[H.A.S.C. No. 116–48]

THEORIES OF VICTORY—INNOVATIVE CONCEPTS FOR NATIONAL SECURITY

HEARING

BEFORE THE

FUTURE OF DEFENSE TASK FORCE

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

HEARING HELD
OCTOBER 29, 2019

U.S. GOVERNMENT PUBLISHING OFFICE
40–506 WASHINGTON : 2020

FUTURE OF DEFENSE TASK FORCE

SETH MOULTON, Massachusetts, *Co-Chairman*
JIM BANKS, Indiana, *Co-Chairman*

SUSAN A. DAVIS, California
CHRISSY HOULAHAN, Pennsylvania
ELISSA SLOTKIN, Michigan
SCOTT DESJARLAIS, Tennessee
PAUL MITCHELL, Michigan
MICHAEL WALTZ, Florida

LAURA RAUCH, *Professional Staff Member*
ERIC SNELGROVE, *Professional Staff Member*
RORY COLEMAN, *Clerk*

CONTENTS

THEORIES OF VICTORY—INNOVATIVE CONCEPTS FOR NATIONAL SECURITY

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
FUTURE OF DEFENSE TASK FORCE,
Washington, DC, Tuesday, October 29, 2019.

The task force met, pursuant to call, at 10:02 a.m., in room 2118, Rayburn House Office Building, Hon. Seth Moulton and Hon. Jim Banks (co-chairmen of the task force) presiding.

OPENING STATEMENT OF HON. SETH MOULTON, A REPRESENTATIVE FROM MASSACHUSETTS, CO–CHAIRMAN, FUTURE OF DEFENSE TASK FORCE

Mr. MOULTON. Good morning. This hearing will come to order.

I would like to welcome our task force members and the witnesses testifying before us today. This is the inaugural hearing of the Committee on Armed Services Future of Defense Task Force. I ask unanimous consent that non-task force members be allowed to participate in today's hearing after all task force members have had the opportunity to ask questions.

Is there any objection?

[No response.]

Mr. MOULTON. Without objection, the non-task force members will be recognized at the appropriate time for 5 minutes each.

The United States faces a diverse, fast-changing range of national security threats, nearly unprecedented in their breadth and pace of change. And we need to understand them better. As we enter a new decade, it is time for a new generation of thinking about these challenges and how Congress and the country can meet and defeat them.

Great power competition from Russia and China, which are rapidly advancing next-generation warfighting capabilities to leapfrog our legacy systems, is real. We have not seen a dual threat like this since the military surge of Germany and Japan in the 1930s. At the same time, the threat of transnational terrorism persists.

Sun Tzu said, "the supreme art of war is to subdue the enemy without fighting."

In 1938, Mao Zedong wrote, "Whoever has an army has power, and that war decides everything."

Over hundreds of years, both Sun Tzu and Mao's influence still guide Chinese policy. Currently, the People's Liberation Army is the largest military force in the world, and China is rapidly modernizing its arsenal while expanding its military footprint globally. Its ambitious soft power endeavor, the Belt and Road Initiative, has invested in the economic development of more than 100 coun-

tries, and made inroads across Asia, Africa, and South America with major economic and infrastructure projects.

In an attempt to recapture Soviet power and glory, Russia is increasingly aggressive in Europe, the Middle East, and the Arctic, and is ramping up its ability to challenge the United States and its security partners across multiple warfare platforms, to include conventional and strategic weapons. Its well-known information exploitation and cyberattacks against U.S. civilian and military targets continues today.

The return of nationalism in Europe threatens to weaken NATO [North Atlantic Treaty Organization] and destabilize the European Union, and embolden Iran who is wreaking havoc in its neighborhood through overt military action and backdoor proxy alike.

North Korea continues its march toward full nuclearization. And violent extremists and transnational criminal organizations continue to cause upheaval globally.

For its part, the United States remains mired in divisive politics at home and conflict abroad, while our adversaries build and expand their war machines in ways that seemed unimaginable just a few short years ago. Warcraft of the future will increasingly rely on electronic sabotage where adversaries seek to disrupt and disable our systems and networks before any fighting begins.

As they once again demonstrated this weekend in the raid to kill Abu Bakr al-Baghdadi, our warfighters and intelligence services are unrivaled in their skill and professionalism. But how do we ensure we're training and equipping them for success on the asymmetrical battlefield of the future?

Each year this committee passes a defense bill. It is hard and important work. But in terms of budgets and policy, it only takes us a few years forward. We need to ask what should our fighting force look like in 2050, or even 2075? Our adversaries are asking themselves this question. And it is this committee's job to start asking that question, too.

Right now our government and entrepreneurs within our country are developing sophisticated technologies: artificial intelligence, robotics, autonomous systems, 5G, quantum computing, and biotechnologies all offer tremendous opportunity for social transformation, yet remain ripe for nefarious exploitation. Our rivals will weaponize these systems. They have already started.

In 2017, China announced, along with its plan to become a global superpower by 2050, its "new generation artificial intelligence development plan," and set the ambitious goal of becoming the world's leading power on AI [artificial intelligence] by 2030. The Chinese have been unequivocal in their intent to develop it for military use. And as we meet here, they are spending billions trying to figure out how.

We cannot cede the advancement of these emerging capabilities to our rivals, because the country that wins this race will write humanity's values. So, we must lead in the technological breakthroughs that will define our time.

Article I of the Constitution clearly delineates Congress' responsibility for our national security. We must work to ensure the Department of Defense is freed up to be more agile and focused on

the needs of the future. Fundamentally, it is on our backs to ensure our young warfighters never enter a fair fight.

Our task force mandate to review U.S. defense assets and capabilities and assess the state of the national security innovation base to meet emerging threats and ensure long-term strategic overmatch of global competitors demands asking tough questions of the Pentagon and of ourselves. We will seek knowledge from longstanding experts, like those before us today, and from unlikely sources, and we will build on the significant work that has been done by the subcommittees.

We will look at ways to supercharge innovation, to improve the pipelines of ideas, technologies, and personnel into our military, and to make tough political decisions that guide the development of our force of the future. We look forward to providing the American people with our findings.

I would like to thank Chairman Smith and Ranking Member Thornberry for supporting the creation of this task force. And I want to recognize my fellow task force members who are joining me in this undertaking, and thank them for their willingness to serve in this important endeavor.

With that, I would like to turn to my co-chair, Congressman Jim Banks of Indiana.

OPENING STATEMENT OF HON. JIM BANKS, A REPRESENTATIVE FROM INDIANA, CO–CHAIRMAN, FUTURE OF DEFENSE TASK FORCE

Mr. BANKS. Thank you, Seth.

I would like to, as well, start by thanking Chairman Smith and Ranking Member Thornberry for establishing this bipartisan Future of Defense Task Force. We have been chartered to review U.S. defense capabilities and assess the state of the national security innovation base to meet emerging threats and the rise of global competitors. It is a vitally important task, and one that I do not take lightly.

I would also like to thank my co-chair Congressman Moulton. I look forward to working with you and the other members of the task force.

And welcome to our witnesses. I cannot think of two more qualified individuals to be here with us today as we kick off this task force. Thank you, Ms. Flournoy, and special thank you to Senator Talent, who I had the privilege of serving with on the Reagan Institute Task Force on Innovation and National Security. It is good to see both of you again.

This task force's mandate underpins the foundations of our competitive advantage as a nation. How will we prioritize research and development, harness emerging technologies, sustain an innovation ecosystem, and rapidly field new capabilities to deliver them into the hands of our warfighters.

The qualitative edge over our rivals is dwindling, and we can no longer afford to take for granted the military dominance that we have enjoyed. China's whole strategy approach, amplified by double digit annual growth in their research and development spending, and frequent malfeasance, intellectual property theft, cyber intru-

sions, and espionage have propelled their defense science and technology efforts.

And while China's rise is a significant example, much of the challenge that we face today has to do with our own ability to create and sustain a domestic national security innovation base. We must address fundamental aspects of our domestic innovation ecosystem by, first, increasing the pipeline of domestic STEM [science, technology, engineering, and math] talent; improving and expanding the infrastructure that will keep us competitive in fields like hypersonics, quantum information sciences, and 5G; removing impediments to innovation, and speed the adoption of commercial technologies; and, creating more opportunities for collaboration and shared experiences between the defense community, policy makers, and private sector technologists.

As we build a blueprint for the future of defense, we must ensure that it has been informed by engagement from this one today, with input from industry, academia, and government. We must embrace our role in not only the development of new technologies, but also as the global leader in the responsible use of these capabilities and counternarrative to China. We must elevate the public conversation surrounding the health of our national security innovation base, and what action is required to meet emerging threats and the rise of global competitors.

In the end, we must ensure all Americans understand the true cost of inaction.

I look forward to hearing from our witnesses today. And with that, I yield back.

Mr. MOULTON. Thank you, Jim. Glad to be here with you and the rest of the task force. And it is truly an honor to have our witnesses here today. So, I am pleased to recognize them.

And, Ms. Flournoy, we will begin with you with your opening statement.

STATEMENT OF MICHÈLE A. FLOURNOY, CO–FOUNDER AND MANAGING PARTNER, WESTEXEC ADVISORS

Ms. FLOURNOY. Thank you so much, Chairman Moulton and Chairman Banks and our distinguished members of the task force. It is truly an honor to testify before you. And I really applaud this effort to focus on the critical challenge of preparing the Department of Defense and the national security innovation base to meet emerging long-term threats.

As has been mentioned, the resurgence of great power competition, combined with an unprecedented pace of technological disruption, requires the United States to reimagine how we deter and, if necessary, fight and prevail in a future conflict. Central to this challenge is ensuring that the U.S. military retains its operational and technological edge over a revanchist Russia and, particularly, a rising China.

America's military advantage is rapidly eroding in light of China's and, to a lesser extent, Russia's military modernization efforts. In fact, if we stay the current course, a rising China will likely achieve overmatch in a number of key capability areas, calling into question our ability to credibly deter, defend, and prevail in any future conflict at acceptable levels of cost and risk.

At the core of this military challenge is the substantial investment made by China and Russia in so-called anti-access/area denial capabilities. These mean that the United States can no longer expect air, space, and maritime superiority early in a conflict. We will need to fight to gain that superiority and then to maintain it in the face of ongoing efforts to disrupt and degrade our battle management networks. Beyond these capabilities, China is investing, as was mentioned, tens of billions of dollars in a directed technology roadmap in key areas from hypersonics to robotics to quantum computing to artificial intelligence and machine learning.

Indeed, the primary competition on which the United States must focus in my view is the tech race with China. Thanks to Beijing's doctrine of civil-military fusion in which any commercial or research-based technological advance that has military applications will be shared with the PLA [People's Liberation Army], the Chinese military has made rapid advancements in AI and machine learning in particular. Given the centrality of emerging commercial technologies like AI, quantum computing, 5G, autonomous systems, and robotics, ensuring that the U.S. military keeps its edge means that we have to have our answer to civil-military fusion. I am not suggesting that we act like the Chinese, but we need to have our own answer, and soon.

In addition, both Russia and China have paired these technological investments with doctrinal innovations. Russia is rapidly modernizing its nuclear arsenal to support its "escalate to de-escalate" doctrine. And with the Trump administration weighing a new START [Strategic Arms Reduction Treaty] renewal in the wake of our withdrawal from the INF [Intermediate-Range Nuclear Forces] Treaty, I feel that the United States and Russia are on the precipice of an alarming period of strategic instability.

Meanwhile, China, for its part, has a theory of victory that is increasingly relying on what they call systems destruction warfare, which is an effort to take out and cripple an adversary's networks at the outset of conflict, deploying sophisticated electronic warfare, counter-space capabilities, cyber capabilities to disrupt our critical C4ISR [command, control, communications, computers, intelligence, surveillance, and reconnaissance] networks, thwart our power projection, and undermine our national resolve. This means that the United States, again, can no longer take space for granted as an uncontested domain. In the future, space will be a domain through which and from which we project power.

Nonetheless, given the reluctance of major powers to enter large-scale conflict with the United States, in the near term we are much more likely to see Russia and China pose challenges in the grey zone at the level below conventional armed conflict. We can expect them to focus on trying to unilaterally and incrementally alter the status quo in their favor using economic, diplomatic, and military coercive means to achieve their objectives.

