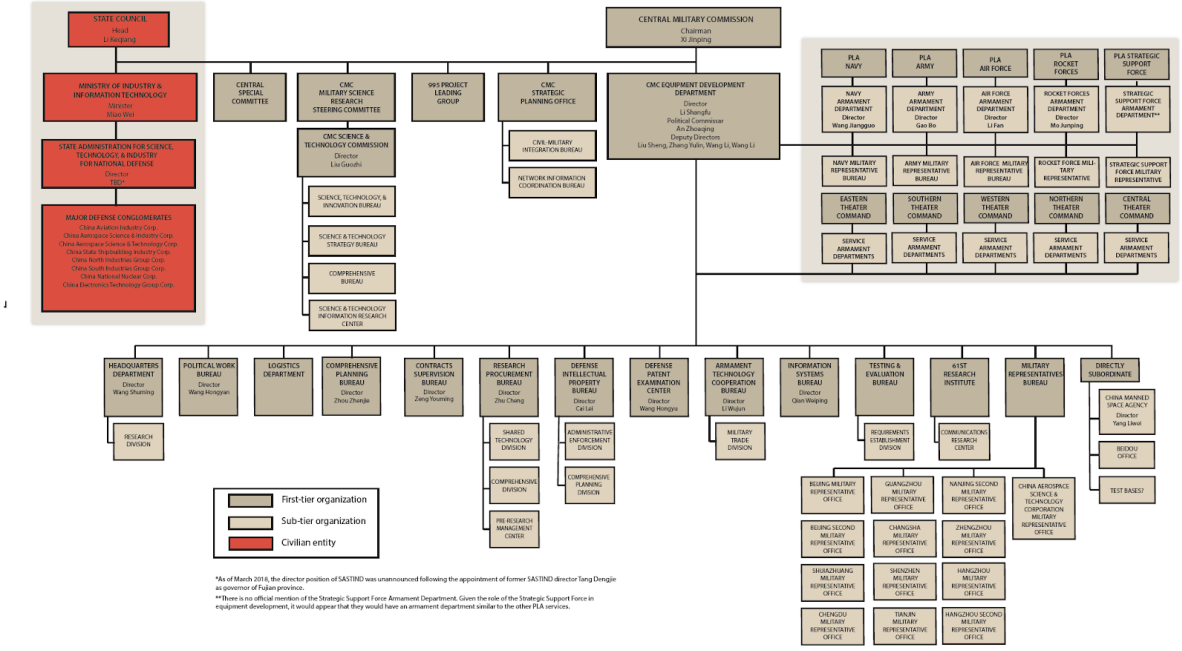
To effect the systemic changes recommended here, several key actions can restore America’s techno-security position. Foremost, Congress must provide a clear vision for the future. By formalizing a strategic industrial policy vision for the technological capability of the United States, Congress can provide DoD and the private sector with a greater ability to invest in and develop new strategic capabilities that will allow the United States to more effectively compete with China. To accelerate these efforts, Congress should allocate a meaningful tranche of money (such as 20% of the topline budget) that will enable DoD to proactively invest in promising new technologies and account for that spending retroactively.

Concurrently, DoD must offer clarity to new potential industry partners by clearly framing the operational problems it seeks to solve and the outcomes it hopes to achieve. Publishing operational problems and target outcomes can serve as market indicators that encourage private investment in early stage companies and capabilities. While some critics have voiced concerns about the declassification of these challenges providing insights to America’s rivals, in truth their classification hinders domestic innovation far more. At the same time, DoD must pivot away from its historical focus and inherent bias towards bespoke hardware, updating its acquisition system to incentivize digital tools that effectively meet DoD’s biggest challenges, even if the deployment of such tools makes existing personnel and systems obsolete. To meet the digital threat posed by its rivals, DoD will need to transform its internal culture towards new technologies by both significantly expanding its computer engineering workforce and training its service members on effective technology development and deployment.

Lastly, both industry and government leaders must seek to rekindle the culture of collaboration that accelerated U.S. defense dominance post-WWII. The efforts outlined above will assist in this goal, but deliberate attention must be given to the fostering of this culture. Strategic efforts towards education, networking, and intentional collaboration among policymakers, civilian innovators, and military personnel will generate the conditions for sustained progress.

Appendix:

CHINA'S ARMAMENT AND TECHNOLOGY DEVELOPMENT APPARATUS, 2018



Acknowledgements: The SVDG 2020 Techno-Security Roundtable series was made possible by the support and coordinated efforts of numerous parties. The University of California Institute on Global Conflict and Cooperation, based at UC San Diego, provided our virtual meeting space; James Lee and Ian Brown from the IGCC research team assisted with documenting and codifying these proceedings. We are grateful to Alicia Bonner Ness for her diligent coordination for the roundtable series and her tireless efforts compiling this report. The roundtables would not have been nearly as impactful without the expert moderation by Joshua Marcuse.

Finally, SVDG would like to thank Representative Mac Thornberry for his leadership and support to our organization. SVDG wishes Representative Thornberry and his family a happy and well-earned retirement after 25 years in Congress.