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.