I think the National Defense Strategy of 2018 provides a critical strategic framework for addressing these mounting challenges, and reflects a growing sense of urgency among the Department's leadership about our eroding military advantage. If you look at the 2020 budget that Congress has supported, you also see bipartisan commitment to ensuring that we invest in the technology and capabili-

ties that we need to implement our strategy in the face of a more contested period of great power competition.

However, the current budgetary environment, and I think what we can project for the future, will require us to make some difficult trade-offs to buy down risk in the future. The central question for this task force and the committee is how do we invest our defense dollars wisely? And how do we invest with the speed and effectiveness required to keep our edge, given the speed with which our potential adversaries are moving.

In the near term, I believe the Department must make reestablishing credible deterrence our central objective. While, again, I don't believe the United States or China or Russia, all nuclear powers, would deliberately start a war, given the dire costs involved, we could nevertheless stumble into conflict if an adversary were to miscalculate either our resolve or our capabilities. I think this risk is greatest in the next 10 years, when the United States has telegraphed its vision for the future force but is yet to procure and deploy all of the systems necessary to fully translate that vision into reality.

To prevent miscalculation or escalation to conflict with a nuclear-armed rival, I think we have to decide what are the capabilities we need to prioritize developing, acquiring, and demonstrating in order to credibly deter aggression either through denial of an enemy's objectives or through the ability to impose crushing costs for any act of aggression.

And, again, I think we need to think in two timeframes. First, what do we need in the next 5 to 10 years, which is largely cobbling together current capabilities in new ways? And what do we need 10 years and beyond for a very different future? We need to think creatively about how we can deter, prevent a great power rival from starting down the road to war. This means we have to—DOD [Department of Defense] should devote considerable effort to conceptual—concept development and war games to develop a suite of interim deterrence approaches, again using existing capabilities in new ways to dissuade aggression.

The fact that several countries around the world are questioning U.S. commitment and resolve means that we also have to do a better job of clarifying our policies about what we will defend, and make sure that our words and messaging, our budgeting, all send a consistent message to, again, strengthen deterrence and shake the risk calculus of any nation who would consider using force to pursue their ends.

We also need a strategic framework to guide whether and when and how we reveal new capabilities to bolster deterrence, and when we keep them in reserve and highly secret.

So, I am conscious of time, but I want to highlight six areas where I think we need to focus our efforts.

First, the DOD needs to implement a series of acquisition, investment, and workforce development reforms to foster the innovation ecosystem that Representative Banks talked about. This is essential to maintaining our military edge.

First and foremost, the DOD has not adequately trained or incentivized its acquisition workforce to employ the authorities that Congress has provided them at scale, more flexibility authorities.

There are pockets of excellence, like SOCOM [U.S. Special Operations Command] and the Air Force, but the bulk of the acquisition corps is not using authorities like OTAs [other transaction authorities], 804, even SBIRs [Small Business Innovation Research], and so forth. As we prioritize procuring software and network capabilities to enable the future joint multi-domain operations, we need an acquisition cadre that is trained and rewarded for rapid and agile development of new technologies.

Second, we also need top-down leadership to provide strategic direction and top cover to pursuing more ambitious goals. I would love to see the Secretary of Defense set an audacious goal for each of the services to say by the end of the FYDP [Future Years Defense Program] we want to see new force units that are focused on human-machine teaming, that are leveraging AI, machine learning, robotics, et cetera. We want to field those, the first of those units by the end of the FYDP to give the service some very concrete goals to work towards.

In addition, various service units like DIU [Defense Innovation Unit] and SOCOM are playing very important tech scouting roles, but there remains what I call the valley of death between having a successful demonstration of prototype and actually getting a spot in the program of record. You know, if you are a small commercial technology company, you often find that valley of death impossible to cross. So we need to accelerate reform efforts to enable that transition.

One approach would be for Congress to authorize more flexible bridging funds that services could allocate on a competitive basis to sustain capability development in that period between prototyping and actually getting a spot in the program of record. Happy to talk about that in more detail.

The point about tech talent. The Department currently lacks the tech talent—senior and junior, civilian and military, Active, Reserve—to develop, integrate, and deploy critical emerging technologies. We need to expand scholarship for service programs beyond cyber to a much broader range of STEM fields. We need to be recruiting mid-career tech talent by expanding scholarships and opportunities for people to come from the tech community into the Department to serve, and vice versa. And we need to be doing a lot more upscaling of the current workforce into technology areas, providing tech talent with viable promotion and career paths in service.

Second big basket is the Department needs to ramp up its efforts to develop joint and service-specific operational concepts to drive more rapid fielding of game-changing technologies.

The United States needs to urgently develop and test joint concepts like multi-domain operations and supporting service concepts. And we need to be testing the technologies that will be most critical to operationalizing these, requiring a continuous reinforcing cycle of war gaming, prototyping, and experimentation.

To do so, Congress has to provide the services with more robust funding to field small numbers of emerging capabilities for early-stage concept development and experimentation. Right now we are sort of in a catch-22 position where, you know, the Navy will come and say I need a handful of undersea unmanned vehicles to experi-

ment with, and play with, and develop a fleet concept. And the Congress will say, well, no, we can't really give you the money—or certain committees, not this one—will say, you know, we can't really give you the money until you have all the concept worked out. So, you are in a catch-22: they need the technology to develop the concept; if you don't have the concept you can't get, you know, get the technology. We need to break that logjam, take a little more risk in the future if we are going to be able to develop new concepts and capabilities fast enough to keep pace with potential rivals.

I think we also similarly need robust concept development and war gaming to look at how existing platforms can be used in new ways to shore up key capability gaps. This is exactly the sort of critical bridging work that the Strategic Capabilities Office, or SCO, was doing before it was moved under DARPA [Defense Advanced Research Projects Agency]. The Department needs a SCO-like office to drive these efforts, to shore up deterrence and our operational edge in the near to mid term. And I think this move to DARPA will undermine that capability.

Third, the Department should adopt best practices and lessons learned from the commercial technology sector about agile development and program management. We are, you know, the Department has very ambitious goals to migrate to the cloud, leverage large data sets for artificial intelligence, build interoperable multi-domain networks at scale. The Air Force is moving out smartly and building an Advanced Battle Management System which is really the long pole in the tent for multi-domain operations.

And I have been very impressed with how that effort has been organized.

But we need to do a better job of integrating private sector approaches to technology development, data management, network security. And, again, we can go into the details of that in Q&A [question and answer] if you are interested.

Fourth, I think that budget realities over time will require us to make tough trade-offs between legacy platforms and critical new technologies. Currently, while we have made some progress, I believe the United States is still underinvesting in the new technologies that will ultimately determine our success in the future security environment, and overinvesting in legacy platforms. This is a recipe for failure.

In order to make the trade-offs necessary, we have to answer a fundamental question for every major program of record: Where is the knee in the curve? Where is the point where it makes more sense to forgo the n+1 platform, aircraft carriers, you know, fighter aircraft, tanks, whatever the major program may be, and instead of taking that one additional platform, take that money and invest it in the capabilities that will make sure that the rest of that fleet is survivable, has the range, has the relevance, has the combat effectiveness for the future security environment.

To me, the SECDEF [Secretary of Defense] should be asking each service those tough knee-in-the-curve questions, and be willing to make those hard choices to prepare for the future fight. And Congress has to support those hard choices, as hard as those are. Because sometimes we are going to have to, you know, decrease or

stop buying some legacy systems in order to make the reinvestment we need in the technologies that will make the difference.

Fifth, we need to adapt our overseas posture and our security cooperation programs to make them much more effective, and leverage the strategic value that our partners and allies bring to the table. Again, we can talk about that in the Q&A if you are interested.

And, finally, I think we need to, again, focus not just on the extreme long term but also shoring up our capabilities in this critical decade for deterrence.

So, in summary—and I am sorry I have gone on so long, but I am passionate about this issue—you know, we are really at a critical juncture. I call it, you know, this is a moonshot moment for the United States. We need national leaders with a vision. We need an urgent call to action. And we need a far more robust and focused investment in the drivers of our competitiveness. That includes research and development with a focus on critical dual-use technologies; STEM education; 21st century infrastructure like 5G; incentives for enhanced collaboration between government, business, and academia; and we didn't coordinate our comments in advance, but many of the things you mentioned.

And speed is of the essence here. The actions we take in the next few years could not be more critical. We also need to be, our vision needs to be informed, as you mentioned, Representative Moulton, by our core values and the interests that we seek to protect.

I believe the United States must maintain our global leadership role as a force for good, a defender of democracy and human rights and the rules-based international order. We need to make sure that our economy remains the most innovative and dynamic in the world, because that is the foundation of both our global influence and our national security. And we need to be leveraging all national security instruments, not just the military, to achieve the ends we've talked about this morning.

So, let me stop there. And look forward to your questions.

[The prepared statement of Ms. Flournoy can be found in the Appendix on page 33.]

Mr. MOULTON. Ms. Flournoy, thank you very much. That was a lot but we have a lot to discuss here. So, we are grateful for your wisdom and insight, as always, before this committee.

Senator Talent, over to you, sir.

STATEMENT OF HON. JIM TALENT, CO–CHAIR, REAGAN INSTITUTE TASK FORCE

Mr. TALENT. Thank you, Mr. Chairman. It is a pleasure to be here, and with Secretary Flournoy. I mean that in all sincerity; I never listen to her without learning something. And we served together on the 2014 QDR [Quadrennial Defense Review], and that was a very instructive process.

I, too, want to congratulate the committee chair, chair and ranking member for establishing this task force which, in my experience with the committee, goes back 25 years, on it part of the time and around it part of the time, I can't think of a precedent like this. I am still at heart a former member. So, from your perspective, what I thought when I heard about it was, oh great, another com-

mittee assignment. Right? Because it is not like they are going to let you off the markup or the other things you have to do to serve on this.

But I think it is very important. It shows your understanding, as the Secretary was saying, we are now firmly in a new era. We have emerged from the post-Cold War era now into something else, which I think is going to be dominated—I think there is a consensus on this—it is going to be dominated by great power competition. There are, of course, other threats. And you all and the government has to walk and chew gum at the same time, right? And innovation is going to be key to everything.

But when you look at great power competition—and by the way, we started moving into that era in the Obama administration with the pivot, with the rebalance. We see it now with the National Security Strategy. And I think it is going to continue for many administrations in the future. I think this is generational, which is why the Reagan Institute formed a task force on the national security innovation base. And that is, I am sure, the reason why you have invited me. I am co-chairing that with Secretary Work, who knows a lot about the Department's approach to innovation.

So, we agree that innovation is going to be the key to the success in the competition. Now, capacity is also important, numbers matter, and they will continue to matter. But—and the Chinese understand this also. We and they recognize the better innovator is likely to win and have success in that competition. And they are the pacing challenge in the sense that they are the closest to a peer competitor. I think in certain respects they are a peer competitor. In certain respects they may be outrunning us in this.

And, also, because if we are prepared to deal with the challenge from China then I think it means we are probably also going to be prepared to deal with competition from Russia, and even Iran and the rest of it.

Now, I have four observations drawn from our experience on the task force that anticipates some of what we are going to have in our report, which should come out in the next month or so. And by the way, thanks to Mr. Banks and also Mr. Kim, and Mr. Gallagher, and Ms. Murphy for serving on the task force and contributing to that. So, they kind of have a head start on this national security innovation base stuff.

So, four observations for you all, from your side of the table.

So, as you do this task and approach this task get clear in your own mind and a common understanding as a group of what the national security innovation base actually is. So, we spent a whole session discussing this. And Mr. Kim gave us I think the word that you are going to see a lot in our report: it is an ecosystem. It is enormous. It is pulsating. It is chaotic in a lot of respects. It is characterized by dynamism, a very risk-positive culture. And it has changed a lot from the national security innovation base in the Cold War.

There are some similarities. The public actors are largely the same. The Department of Defense, the intelligence agencies, the National Labs, they are still in the national security innovation base. We still have universities attached to it.

But now, a huge part of the base, in fact the dominant with regard to certain technologies, are private sector actors primarily in the for-profit tech community who are pursuing dual-use innovation that is of vital importance to the national security of the United States but who, you know, who are pursuing it for their own purposes. They are perfectly legitimate, largely commercial purposes. These actors have little or no experience dealing with the government, and the culture of the government, and the regulations of the government, and the procurement processes of the government. And they are often not even aware of the national security implications of their work.

So, your task is basically, I would approach it this way, it is to coordinate, to direct, and empower the national security base, innovation base, but without suffocating the aspects of the base that are its greatest strength. Right?

So, I would think about it in terms of defining priorities, structuring incentives so that the various elements of the ecosystem work together towards common goals. In other words, they all see what the common goals are, the incentives are structured so they can do it and even have incentives to do it, and so they are like a team moving towards the same thing. And I think if you do that we are going to have a tremendous advantage over the Chinese industrial base which, as Secretary Flournoy was saying, is much more authoritarian, much more top down, and where they are trying to make it more so with their military-civil fusion process.

Now, you are going to have to be proscriptive sometime, you are going to have to prescriptive sometime, you are going to have to require some things and forbid some things. But I think it will work if the actors in the system at least understand why you are doing that. So, they go, well, you know what, we don't like that restraint but we get it. Okay, we understand why we can't go out and partner on that technology.

That is related to the second point. So, you are going to encounter, I think, as you approach the national security innovation—you already do all the time in legislation—constant tension between protecting the technology we have and getting the new technology we need between security on the one hand and innovation on the other; between, if you want to think of it this way, defense, right, and offense.

So, defense suggests siloed supply chains which the Department is talking about, limiting interactions, export control. You can't do partnership with certain, you know, the universities and the firms can't do partnerships with certain actors. The public actors in the system are comfortable with that because that is how they have been, that is the culture they have been living in for a long time.

Offense on the other hand, getting technology, requires a degree of transparence, it requires partnerships, consortiums, sharing ideas. Now, there is security. They get that. They all have to keep their patents secure and the rest of it. The private actors are more comfortable with that.

So, in my written testimony, how do you resolve it? It is going to be a case-by-case thing. We did come across an idea that was suggested by one of our national partners in the national technology industrial base, you know, this new, and you guys expanded

this I think in the Defense Act last year. It now includes the Australians, the Canadians, as well as the Brits. And we had a briefing session with partners. And they are coming and discussing strengths and weakness of sharing technology with the United States.

And the Australians made, I thought, a very good suggestion. They said, look, if we were you we would build higher fences but around fewer things.

So, decide what the technology is that really is vital, that we do control. Because if they can get it from somebody else anyway, it doesn't make as much sense to restrict our actors, our segments of the ecosystem from partnering, right? And build high fences around that. And otherwise err more on the side of offense, because I think we are probably going to win this competition more through offense than defense. Whatever you do, be clear about it because, remember, this is a big, pulsating, chaotic ecosystem. They are all going to want to do and they know they need to do what you insist that they do, but uncertainty from you or the government is the enemy of both security and innovation.

Third point, and I will go briefly through this because I am taking too long. I want you guys to be able to get to the questions. But this is, just because I am brief about it doesn't mean I think it is an unimportant point.

Take an inventory of what the Department is already doing and pull out the models that are really working, for a couple reasons. One, because you may be able to scale and expand them. But the other is because those models will be working for a reason. And if you can figure out why they are working, the characteristics that make them successful, then you can replicate that in other parts of the ecosystem.

So I suggest in my testimony, and we are going to focus on this in our report, obviously DIU, which you all deal with all the time, although we do suggest that the investment policies of the Defense Innovation Unit be reoriented a little bit more in the direction of trying to get innovative new tech companies, programs of record sooner in the time horizon. Because if the tech investment community believes that by putting money, investing in different tech start-ups is a realistic possibility that they can hit the jackpot with an 8-figure program within a realistic period of time, what we are assured by the venture capital community is they will all start wanting to go into it, which is I think what we want, right?

But also look carefully at the Defense Digital Service, which we have not, and at Hackers for Defense. You are nodding heads. I should have known, you are already familiar with this. But I was so excited. I briefed both of those because those are, one is an inside-out program, the other is an outside-in program. They are organically linking together these two cultures. They are organically drawing bright young tech talent into the national security world. They are changing—it is almost like joint assignments over time, creative jointness.

Really look at that, and see if you can scale it and expand it. They are expanding anyway. Hackers is expanding, or Hackers for Defense. I shouldn't say just "hackers," Hackers for Defense. Perfectly legitimate, if you are not familiar with it, but they are bring-

ing tech talent into—and by the way, they are helping the Department redefine, reimage how it asks questions. That is one of the things Hackers, these are teams of kids in universities around the country, they take this course for credit, but they are linked into the national security community. And problems, actual problems are presented to them to solve.

And one of the first things they do is work with the government sponsors to ask the questions in different ways, in ways that will make it amenable and open to tech solutions, which is teaching our people in the Department how to think in terms of technical solutions.

So, I was really excited about it, I think you can tell.

Okay, the final point is this. We are all, as Secretary Flournoy said, we need to get breakthroughs in key areas of innovation: AI, directed energy, quantum computing, the list goes on and on. If you want breakthroughs it means you have to take a gamble on technology by definition that isn't already proven, right, because you are going for breakthroughs. Which means you have to make investments that are a little bit riskier than the government is used to making, which means you have to be prepared to fail sometimes.

And I think I didn't realize from that side, when I was on that side of the table what I realize now is how important it is for these actors in the Department and all throughout the public segment of the ecosystem to know that you understand that and you will have their backs. They are very afraid of making an investment, particularly if they have to use authority to go outside the established rules and they don't go through all the regulations to invest and the rest of it and it doesn't work. And what will Mr. Smith think of that? What are they going to say? Am I going to get called before them in a hearing? How am I going to explain it? Is it going to be a career ender? Okay?

And I think you need to find ways to send a message to them that, look, just as the tech community does, they know that they couldn't, can't achieve the successes they want with the payoff they want unless they fail sometimes. So, I think you need to find a way to send a message. Of course you want the due diligence done. Of course you want thoughtfulness and purposefulness. Of course you want them to keep you informed. You are entitled to oversee what they are doing. Okay. But within those limits it is okay to fail. And as a matter of fact, I think you should send a message that if 5 or 10 years from now all of their experiments have succeeded, they are probably not experimenting enough.

And if you send that message, then I think—and you do that consistently, then I think there is a greater chance that they will reach out in the way that Secretary Flournoy has suggested.

So, thank you. Ready to take your questions.

[The prepared statement of Mr. Talent can be found in the Appendix on page 43.]

Mr. MOULTON. Okay. Thank you both very much. I know we have learned a lot already.

Let me dive into questions. And, Secretary Flournoy, we will start with you.

You concluded your statement by talking about how fundamentally this is a fight for the survival and success of American values,

and that is why it is important to win this fight. One of the things I think we struggle with is the concurrent development of technology and the policy around that technology, the norms of its use, its employment, training, and doctrine or whatnot.

In your view, what actions does the Department need to take to promote more alignment in policy, employment concepts, training doctrine, and other matters as technology matures?

Ms. FLOURNOY. I think as we undertake the technology development and conceptual efforts we need to have a policy conversation that is in each of the key areas that is trying to come up with a set of principles or guidelines that are rooted in our core values and who we are as the United States.

I think an example of this is the Defense Innovation Board which, you know, is a lot of really talented tech people who are working for free, has taken a stab at AI principles to guide our artificial intelligence work in the Department. That is the kind of thing. And I think that is a great basis for them to have conversations with the private sector and with the tech providers about what the Department is and will do and won't do. And I think it will clear up, frankly, a lot of misconceptions that sometimes exist in the tech workforce.

But I think in each of the areas where we are moving out we should be in parallel having those policy conversations. And I think it is sort of incumbent on the Department to sort of initiate those, but also to draw in other members of this innovation ecosystem.

Mr. MOULTON. Senator Talent, do you want to add anything to that?

Mr. TALENT. You know, I think, I think one of the, one of the things we need to do—and Michèle mentioned this in her testimony, I think you did in your opening statement—one of the things the Department has to do, it has to refine its operational concepts first. It has to define how is it going to operate in response to a particular challenger?

Reduce it to its essential. Okay, how are we going to fight China if we have to fight China? Although I would put it, how are we going to respond to provocations in a way where the Department plays its role in a sophisticated cost imposition strategy?

Now, when you know what it is you want to do in response to a particular challenge, then you have a more concrete opportunity to consider what are the ethical considerations or the other considerations that are likely to come up in the context of that. And so, if you don't know what you are trying to do, it is hard to anticipate what the constraints ought to be in doing it.

Mr. MOULTON. Senator, when you talk about that, are you talking at the strategic level, like, how do we go to war with China if it comes to that? Or is it more at the sort of technological level where we talk about the norms for the use of AI?

Mr. TALENT. I think it is both. Although I would say on the strategic level this is a job that is as much or more for you all on your side of the table. In other words, okay, we are in this competition. Let's just pick with a particular actor, with China, since I think it is the pacing challenge. So, what does winning the competition look like? What does success mean? Where do we want to be 5 years, 10 years, 15, 20 years from now?

They are defining that. And I think the top-level political authority, which you all represent, what is it you want the outcome of this to be and why?

Now, once you have provided that direction—and I don't think we have done it yet to the Department—then they can play their role in saying, hey, what is the National Defense Strategy in terms of that? I would just suggest I think success means protecting the American homeland, the territorial integrity of allies, the economy, from attacks. And I think it means what Michèle was talking about, the preservation of a system throughout the Indo-Pacific and the world where nations relate to each other according to rules, and resolve disputes peacefully, and not according to who is bigger.

Let me add this because it may be a useful way of thinking. And it is not mine. I was in Tokyo with the China Commission a few years ago talking to a Japanese scholar, and he was referring to Beijing and the rulers of Beijing. He says, you've got to understand, he said, we look at the world horizontally and they look at it vertically. We look at it as a world where nations basically have equal rights and operate according to norms. Now, obviously everybody maneuvers around the edges for advantage. They look at the world where—and this is an historical view, this is not something recent with the Chinese Communist Party—where they are the Middle Kingdom in a position of suzerainty, in essence. And the big dogs get the benefits, and they are the big dog.

And this is the fundamental conflict of vision that I think the Obama administration, one of the tremendous gifts the Obama administration gave us was they identified right at the beginning that that was the object of our policy. So, once that is set, then we can say to the Department, okay, we are going to fight the grey war, too, within certain limits. How are you going to contribute to that. And then what kind of limits do we want to insist upon because of our values?

Mr. MOULTON. That is very helpful. Let me just ask one more question. Secretary Flournoy, I'd start out with you.

You stated in your testimony that rather than provoke a major confrontation, our adversaries will continue to try to unilaterally and incrementally alter the status quo in their favor, using economic, diplomatic, and military coercion to achieve their objectives. Think Russian information operations in Ukraine and Europe, China's efforts to fortify artificially created islands in the South China Sea.

What are some examples of things the Department is doing that you see as a, quote, "waste of time, money, and resources" that could be better used to counter these threats?

Ms. FLOURNOY. Well, this is where, you know, I do think this is why I proposed this sort of knee-in-the-curve thinking about major, like, how many numbers of legacy platforms, what size, how many aircraft carriers, JSFs [Joint Strike Fighter aircraft], you know, pick your, pick your flavor. Because in addition to the strategic thinking that Senator Talent mentioned, which is absolutely right, I think this body also has to dive into the operational level sort of campaign concepts. Because we are equipping ourselves to fight the last war right now. And we are not going to have that luxury.

And we have to be thinking—and I want to applaud, the Department is really trying, thinking through multi-domain operations, the services, the naval services have distributed maritime operations. The Air Force is coming up with its concept; the Army. I mean, I would hope that you, you know, whether it is this task force or the broader committee is diving into that conceptual work to really understand because that is the basis on which we should be making the eaches, eaches of program decisions.

I mean, if the whole—I will give you an example. Long pole in the tent for multi-domain operations is a multi-billion dollar investment in cloud data infrastructure, networking, interoperability, basically building an advanced battle management system. And that is going to require trade-offs. We are going to have to take money from elsewhere in the program.

But if you, you know, have no, if there is no conceptual grounding for those individual trade-offs, how are you supposed to make those judgments? And so, I would really encourage you all to dive into that conceptual work at the sort of campaign level because I think that is really critical to making the hard choices. And they will be hard choices because in every case you are going to be taking a legacy program with a defined and powerful constituency, and trying to shift money to something new that has no constituency yet but without which we will fail. And whether it is failure of deterrence or failure to actually deal with aggression when it occurs.

So, that is a—I haven't given you a list of programs to—but I do think we need to communicate our commitment: what are we committing to defend? And every day, potential, you know, rivals need to see us doing freedom of navigation operations, showing up at regional fora, standing behind allies and partners who are risking, taking risk alongside us.

And here I have to say, the recent abandonment of the Kurds in Syria is not only a terrible decision for fighting ISIS [Islamic State of Iraq and Syria], but also sends a horrible message to every partner and ally we have around the world. And that is going to take quite a number of years to overcome, I think, sadly.

Mr. TALENT. I will address it. And I don't think I addressed the second half of your question, Mr. Chairman, before, so maybe I will just do it now.

So, I think the key is to think in terms of how do we impose costs on the competitors in a way that is real to them so that we have actions for deterrence but in a way that is not escalatory, at least in the military sense.

What are our horizontal options?

Now, some of those, and we have to begin thinking more consistently in terms of the fact that this competition is across a number of domains, obviously, and they all have to work together. So, there is economic, there is reputation. You have done that with the BUILD [Better Utilization of Investment Leading to Development] Act. I was so encouraged when I saw that, because that is an opportunity for us to put some money in, for example, in Southeast Asia, which Beijing views as its sphere of influence. And that is going to set alarm bells off in Beijing. What are the Americans doing in Southeast Asia and in South Asia?

See, that is a way of imposing cost on them.

So, the curious thing, Mr. Chairman, is that I think some of this can be expressed in low-end options—we are here talking about technology—that could be very helpful in the short 5- to 10-year windows that Michèle was talking about.

I will just throw out an idea. Okay? Russia is very interested in the Arctic. China is very interested in the Arctic. We could present a real alternative as competitors to them in the Arctic if we had more icebreakers, and if the Coast Guard had more of those cutters. I think you are buying three of them. They want six. So, these are low-end options. But why don't we get involved in areas they think are very important? Make them think.

See, that is a cost imposition thing. Really what you are doing here, there is a similarity to the Cold War. It is not a Cold War. But just as in the 1945–1955 timeframe Congress created, on a bipartisan basis, an architecture of national security tools which was then used by Presidents of both parties to prosecute the Cold War, that is what you are doing now. You are doing it with the CFIUS [Committee on Foreign Investment in the United States] reform, you are doing it with the BUILD Act, you are doing it with ARIA [Asia Reassurance Initiative Act of 2018], and you are going to do it with procurement. That is the question you are asking.

So, I think in terms of if you were down there at the White House and at the end of the table—and Michèle's been in those rooms—making decis—what would you, what options would you like to have? And this is, this was the problem with AirSea Battle. And I said at the time, wait a minute, if our option in dealing with the Chinese is to bomb the Chinese homeland—and I know that is oversimplistic——

Mr. MOULTON. Right.

Mr. TALENT. What President is going to order that——

Mr. MOULTON. Right, right.

Mr. TALENT [continuing]. Because, because they have taken the Second Thomas Shoal?

Mr. MOULTON. Right. Sir, thank you very much. I know we are running over here on time. And we are grateful.

Mr. TALENT. In Missouri——

Mr. MOULTON. I want to defer to not——

Mr. TALENT. I was going to say in Missouri we would say that I gave you more answer than you gave me question. So, I am sorry about that.

[Laughter.]

Mr. MOULTON. So, I am happy to turn over not to the ranking member but to my co-chairman. This is a very bipartisan task force. And with that, Mr. Banks.

Mr. BANKS. Thank you, Chairman Moulton.

Ms. Flournoy, in your testimony you highlighted Beijing's doctrine of civil-military fusion, while here in the U.S. there seems to be a growing rift between commercial technology hubs and the Pentagon. What additional efforts can be undertaken to help create a model of civil-military fusion domestically?

Ms. FLOURNOY. I think that, you know, in my current capacity in consulting I am actually finding there are a lot of folks in the tech community, whether it's Silicon Valley, or Austin, or [Boston's

Route] 128, or wherever the hub is, who actually want to contribute to the national security space. And so, we have to make it easier for them to do that.

And I think it is a matter of systematically sort of identifying the key barriers, whether they are acquisition barriers, whether they are tech talent barriers, we need to, I mean I listed a number of them in my statement, and you listed a number of them in your opening statement. But I think we, we need to systematically break down those barriers to allow them to contribute more.

I do think that one of the ways to really incent the private, the commercial tech ecosystem is to put, to help them, you know, companies cross this valley of death. Right now the narrative in Silicon Valley is, you know, we had an AI company, it had a couple of SBIR contracts with a service, it was—we really bet on this turning into something. The service loved the technology. And then it got canceled because the service didn't have the cloud, you know, infrastructure and the data architecture to then take it to the next level as a program of record.

Or, we have another—we have an AI-enabled quadcopter company. They have won all of the SOCOM and SOFWERX, and all of the prototyping contests and demonstrations. And, you know, that was in fiscal year 2019, and we are going to put them in the program of record in 2021. And their investors are, like, what happened? We need $10 to $20 million to survive to get to 2021, what happens in 2020? And there is literally no color of money that can help them in that bridge.

So I think that bridging work. I think the tech scouting is working, you know. The demonstration prototyping is working. You need to, it needs that bridge to the program of record, and putting real money on the table. That is what is going to get the venture capital community excited. Because right now most of them, with a few exceptions, are advising companies don't develop a national security business because it is too uncertain, the risks are too high, we won't get the return on investment, you are wasting your time. You are just going to suffer a horrible, you know, flame-out after a few years of effort.

So we have to change that incentive structure. And I do think there are ways that you could provide some more flexible bridging funding that companies can compete for to get some of them to programs of record. And once they are at scale, they will come. You know, if you build it, they will come. But you have to get them to—you have to put some successes on the board.

Mr. BANKS. Thank you.

Senator Talent, in your testimony you mentioned the need for the DOD to move toward a different procurement strategy and allow for additional risk. Over the past year, China has made significant strides in the development and testing of hypersonic weapons.

How has China been able to develop those technologies at such a fast rate?

Mr. TALENT. That is a good question. I am concerned that this is real and that they are, the latest developments are reflective of what is actually happening and that they may be well ahead of us. They have been putting a consistent emphasis on hypersonics for

a long time. I think part of it is the fact that they are very comfortable with a missile-centric military, and this was a logical development.

When I was in the Senate I was trying to get the Department to focus. I put money in for that. It was difficult. This was in the mid-aughts. Difficult to get them to focus, and the Chinese were working on it. I think this is a result of effort over time.

I think generally speaking they are better at incremental innovation than at breakthrough. And I think it is because their system is such a top-down system it doesn't encourage it.

I would also not be surprised to find out that they stole a lot of the foundational technology. And one of the things you have to keep in mind, particularly with this aspect, with this competitor is that they are very good at that and they build it into their plans. Okay.

So, specifically with respect to hypersonics that is what I, that is what I would say. That is one of the vital technologies where I think funding is still basically dominated by government money, which is unusual, like compared to AI or quantum. So, I think the Department can do a lot about this. But it is really important because the impact of the next 8 to 10 years, particularly in that theater, if they are able—I don't have to tell you all—to operationalize hypersonics, we have trouble because our missile defenses go out the window.

So, that is what I would say specifically with regard to that.

Mr. BANKS. Ms. Flournoy, any thoughts on that? Or what are the barriers that are preventing the United States from catching up?

Ms. FLOURNOY. Again, I think that our efforts on hypersonics have been primarily sort of programs through DARPA in the past. Those have not generally, you know, led to programs of record.

I do think, you know, consistent focus on this will change that outcome. And there is amazing innovation happening. I mean, one of the companies that I recently visited is 3D printing 80 percent of hypersonic engines, which will dramatically reduce from design to production to, like, 15 months. It is amazing.

But, so, you know, we are starting to get traction in really interesting areas. But we, as the Senator said, we are just playing catch-up.

Mr. TALENT. Yeah.

Mr. BANKS. Well, thank you to both, both of you. I believe you have done very well to set the stage for what we are trying to accomplish through this task force. With that, Chairman Moulton, I yield back.

Mr. MOULTON. Thank you, my friend. Now I would like to turn to Congresswoman Slotkin, who has spent a lot of time leading from inside the Department of Defense before coming to be a leader in Congress.

Ms. SLOTKIN. Greetings to both of you. Sorry, I have a cold. I apologize. And especially Ms. Flournoy is the person who brought me over to the Pentagon. It is great to see you.

So, couldn't agree with more on in particular how much we are sort of on our heels when it comes to bringing in defense innovation and the speed, the bridging the gap between concept and actual program of record. But I actually think personally there is a

group of us who think it goes deeper than that, that we just don't have a doctrine of innovation at the Department. We don't have a sort of theory of how we bring new innovation in.

And you talked about how you need to see top-down leadership in order to get people to take risks, get people to use the authorities Congress has given them. Can you tell me, you know, can you flesh that out a little bit? If a new Secretary of Defense came in and said, I really want to try and deal with this problem, that we are not taking advantage and bringing in, you know, new innovation, how would you specifically help filter that down to the depths of our acquisition officers?

Ms. FLOURNOY. I actually—I think there is a leadership component. But I think the best way to change behavior is through training and incentivizing your human capital differently.

Right now, you know, as the Senator described, people are terrified of failure in the acquisition—in any aspect of the acquisition system. You need to change the incentive to say, yeah, we want you to deliver major programs of record on time and in schedule and in costs. But when it comes to agile development of new technologies where we are experimenting and getting feedback from operators and then, you know, failing it, and then learning, and then doing better the next time, and it is this iterative process, you have to have a tolerance for failure.

That means looking at how you reward and promote people. It means training them in a very different approach. Agile development is totally different than the traditional DOD 5000 approach to acquisition. And I will give you an example of something great.

Secretary "Hondo" Geurts is the acquisition executive in the Navy. This year the Navy's acquisition award went to someone who presided over a tech failure but learned. And that learning is what created the success for the Navy. And so he wanted to hold this guy up and say this is the new poster child. This is someone who took risk. By taking risk, you know, we failed, we learned, and now we are on the path to success much faster than we would have been had he been risk-averse.

So that is the kind of thing, but it takes training people differently. It means rewarding them differently. It may even mean that we need a separate sub-cadre of acquisition professionals that are trained and incented differently than the rest. But—and it means the human capital piece, we have got to get more tech-savvy talent coming in and out of the Department at all levels, civilian and military, because, you know, it is a totally different skill set that requires a different approach.

And, you know, so I would focus less on a doctrine and more on looking at the human capital piece and that training and incentive structure to get the change in behavior that you're looking for.

Mr. TALENT. Yeah, I couldn't agree more with that. I will just offer two things: one an inside-out feature, the other an outside-in feature.

So, we need to reform the Pentagon personnel system in general. I did a project with Leon Panetta and Jim Jones a couple years ago. But it is absolutely crucial in this area, particularly hiring, retention, et cetera. And I am thinking area of Cyber Command, Space Command, high-tech areas, we cannot use a system that was

designed to produce, you know, to get people in at age 19 and produce fighter pilots and ship captains. It works for that. It does not work for cyber and technology.

And I think to the extent that we can just insist to the chiefs, make it a priority, and then SECDEF just says, Look, I want to see at the end of this year that you are using the authorities Congress has given you. And if you need more authorities, ask for them. And you are bringing people into these tech, whether it is procurement or whatever, and you are hiring them directly out of Silicon Valley on a specialized 2-year package where they come in as a captain, or whatever it takes. I want you to recruit talent that way.

And then the outside-in feature is this, and it is actually probably more hopeful: I do get a sense after looking at this that if we can do the bridge funding right, the procurement right, get the incentives right for the tech community so they see opportunities here, and I think a good deal of patriotism will go with this. If you look at the Hackers for Defense, these kids are excited by the prospect of standing up for human rights, and peace and, you know, and the norm-based system and the rest of it. But anyway, if you can get them to think of this as something they want to do, it is a business problem they need to solve to accomplish their objectives, I think from the outside-in they will find ways around the Pentagon culture and rules.

And if you talk to the Digital Defense Service people, that is one of the things they do. When they describe how they hire people in—who is the fellow who runs that who briefed us at—yeah. And he said we worked through, we got out the book on the Pentagon personnel hiring system and we figured out all kinds of workarounds, their stupid rules and the rest of it, so we were able to get people in on certain terms. So, I would really have him in here and talk to him about how he did it.

Mr. MOULTON. Thank you. Thank you very much.

We now turn to the medical doctor on the task force. You know, there are a lot of places where we are facing competition from around the globe, but one place where people still come from all over to get American care is in our medical system. Our healthcare system is far from perfect, but in terms of technological innovation it remains unrivaled as a world leader. And so we are delighted to have Congressman DesJarlais' perspective on this task force.

Mr. DESJARLAIS. Thank you, Chairman. And I am not going to ask any medical questions today. But——

Mr. MOULTON. We might ask you some.

Mr. DESJARLAIS. Okay. I would just like to quantify things a little bit and the whole purpose of this task force to see where we are going to be and where we need to be. And I don't know if you can answer this question or not, but maybe try, play with me.

We consider ourselves the greatest fighting force on Earth. And I think that is probably true. But, you know, we are here today because we have concerns of peer adversaries who are catching up. If you could, assuming that the United States is a 10 when it comes to overall military, where was China and where was Russia 10 years ago, and where are they now on that scale?

Ms. FLOURNOY. Yeah, that is a tough one. You know, I think let's start with, you know, I think overall as a military there is still no comparison between the Russian military and the U.S. military. But they have pockets of excellence where they have invested. They have invested in nuclear forces. They have invested in cyber. They have invested in space. They have invested in little green men and irregular forces that can do things like the operation in Ukraine.

But, you know, it would not be a fair fight if we ever got into something with them. But, they are very, very good in this anti-access/area denial [A2/AD] capability in terms of what they have set up in and around Europe. And so, we want to make sure that we would do even bett—you know, I think that in a conflict, you know, they crossed a NATO border, we had a war with Russia, NATO would prevail; but it would be more costly today than it should be because we haven't made the necessary investments to counter their A2/AD capabilities.

With regard to China, same thing. I mean, the military overall, you know, whether it is human capital, whether it is training, whether it is operational experience, it is nothing like the U.S. military. But that is not the point. I mean, they are taking an asymmetric approach. And the question is not so much, you know, in a conventional fight how would they compare. It is more have they invested enough and made enough progress in key asymmetric areas that they can actually undermine our strengths, and they can exploit our weaknesses and prevent us from being successful in even getting to the region and being able to operate effectively in the region.

So, I think you have to look more—less at a sort of direct apples to apples comparison, and more of an asymmetric encounter kind of evaluation.

Mr. TALENT. Their militaries are adapted to their strategy better than ours is, in part because they, they were rising powers, they are revanchist powers, and they looked at what we did in the early 1990s, and they had problems they had to solve if they were going to exercise influence. So they—and they have adapted their military to those purposes. So, anti-access/area denial, et cetera.

At the task and the missions that are most relevant to their regions of the world, they have armed forces that are suited to that. Okay. Now, when you get beyond that, expeditionary, that sort of thing, there is no comparison that we are superior.

But we have not, look, I think there was—and I was in, I was here and in the Senate for a long period of this time; we were distracted by other things, we were also the top dogs. We just didn't really think—and for a long time in the Department the assumption was that nobody would be able to challenge the United States for decades, right? And we weren't really thinking about it.

I do think as regards the Chinese this is something—I am also on the China Commission and we studied this, so it's something that is actually quite relevant to our consideration. I reached the conclusion that Beijing really, really is concerned about the operational capabilities of the PLA. They have all this shiny new equipment and the rest of it, but they are very concerned about their ability to execute in a mission. And that is important.

So, I would just say again it comes back to operational concepts and the rest of it. We've got to think in terms of how do we impose costs that are effective and real, short of escalating conflict? Because if the answer to something they are doing in the South China Sea, building an island, is to escalate it up, we are not going to do it. And they know we are not going to do it.

Mr. DESJARLAIS. I asked—I am about out of time but thanks for the answers—I asked the question because we have challenges within our own defense budget. We spend way more than other countries combined, as has been pointed out again and again. And maybe a question for another time is, you know, how do we approach the Pentagon to re-prioritize that budget that we have to work with, if it's 710 or 750 billion, what do we get rid of and what do we change to change the culture that we need to to be where our adversaries want to be in 10 years, where we are now and where we will be then?

So, thank you for the answers.

Mr. MOULTON. Scott, thank you very much.

So, we now turn to Congressman Mitchell. One of the emergent themes from the early discussions of this task force without question is the integration of the private sector into what the Department of Defense is doing. And Congressman Mitchell brings tremendous experience from the private sector, and we are delighted to have your perspective on the committee.

Mr. MITCHELL. Thanks. Very kind of you.

Let me start. I think one of the mistakes—and your feedback would be useful—the mistakes in our thinking in this nation is we separate out military power from national power. China in particular, but Russia has evolved, especially what Putin did, national power is linked to all their capabilities and they intertwine them. Somehow we think we have this distinct little military world and then our economic activities. Ah, there is some overlap but we—and I think we are losing the point.

So, my question is, is how do we, how do we get that point across, not only just Congress but to the general public, that national power is in part based upon our economy, our educational system, as well as in the application of that in our military systems?

Ms. FLOURNOY. Yes. No, it is such an important point. And we have talked a lot about the military because this is a task force of the House Armed Services Committee. But when I am out, you know, in public talking about this and people say, well, what do we do about China? I say the first thing we should do is invest in the drivers of our own competitiveness. And, yes, the military is on the list but it is not, you know, it is research and development. It is STEM education. It is 5G and 21st century infrastructure. It is cutting-edge technologies. It is smart immigration policy that attracts and tries to keep the best——

Mr. MITCHELL. Yeah.

Ms. FLOURNOY [continuing]. Tech talent in the world here in the United States, which is what our history has been.

So it is all of those things. And then, yes, we also have to, you know, talk about how does the military contribute to deterrence and shaping the calculus of countries so that they don't commit ag-

gression, and all of that. But it is first and foremost investing in those other areas and, oh by the way, investing in our diplomatic instruments, our ability to, you know, offer a counterpoint to the One Belt One Road, through maybe we need a digital, you know, infrastructure fund, or what have you, to offer, you know, other countries more open, transparent societies and so forth.

So, anyway, but I totally agree with your point.

Mr. MITCHELL. Well, let me comment for both of you, and Senator, your feedback, I think I agree with you. Our decision-making processes on Syria leave a lot to be desired. I don't think it sends the proper message to the world. And, frankly, canceling the summit in Copenhagen was not a great idea. That, in fact, one of the topics for that meeting was in fact investment in the Arctic, joint investment with Denmark and other countries, not just militarily, but other investment. And canceling that was a destructive act as well in my opinion. But we will see how we can get that back on track.

Question: how is it that we, what is your idea in terms of co-investment with venture capital? You talked about it as well, getting venture capital involved. Rather than simply a bridge fund which is just send money, how do we, do you have any recommendations on how we encourage that co-investment between the government and venture capital, private equity, in technologies for mutual joint use? Senator, do you want to start this time? Or whoever.

Ms. FLOURNOY. I mean, there have been some, you know, In-Q-Tel is probably the best example of early-stage co-investment. And it sort of it is basically a Good Housekeeping Seal of Approval that, you know, the intelligence community is interested in this company, in this technology. And that tends to attract outside investment to support it.

But I really don't think that—I think better than co-investment, frankly, they need the market opportunity. It is much more powerful for DOD to say we are going to spend $10 billion on AI technologies over the next 5 years, and to put out that target and that, you know, kind of commitment. And we are going to hold a series of competitive contract, you know, requests for proposals and other things to build an ecosystem around defense AI applications.

That would move the needle far more for venture capitalists who are advising their companies on whether to pursue national security business or not than, you know, a $10 million co-investment in a given company on AI.

So, that is my view.

Mr. TALENT. I agree with that.

Can I just make a couple of brief comments in response to your first question?

Mr. MITCHELL. Absolutely. Sure.

Mr. TALENT. I could not agree more with what Michèle was saying about we need a whole-of-government approach to these competitions. Part of what you are doing and need to do is to strengthen the civilian elements of national influence. And I think somebody at some point needs to make a deal with the State Department which is, look, we are going to increase your funding, we are going to give you more authorities. You have got to become more

like the Department of Defense in terms of planning and how you—we need them to play a stronger role.

Now, a lot of that is not their fault. They don't have the funding, the training, the rest of it. But I want to see that happen with the State Department. I have talked with former SECSTATEs [Secretaries of State] about this, and they all want to do it.

The only other comment I would make is this: I completely agree a lot of this competition is going to be prosecuted, and the primary tools we should want to use are the civilian tools of national influence. But the foundation of those tools is and will remain the United States ability to deter kinetic aggression. Okay.

And one of my big concerns is if we start winning the competition on other fronts—reputationally, economically, and otherwise—these authoritarian regimes are fully capable of expressing their ambitions and responding through aggression, if that avenue is left open to them. As a matter of fact, that is a classic tactic, is to direct dissent outward by starting something with your neighbors.

So, we can't—the hard-power tool is and will remain the foundation of the effort.

Mr. MITCHELL. Let me pose a quick question again, Mr. Moulton, and it won't be for this.

You both had comments about investing in legacy technology. This is not the right environment to have that conversation, but I agree with you.

But the question then gets down to specific recommendations of what it is we delay investment or consider not and invest elsewhere? I agree with the discussion, it is easier to make that kind of general comment. But then in a classified environment we can talk about what do we, where do we start on that, and it's not going to make a variety of people happy. But that is part of why we have this group.

Ms. FLOURNOY. Just make a 10-second conceptual answer which is I really—for me what has been helpful is this knee-in-the-curve idea which is, you know, if you took the money for the n+1 platform, or whatever that type is, and you folded it into, you know, this is, okay, it is going to be operating in a more contested environment, so I am going to put money into the defenses of that system. I am going to put money into buying back that system's range and ability to reach out and touch, you know, a much more protected adversary. I am going to make sure it is cyber secure. I am going to make sure it can leverage and plug into an interoperable network.

So, I think it is really, like, it is really where does—it is not worth buying that additional platform but to take that money to make all of the other platforms in that class more survivable, more effective, more relevant.

Mr. MITCHELL. That is my questions for you is which ones? Where do we start? That is the question.

Ms. FLOURNOY. Okay, yes. We can, we can follow up on that.

Mr. MOULTON. Thank you. Thank you very much.

So, we now turn to the first Green Beret in Congress, Congressman Michael Waltz. I spent quite a good deal of time working on the ground in Iraq with Green Berets, and I always found them generally quite talented, and capable, and smart, and all the above.

So I am not quite sure what took so long. But we are delighted to have you here, Mike.

Mr. WALTZ. I have a side mission to make "De Oppresso Liber" as popular as "Semper Fi," but I have a long way to go, man.

So, just two quick comments. And first of all, it is great to see you again, Michèle, and good to meet you, Senator. Two quick comments on some of the things that you have talked about because I also sit on the Science and Technology Committee. And, yes, we need to invest in foundational research, R&D [research and development], all of those pieces. But it is much broader than defense investment. And we need to re-look at how the Chinese are taking advantage of what I think is our greatest strength, which is the openness of our educational system.

But, for example, you know, if you receive a grant from the National Science Foundation and come up with some amazing research, statutorily you have to make that publicly available. And so what I don't want to see, or what we are looking at on the other committee is how do we, you know, how do we maintain that openness but then also protect it?

Because I would hate to see all of this taxpayer investment just for it to continue to be stolen. Whether it is Confucius Institutes or, you know, in a number of other ways.

So, that is one. And then, two, Senator, I do think we have a fantastic bridge in place in terms of personnel reform where you are looking to bring in folks from Silicon Valley, give them a few years, or bring in specific types of talent. It is called the National Guard and the Reserve. And I don't think we use them and think about them nearly as effectively. I mean, you have to think about, you know, I had a master sergeant who is a fantastic weapons guy, but he was also a vice president for Verizon's cell phone network. Where is he better used?

But when I asked the Guard, can you tell me how many people you have working in Silicon Valley, that is just not how they are organized. They are organized to be a supplement for a brigade combat team.

So, looking at ways that we can really—I mean, I think those bridges are in place. You could take a cyber expert that is learning the latest and greatest and put them on orders for a year or two to infuse that back in.

So, I would just encourage as you guys, as you both engage, to think about that as well, whether it is stability operations, cyberspace, election security. Who is in all 9,000 counties in the United States? The Guard. It is really our only national entity.

Question for you, because I was reading through your trade-off component, and it is similar to my colleague that I am still trying to convince not to retire, who I think is fantastic. You know, I am really interested in what we don't do. What do we give up in terms of platforms and missions? I think the existential question for this committee is how do we deal with extremism, China, Russia, rogue states, overlaid with $23 trillion in debt? There at some point has to be trade-offs. So, what systems more specifically would you advise that we give up to invest elsewhere?

Ms. FLOURNOY. Well, let me start by directing you to if you have, I am sure you have, but if you take a second reading of the new

Commandant's statements, he has basically presented this framework for the Marine Corps to say, look, the things that have been, the metrics by which we measured our power in the past, you know, how, you know, amphibious shipping, large deck amphib, et cetera, you know, that is not necessarily the right—what is going to determine whether we win in the future. I have a new concept of distributed maritime operations. There are lots of things I need to invest in to make the Marine Corps able to really support the broader Navy in sea control in this much different kind of way of operating in a contested environment.

And so, you know, watch this space. You should expect that I am going to make some trade-offs in traditional platform buys in order to invest in a whole lot of new technology areas.

So he, of all of the chiefs, I think he has been the most explicit on how he is starting to frame those trade-offs.

MCCDC has done—the Marine Corps Combat Development Command down in Quantico has done really cutting-edge work conceptually to kind of try to frame this so that individual tech and program decisions have a conceptual basis for being made.

So, I do think that is probably the most forward-leaning example. But all of the services are busy trying to get at exactly this point. And, you know——

Mr. WALTZ. Right. I——

Ms. FLOURNOY. Sorry.

Mr. WALTZ. No, I think it is a great example just in the interests of time of kind of taking on what we talked about in terms of sacred cows.

But I would love either for the record or in a follow-on session, as you look at the new NDS [National Defense Strategy] and then you look at where we are actually spending, you know, what is outside of that scope? What is—where are we basically spending on what I call, you know, great traditions that we often find in the services, whether it is static line airborne operations or, you know, Inchon-style amphibious landings, or the 12-carrier fleet, what conceptually are you seeing that falls outside of that framework and we are doing it just because?

Ms. FLOURNOY. I would be happy to come back and talk to you individually or to the task force.

Mr. WALTZ. Thank you.

[The information referred to can be found in the Appendix on page 49.]

Mr. MOULTON. The one other question I was going to ask is actually about the Commandant's new guidance. So, we are in good shape there. Thank you.

Mr. WALTZ. Marines can be forward-thinking, too.

Mr. MOULTON. Well, thank you all very much. This has been fantastic and we have covered a lot of ground.

I will give the two witnesses an opportunity to provide any closing remarks, if you have any, and then we will conclude the hearing.

Ms. FLOURNOY. Just to say thank you for the work you are doing. I think this is one of the most important things that the House and, you know, the Congress in general is doing. It is so important that we get this right and get it right quickly.

And just to say I am happy to support your work in any way that I can in a follow-on way. I will also just flag that we are currently involved specifically on a project on this human capital question on tech talent. Happy to share those results with you when we get there.

Mr. MOULTON. Great. Thank you, Secretary.

Mr. TALENT. I just want to repeat, I was greatly encouraged to see the formation of this task force. I cannot think in 25 years of when the committee has done something like this. And its existence is sending the right signal to the Department.

In fact, I don't know, you probably have the same experience, I have had a number of people, not from inside the government, but people call me when you put the hearing notice out, because I was testifying, to urge me to talk about this or that or the other thing, and to say how excited they were that you all were here. And so, I am grateful that you are doing it. And if we can help in any way, either one of us I am sure, let us know.

Mr. MOULTON. Well, thank you. I am confident we will take you both up on those offers. We are excited as well, but we have an awful lot of work ahead of us in a mere 6 months. We look forward to being in touch.

With that, this concludes the hearing. Thank you all very much.

[Whereupon, at 11:31 a.m., the task force was adjourned.]

A P P E N D I X

OCTOBER 29, 2019

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

OCTOBER 29, 2019

Testimony before the House Armed Services Committee Future of Defense Task Force

Recharging the National Security Innovation Base to Meet Emerging Threats

Michèle A. Flournoy, former Undersecretary of Defense for Policy

October 29, 2019

Chairmen Moulton and Banks, distinguished members of the House Armed Services Committee Future of Defense Task Force, it is truly an honor to testify before you today on the critical challenge of preparing the DoD and national security innovation base to meet emerging, long-term threats.

The Geostrategic and Technological Landscape

The resurgence of great power competition combined with the unprecedented pace of technological disruption require the United States to reimagine how we deter and, if necessary, fight and prevail in a future conflict. Central to this challenge is ensuring the U.S. military retains its operational and technological edge over a revanchist Russia and particularly a rising China.

Since the end of the Cold War, the United States has enjoyed a period of unrivaled military and technological superiority, but we can no longer afford to rest on our laurels. America's military advantage is rapidly eroding in light of China's and, to a lesser extent, Russia's military modernization efforts. In fact, if we stay the current course, a rising China and revisionist Russia will likely achieve overmatch in a number of key capability areas, calling into question our ability to credibly deter aggression, defend our interests, allies and partners, and prevail in any future conflict at acceptable levels of cost and risk.

Since the first Gulf War, both Russia and China have gone to school on the American way of war and have developed asymmetric approaches to undermine our strengths and exploit our vulnerabilities. At the core of the military challenge to the United States and our allies is the substantial investment by China and Russia in anti-access/aerial denial or "A2/AD" capabilities. These A2/AD capabilities -- ranging from persistent precision strikes on U.S. logistics, forces, and bases to electronic, kinetic, and cyber attacks on every digital connection and system inside our battle networks -- mean that the United States can no longer expect air, space, or maritime superiority early in a conflict; we will need to fight to gain superiority and then to maintain it in the face of ongoing efforts to disrupt and degrade our battle management networks.

Beyond these A2/AD and counter-network capabilities, China is investing tens of billions of dollars in a state-directed technology roadmap for emerging technologies – from hypersonics and robotics to quantum computing and artificial intelligence. Indeed, the primary competition on which the United States must focus is the tech race with China, as it is this competition that will be the pacing threat for our military and will have the most profound and long-lasting impacts for U.S. prosperity and security over the next half century.

Thanks to Beijing's doctrine of "civil-military fusion," in which any commercial or research-based technological advancement with military applications must be shared with the People's Liberation Army, the Chinese military has made rapid advancements in its artificial intelligence and machine learning capabilities. Indeed, Chinese military doctrine is now premised on the belief that the side that can make and execute battlefield decisions most quickly – and preferably well inside the decision-making cycle of the adversary – will gain the strategic advantage in a future conflict. Given the centrality of emerging commercial technologies like

AI, quantum computing, 5G and autonomous systems in ensuring the U.S. military keeps its edge, the United States needs an effective answer to "civil-military fusion," and soon.

In addition, both Russia and China have paired these technological investments with doctrinal innovations. Russia is rapidly modernizing its nuclear arsenal to support its "escalate-to-de-escalate" doctrine. With the Trump administration weighing New START renewal and in the wake of U.S. withdrawal from the INF Treaty, the United States and Russia are on the precipice of an alarming period of strategic instability. Meanwhile, China's theory of victory increasingly relies on "system destruction warfare," an effort to take out or cripple an adversary's networks at the outset of conflict – deploying sophisticated electronic warfare, counter-space, and cyber capabilities to disrupt critical C4ISR networks, thwart U.S. power projection, and undermine our national resolve. This means the United States can no longer take space for granted as an uncontested domain from which to provide services like early warning, navigation and communications. In the future, space will be a critical warfighting domain through which and from which to project power.

Nonetheless, given the reluctance of major powers to enter a large-scale war with the United States, in the near term it remains more likely that both Russia and China will rely on "grey zone" approaches to compete below the level of conventional armed conflict. Rather than provoke a major confrontation, our adversaries will continue to try to unilaterally and incrementally alter the status quo in their favor, using economic, diplomatic, and military coercion to achieve their objectives. Think Russian information operations in Ukraine and Europe, and China's efforts to fortify artificially-created islands in the South China Sea.

DoD's 2018 National Defense Strategy (NDS) provides a critical strategic framework for addressing these mounting challenges and reflects the growing sense of urgency within the Department about the United States' eroding military advantage. The FY2020 budget sends a reassuring signal about Congress' continued, bipartisan commitment to the technology and capability investments necessary to implement the NDS.

However, the current budget environment will require Congress to make difficult trade-offs now to buy down risk in the future. The central question remains: How do we invest these dollars wisely to ensure that we can protect U.S. interests and allies, deter conflict, and, if necessary, fight and win in a far more contested future security environment? And how do we invest with the speed and effectiveness required to keep our edge given the speed with which potential adversaries are moving?

Re-Establishing Credible Deterrence

In the near term, I believe the Department must make re-establishing credible deterrence our central objective. While I believe neither the United States nor its potential adversaries are likely to deliberately start a war given the dire costs involved, we could nevertheless stumble into conflict if an adversary were to miscalculate the ability or willingness of the United States and our allies to respond to provocations or outright aggression. I assess that the risk of

miscalculation is greatest in the next 10 years – when the United States has telegraphed its vision for the future force but has yet to procure and deploy all of the systems necessary to fully translate this vision into fielded capabilities.

To prevent a miscalculation or escalation to conflict with a nuclear-armed rival, the United States must decide what capabilities we need to prioritize developing, acquiring, and demonstrating in order to credibly deter aggression, deny any adversary the ability to rapidly seize territory, and prepare to impose significant costs for any act of aggression. And we need to do this with two timeframes in mind: deterrence in the interim (the next 5-10 years) and deterrence in the long term (10 years and beyond).

We need to think creatively about how we might stop a rival great power from starting down the road to war. For example, what capabilities would U.S. naval and air forces need to credibly threaten to sink 300 military vessels, submarines, and merchant ships within 72 hours? Such a capability would certainly pose a fundamental dilemma for any great power contemplating aggression, forcing them to consider whether they want to put all the ships in their fleet at risk. Undoubtedly, there are other approaches to be considered to give an adversary pause in the near to mid-term; DoD should devote considerable effort to conceptualizing and wargaming a suite of interim deterrence approaches using existing capabilities in new ways to deny or dissuade aggression.

The fact that several countries are questioning the United States' commitment to defending its interests, allies, and partners only underscores the importance of doing far more to communicate and demonstrate our resolve. Clear policy, action, budgeting, and messaging are all critical to strengthening deterrence and shaping the risk calculus of any nation that would consider using force to pursue their aims.

Strengthening deterrence will also require major, focused efforts to enhance and demonstrate our capabilities, including emerging capabilities that could dramatically increase the costs borne by an aggressor in the longer term. New technologies will enable potential adversaries to challenge us with new threats on the battlefield, but these technologies can also greatly strengthen our ability to deter aggression and bolster our response capability should conflict break out. The United States also needs a strategic framework to guide whether, when and how to reveal new capabilities that could cause a future adversary to rethink the costs and risks associated with an act of aggression.

Recommendations

Today, I'd like to recommend six lines of effort the United States should pursue to re-establish credible deterrence and regain our operational and technological edge.

First, the DoD needs to implement a series of acquisition, investment, and workforce development reforms to foster the innovation ecosystem necessary to maintain the U.S. military's technological edge. While Congress has provided the Department with a number of

more flexible authorities, such as SBIRs and OTAs, which enable a more agile approach to acquisition, DoD has not adequately trained or incentivized its acquisition workforce to employ these authorities effectively and at scale. While there are pockets of excellence (e.g., in SOCOM and Air Force acquisition), the bulk of the acquisition corps is not using these authorities at scale. As the Department prioritizes procuring the software and network capabilities critical to enabling future joint, Multi-Domain Operations, it will need an acquisition cadre trained and incentivized for the rapid and agile development of new technologies.

Fully leveraging these authorities and incentivizing program managers will also require top-down leadership to provide strategic direction and top cover in pursuing more ambitious goals. For example, what if the Secretary of Defense were to set an audacious goal for each of the services to drive more rapid integration of transformative technologies into the force? For example, he could direct the Marine Corps to field a newly conceived Special Purpose Marine Air Ground Task Force built around human-machine teaming and leveraging AI and unmanned systems to the maximum extent possible by the end of the FYDP. Similar goals could be set for a reimagined Navy Carrier Air Wing or Battle Group, an Army Brigade Combat Team or Combat Aviation Unit, and an Air Force Fighter Squadron or Air Expeditionary Force.

Further, while DIU, SOCOM, and various service units are playing important tech scouting roles, there remains a "valley of death" between a successful demonstration/prototype and becoming a program of record that many small commercial technology companies have found it impossible to cross. To source more commercially, DoD must accelerate reform efforts to make it easier for leading-edge technology companies to do business with the Department, including increasing the availability of funds to rapidly scale successful prototyping efforts. One potential approach would be to authorize funds that each service could allocate on a competitive basis to sustain continued capability development in priority areas and bridge the gap between prototyping contracts and formal competitions for programs of record. For example, let's say an AI company won a SOFWERX competition in FY2019 and the Army decides to put out an RFP to acquire the capability at scale in its FY2021 budget request. How does that small company stay in the game through FY2020? Bridge funding can provide a critical lifeline to small technology companies looking to continue the development of urgently needed, cutting-edge capabilities for the U.S. military.

Further, the Department currently lacks the tech talent –senior and junior, civilian and military, active duty and reserve – to develop, integrate, and deploy these critical emerging technologies. DoD should work with Congress to expand programs (currently focused on cyber talent) that offer scholarships to students in a broad swathe of tech fields in return for a government service commitment. DoD should also recruit mid-career technical talent by expanding fellowships for private-sector technologists to serve a tour of duty in national security, bringing in private sector HR best practices, educating national security leaders about the range of expedited hiring authorities at their disposal, and overhauling the painfully slow and antiquated security clearance process. Meanwhile, DoD can meaningfully enhance the tech skills of existing employees by providing more training opportunities in key areas and creating

viable career paths for technical talent that allow for both promotion and continued professional development, including rotations in private sector tech companies.

Second, the Department should ramp up its efforts to develop joint and service-specific operational concepts to drive more rapid fielding of game-changing technologies. The United States needs to urgently develop and test joint concepts, such as Multi-Domain Operations, and service concepts, such as the Navy/Marine Corps' Distributed Maritime Operations, both of which are premised on eroding adversary advantages by creating simultaneous dilemmas across multiple domains, spreading out (rather than concentrating) the force across the theater of operations. Testing the technologies that will be most critical to operationalizing these concepts -- from battle management networks to unmanned systems to long-range precision fires -- will require a continuous, reinforcing cycle of wargaming, prototyping and experimentation.

To do so, Congress should provide the services with robust funding to field small numbers of emerging capabilities for early-stage concept development and experimentation. For example, Congress should not hesitate to allow a service to acquire small numbers of AI-enabled unmanned systems of various types to facilitate the development of new concepts for human-machine teaming. Unfortunately, DoD and Congress now find themselves in a Catch-22 -- Congress wants more clarity before it funds experimental systems, while the Department needs a certain number of these systems to experiment with in order to develop a compelling case for Congress to fund the capability long-term. It's time to break this log jam, accept a bit more risk in the short term, and allow the services to acquire the prototypes they need to enable an agile development process that includes field experimentation and iterative feedback from the warfighter. This is the only way we will be able to develop new concepts and capabilities fast enough to keep pace with potential adversaries.

Meanwhile, in the short term, concept development and wargaming can also provide insights into how to reconfigure existing platforms to shore up critical capability gaps. For example, as the Department continues to develop new long-range weapons systems, the Navy and Air Force could experiment with reconfiguring bombers with LRASMs for long-range sea patrol against Chinese surface combatants and the Chinese A2/AD complex. This is exactly the sort of critical bridging work that the Strategic Capabilities Office (SCO) was doing before it was moved under DARPA and given a more future oriented focus. The Department needs a SCO-like office to drive the effort to shore up deterrence and our operational edge in the near to mid-term.

Third, the Department should adopt best practices and lessons learned from commercial sector technology development and program management. The Department has ambitious goals to migrate to the cloud, leverage large data sets for artificial intelligence and machine learning solutions, and build interoperable, multi-domain networks at scale. The Air Force is already building its Advanced Battle Management System -- the long-pole in the tent for bringing Multi-Domain Operations to life -- which will require rapid advancements in sensor integration, data processing, artificial intelligence, network connectivity, and cloud computing.

Integrating private sector approaches to technology development, data management, and network security will be critical to realizing these advancements. As previously mentioned, this means using a spiral development model with integrated prototyping that enables substantial input from real-world operators. It also means exploring how to incentivize industry to leverage open-source approaches that support iterative design and testing and provide platform and system interoperability. Finally, it will require prioritizing what elements of a complex network of networks must be secured, continuously weighing and re-evaluating potential trade-offs between openness, security, and resiliency.

Fourth, budget realities will require the Department and Congress to make urgent trade-offs between legacy platforms and critical new technologies. Currently, the United States is under-investing in the new technologies that will ultimately determine our success in the future security environment and over-investing in legacy platforms and weapons systems. This is a recipe for failure. In order to make the trade-offs necessary to position the United States to compete and win, DoD and Congress must answer a fundamental question for every major program of record: Where is the knee in the curve? Where is the point where it makes more sense to forgo the n+1 platform to, instead, invest those resources in the cutting-edge technologies and capabilities that will keep the existing platforms survivable, combat-relevant, and effective? For example, if the cost of a single additional aircraft carrier could cover the cost of electric weapons for ship defense, UAVs for ISR, refueling and electronic warfare, and new longer-range penetrating weapons for strike, would it be smarter to trade that extra carrier for a slightly smaller, but much more capable fleet? The same question can be used to frame the trade-offs associated with buying more amphibious ships for the Marine Corps, fighter squadrons for the Air Force, or tanks for the Army. The Secretary of Defense should ask each service tough "knee in the curve" questions and be willing to make the hard choices necessary to prepare for the future fight – and Congress should support the Pentagon when these hard but correct choices are made.

Fifth, the United States will need to adapt and enhance our overseas posture and shore up ally and partner capability to deter and operate in more contested, lethal environments. The United States should expect that Russia and China will seek to disrupt our ability to project power to re-enforce forward forces from the outset of a conflict and in all domains – air, sea, undersea, space, cyber. Therefore, we need to make our forces, forward bases, logistics networks, and C4ISR networks more survivable, resilient, and geographically dispersed.

The United States must fortify key overseas bases, while also moving towards a model of distributed "places not bases." Key forward bases that sit at the outer edge of China's threat ring will still be critical for staging and logistics. However, the military services will increasingly rely on smaller, distributed, more agile force packages to operate within the densest Chinese A2/AD threat rings. These forces, working with allies and partners, will provide temporary bases and resupply for forces in the area as well as more distributed fires to further complicate adversary planning.

Enabling our allies and partners to serve as critical force multipliers and better defend their own sovereignty necessitates a more strategic approach to security cooperation. This should begin with a clear-eyed assessment of what each partner country can contribute, followed by the development of multi-year security cooperation plans for each country and region – laying out what capabilities we collectively need to deter coercion and aggression. One low-cost, high-value opportunity is to invest in AI-enabled systems that fuse unclassified data streams to identify, track, and characterize the behavior of ships at sea or aircraft in the air; these unclassified systems can be easily shared with partners and dramatically improve their situational awareness.

Sixth, the Department should align its efforts around shoring up near-term vulnerabilities that undermine deterrence even as we invest in longer-term technological and organizational innovations. As I've noted, I believe that the next five to ten years will prove the most challenging and determine the course of U.S-China relations for many decades to follow. In the near term, the United States must work with greater urgency to close this vulnerability gap by re-configuring current platforms with new technological enablers, re-evaluating our "reveal or conceal" posture to demonstrate resolve, re-investing in building ally and partner capacity, and fortifying vulnerable forward bases and establishing new ones. Long-term superiority, however, will require fundamental shifts in technological capability, operating concepts, and force posture.

Conclusion

In conclusion, the United States needs to make urgent investments in its technological and organizational capacity to prevent other great powers from eclipsing U.S. military advantage. We are at a "moon shot" moment – we need national leaders with a vision, an urgent call to action, and far more robust and focused investment in the drivers of American competitiveness. These drivers include: increased federal investment in R&D with a focus on critical dual-use technologies, STEM education, 21st century infrastructure like 5G, incentives for enhanced collaboration between government, business and academia in priority areas like AI and unmanned systems, and a smarter immigration policy that attracts and keeps the best tech talent in the world. Speed is of the essence, and we are not moving fast enough given how rapidly the challenges we face are evolving.

The actions we take in the next few years could not be more critical. They must be driven by a broader strategic vision of the core values and interests we seek to protect. The United States must maintain its unique leadership role as a force for good in the world -- a defender of democracy, human rights, and the rules-based international order. We must also ensure our economy remains the most innovative and dynamic in the world, for it is the foundation of our global influence and our national security. And finally, the United States must maintain its ability to leverage all instruments of national power, not only defense, but also diplomacy, development, and economic influence. Only by harnessing all of these levers can the United States demonstrate the resolve and capability to compete effectively on the world stage, deter

war among the great powers, defend our interests, allies and partners, and, if necessary, fight and win in a far more challenging future.

Michèle Flournoy

is Co-Founder and Managing Partner of WestExec Advisors, and former Co-Founder and Chief Executive Officer of the Center for a New American Security (CNAS), where she currently serves on the board.

Michèle served as the Under Secretary of Defense for Policy from February 2009 to February 2012. She was the principal advisor to the Secretary of Defense in the formulation of national security and defense policy, oversight of military plans and operations, and in National Security Council deliberations. She led the development of the Department of Defense's 2012 Strategic Guidance and represented the Department in dozens of foreign engagements, in the media and before Congress.

Prior to confirmation, Michèle co-led President Obama's transition team at the Defense Department.

In January 2007, Michèle co-founded CNAS, a bipartisan think tank dedicated to developing strong, pragmatic and principled national security policies. She served as CNAS' President until 2009, and returned as CEO in 2014. In 2017, she co-founded WestExec Advisors, a strategic advisory firm.

Previously, she was senior advisor at the Center for Strategic and International Studies for several years and, prior to that, a distinguished research professor at the Institute for National Strategic Studies at the National Defense University (NDU).

In the mid-1990s, she served as Principal Deputy Assistant Secretary of Defense for Strategy and Threat Reduction and Deputy Assistant Secretary of Defense for Strategy.

Michèle is the recipient of numerous honors and awards, including: the American Red Cross Exceptional Service Award in 2016; the Department of Defense Medal for Distinguished Public Service in 1998, 2011, and 2012; the Chairman of the Joint Chiefs of Staff's Joint Distinguished Civilian Service Award in 2000 and 2012; the Secretary of Defense Medal for Outstanding Public Service in 1996; and CARE's Global Peace, Development and Security Award in 2019. She has edited several books and authored dozens of reports and articles on a broad range of defense and national security issues. Michèle appears frequently in national and international media, including CNN's State of the Union, ABC's This Week, NBC's Meet the Press, BBC News, NPR's Morning Edition and All Things Considered and PBS' News Hour, and is frequently quoted in top tier newspapers.

Michèle serves on the boards of Booz Allen Hamilton, Amida Technology Solutions, The Mission Continues, Spirit of America, The U.S. Naval Academy Foundation, CARE, and sits on the Honorary Advisory Committee of The Leadership Council for Women in National Security. Michèle is also a former member of the President's Intelligence Advisory Board, the CIA Director's External Advisory Board, and the Defense Policy Board, and is currently a member of the Council on Foreign Relations and the Aspen Strategy Group, and is a Senior Fellow at Harvard's Belfer Center for Science and International Affairs.

Michèle earned a bachelor's degree in social studies from Harvard University and a master's degree in international relations from Balliol College, Oxford University, where she was a Newton-Tatum scholar.

Written Statement of Senator Jim Talent

I want to thank the co-chairs for inviting me to share my thoughts on the state of the National Security Innovation Base (NSIB). I also want to commend you and the full Committee leadership for creating this task force. The existence of this bipartisan task force committee will signal to the Department of Defense how seriously the Congress takes the health of the NSIB, and that signal has value even apart from the legislation that will result from your work.

I'm sure you invited me because former Deputy Secretary Bob Work and I are currently co-chairing a task force on the NSIB for the Reagan Institute. We're pleased to have Congressman Banks on that task force, as well as Mr. Kim, Ms. Murphy, and Mr. Gallagher. Secretary Work and I will be eager to share with you our specific conclusions and recommendations after we issue our report in a month or so, but for now I think I can be most helpful in offering four general observations to help you frame your own investigation.

First, it's important for your task force to come to a common definition of the National Security Innovation Base. You can't direct and motivate the NSIB if you're not sure what it is, or if you don't understand the characteristics and incentives of the various actors in it.

Our Task Force spent a whole session on this issue and will in our report suggest a definition something like the following:

The NSIB is an enormous, pulsating and chaotic ecosystem of public and private actors including but not limited to the national security agencies, the National Laboratories, the great research universities, the traditional defense primes, the huge global tech companies, startup tech firms, and the venture capital community that regularly invests in groundbreaking research and technologies that are relevant to our national security.

The segments of the system both cooperate with and compete against each other. They have different goals, incentives, cultures and characteristics. In their efforts at innovation the private firms in the NSIB are working towards commercial ends and are often unaware, or at least not fully aware, of the national security implications of their work.

In contrast, China has a top down innovation system where all the actors, including the nominally private ones, are yoked together in harness to the authoritarians in Beijing. Our NSIB should not and cannot be like theirs, yet at the same time the government does need to coordinate and build partnerships within the system towards common goals.

During the Cold War, national security innovation was driven by DOD funding and conducted in government labs or by a relatively small set of private companies who could be expected to adjust to the culture and processes of the government. In today's NSIB much of the most important research is dual-use – driven by private actors for commercial purposes – which means the government will have to do a fair amount of adjusting itself to the commercial world.

So your task, as senior political leaders, is to focus the ecosystem on national security priorities, create a more comprehensive security consciousness among the private actors, and coordinate the segments enough to get the necessary synergies -- all without straightjacketing the creativity of the ecosystem or sacrificing the freedom, openness, and risk positive culture that is one of the NSIB's greatest strength.

It will be a difficult, delicate, long term and absolutely vital project.

My advice to the task force as a former Member is to be certain to take the time to learn from the various segments in the NSIB ecosystem and especially from the private actors in the tech world and the universities. Ask the players on the ground about the obstacles to partnering with the government and how the DOD can structure incentives so that the ecosystem more or less naturally bends its activities towards the technological priorities of the government.

The point is to push the ecosystem towards better integration and common goals at least mostly by aligning incentives rather than through highly prescriptive mandates.

Second, you are going to have to deal constantly with the natural tension within the NSIB between security and innovation – between defense and offense, if you will. Examples of this tension abound. We want our tech companies to be vibrant, benefit from capital market flows and gain market share; but we worry when they partner with foreign companies or accept foreign investment. We want to attract top level technical talent into our NSIB; but we know the PLA and Chinese intelligence agencies are very good at planting agents and infiltrating institutions to steal our technology. We want to partner more closely with allied countries in developing new technology; but that means giving those countries more freedom to have and handle our technology, with the attendant security risk.

My own belief, after months of work in our own task force, is that the government should build higher fences around fewer things. In other words, we need to do a better job of identifying and fencing off the really vital technology that only American actors control and can develop, while allowing the ecosystem freedom to share or sell technology that, as a practical matter, our national competitors can get no matter what we do.

My instinct is that Beijing is so good at stealing or appropriating the technology of others, and has devoted so many resources for so long to developing that capability, that we should plan on the assumption that offense will be more effective than defense, in the long run, in winning this competition.

But however you resolve the tension, it's important for the political leadership to recognize that there are important equities on both sides, that trade offs will be necessary, and that whatever you decide you must set clear rules that the whole ecosystem can understand. Uncertainty is the enemy of both security and innovation.

Third, I'm sure you are planning to inquire carefully into the efforts DOD is already making to energize and use the capabilities of the NSIB.

Our task force was particularly impressed with two DOD programs working to harness tech innovation—and innovators—to solve problems: Defense Digital Service and Hacking for Defense. The former approaches the problem from the inside out; the latter from the outside in. Both programs are shaking up the DOD enterprise by:

- Reinterpreting and reimagining mission challenges in useful ways;
- Bringing the best civilian tech talent to bear on behalf of national security;

- Breaking down cultural barriers, pulling the tech and defense worlds together, and creating a recruitment pool of tech talent for the future;
- Leveraging the knowledge of private tech leaders to seek out the best problem solvers for particular challenges;
- Introducing the DOD to other parts of the NSIB ecosystem (e.g. the academy, tech entrepreneurs);
- Acclimating our warfighters to thinking from a tech point of view about solving problems; and
- Blazing the trail in navigating around existing DOD processes to bring new innovation and energy to the Department.

Programs like these, which operate at the grass roots, are good ways to coordinate the NSIB ecosystem without straightjacketing its independence and dynamism. They may not be easy to scale, but if you study the characteristics that have made them successful, they can be models for similar efforts. The more visible successes you create in any part of the NSIB, the more likely it is that the ecosystem will see the value in these partnerships and spontaneously begin producing them without stimulus from the government.

Fourth and finally, one vital role for Congress to play is to give clear permission to the DOD to take greater risk with its procurement dollars where innovation is concerned. That is not a natural thing for the Department. Innovation is a risky business, whereas government is typically, and appropriately, risk averse with public funds.

When our task force visited Silicon Valley, I was greatly impressed by the attitude of tech investors. They knew that many of their investments would produce little return, and they accepted that as a necessary aspect of creating hugely successful enterprises with the investments that did succeed. They advised us that venture capital would invest much more, and much more often, in new and groundbreaking defense companies if programs like DIU had more discretion to give fewer, larger contracts to newer companies over a shorter time horizon.

In other words, if the Department is to succeed in getting breakthrough successes, it must have permission to fail. Of course we want due diligence to be done; of course we want public funds to be spent thoughtfully and purposefully. But we also want and need much greater private investment in national security throughout the NSIB ecosystem, and that will not happen if the government cannot acculturate itself to a higher level of risk.

I hope you will find ways to reassure those you oversee that you will have their backs when they take intelligent gambles on promising technology. In fact, your message to the Department should be: if all of your experiments succeed, it means that you are not experimenting nearly enough.

I thank the Co-Chairs again for the opportunity to testify and look forward to your questions.

Senator Jim Talent

was appointed by Senate Republican Leader Mitch McConnell for a two-year term expiring December 31, 2017. Senator Jim Talent is a national security leader who specializes in issues related to the Department of Defense. He has been active in Missouri and national public policy for over 25 years.

Senator Talent's public service began in 1984, when at the age of 28 he was elected to the Missouri House of Representatives where he served eight years, the last four as the Republican leader in the Missouri House.

In 1992, he was elected to the first of four terms in the U.S. House of Representatives where he represented Missouri's Second Congressional District. During his eight years in the U.S. House of Representatives, Talent co-authored the historic welfare reform bill, championed national security issues on the House Armed Services Committee, and enacted legislation to help revitalize distressed neighborhoods, both urban and rural. He was the Chairman of the House Small Business Committee from 1997-2001, where he worked on regulatory reform issues and on legislation to lower health care costs for small business people and their employees. Under Senator Talent's leadership, the Small Business Committee became one of the most prolific and bi-partisan in the House of Representatives, passing numerous bills without a single dissenting vote.

In 2002, Missourians elected Talent to serve in the United States Senate where he worked with Republicans and Democrats to enact critical legislation for Missouri. He served on the Senate Armed Services, Energy and Natural Resources, and Agriculture Committees. Working with Oregon Democrat Ron Wyden, Senator Talent was successful in securing critical funding through construction bonding in the highway bill. He and Senator Dianne Feinstein (D-CA) succeeded in passing the most comprehensive anti-methamphetamine bill ever enacted into law. Senator Talent was a leader on energy issues and was instrumental in the passage of the renewable fuel standard.

After leaving the Senate in 2007, Senator Talent joined The Heritage Foundation as a Distinguished Fellow specializing in military affairs and conservative solutions to poverty. In 2008, he served as Vice Chairman of the Commission on Prevention of Weapons of Mass Destruction Proliferation and Terrorism. In 2010, he served on the independent panel that reviewed the Quadrennial Defense Review of the Department of Defense. He also served on the independent panel that reviewed the Quadrennial Defense Review of 2014. He also has been a member of the executive panel advising the Chief of Naval Operations. Senator Talent was the first national figure outside Massachusetts to endorse Governor Mitt Romney for president in 2007 and was Governor Romney's senior policy advisor in both the 2008 and 2012 campaigns for president.

Senator Talent is an attorney and currently a Senior Fellow at the Bipartisan Policy Center and a Visiting Senior Fellow and Director, National Security 2020 Project, Marilyn Ware Center for Security Studies at the American Enterprise Institute. He earned his B.A. from Washington University in St. Louis and his J.D. from the University of Chicago Law School.

WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING

OCTOBER 29, 2019

RESPONSE TO QUESTION SUBMITTED BY MR. WALTZ

Ms. FLOURNOY. I am not sure I can give you a short answer to your very important question. But I do believe that the best way for the DOD to answer your question is to ramp up its efforts to develop joint and service-specific operational concepts to inform tough decisions about where to divest or accept and manage greater risk. The United States needs urgently to develop and test joint concepts, such as Multi-Domain Operations, and supporting service concepts, such as the Navy/Marine Corps' Distributed Maritime Operations, both of which are premised on eroding adversary advantages by creating simultaneous dilemmas across multiple domains, spreading out (rather than concentrating) the force across the theater of operations. Testing the technologies that will be most critical to operationalizing these concepts—from battle management networks to unmanned systems to long-range precision fires—will require a continuous, reinforcing cycle of wargaming, prototyping and experimentation. One way Congress can help would be to provide the services with robust funding to field small numbers of emerging capabilities for early-stage concept development and experimentation. For example, Congress should not hesitate to allow a service to acquire small numbers of AI-enabled unmanned systems of various types to facilitate the development of new concepts for human-machine teaming. Unfortunately, DOD and Congress now find themselves in a Catch-22—some appropriators want more clarity before they fund experimental systems, while the Department needs a certain number of these systems to experiment with in order to develop a compelling case for Congress to fund the capability long-term. It's time to break this logjam, accept a bit more risk in the short term, and allow the services to acquire the prototypes they need to enable an agile development process that includes robust field experimentation and iterative feedback from the warfighter. This is the only way we will be able to develop new concepts and capabilities fast enough to keep pace with our competitors. And it is this work that will ultimately enable us to have definitive answers to your question. [See page 27.]

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

OCTOBER 29, 2019

QUESTIONS SUBMITTED BY MS. HOULAHAN

Ms. HOULAHAN. Is the Department prepared to consider the ethical implications of artificial intelligence? I understand the Pentagon is looking to hire an AI ethicist, though just the one seems to be inadequate. Is there more the Department should do? If so, what?

Ms. FLOURNOY. I am encouraged by the Defense Innovation Board's release of its AI ethics principles and the positive response from the Department. The United States should continue to play a leadership role in setting the rules that will govern the ethical use of AI and other critical emerging, dual-use technologies. I agree with the DIB's recommendations that the use of AI should be governed by a continued commitment to develop, test, and deploy systems that reliable, equitable, traceable, and governable. I also believe that as the Department implements and formalizes these principles, DOD and Congress should engage with industry partners—both traditional primes and tech companies—to ensure greater cooperation in building and leveraging these capabilities.

Ms. HOULAHAN. I understand the Presidential Policy Directive 21 (PPD–21), which divvies up responsibilities within the Federal Government for cyber, was issued in 2013. Given the rapid development of cyber, do you have any insight into whether PPD–21 is due to be updated to reflect the developments in cyber? Are there other directives that are due for modernization that this committee could take action on?

Ms. FLOURNOY. [No answer was available at the time of printing.]

Ms. HOULAHAN. In nuclear policy, the concept of deterrence is founded in our understanding of our adversaries' nuclear capabilities and our adversaries' understanding our own nuclear capabilities. Do you have an understanding of what work is being done to establish global cyber norms? Further, is there work to be done on development of global cyber norms that is not currently being done?

Mr. TALENT. The Task Force did not inquire into the question of global norms for cyber or cyber deterrence theory. I am not familiar with efforts on a governmental level to establish such norms, other than the work in both the Obama and Trump Administrations regarding cyber espionage and cyber theft. I know Cyber Command is working out operational concepts and doctrine regarding its own capabilities. I certainly agree that these are vital concerns, given the power of cyber weapons, their escalatory potential, and the downside consequences of a miscalculation.