CONGRESSIONAL TESTIMONY: FOUNDATION FOR DEFENSE OF DEMOCRACIES

House Armed Services Committee
Subcommittee on Cyber, Information Technologies, and Innovation

The Future of War:

Is the Pentagon Prepared to Deter and Defeat America's Adversaries?

RADM (RET) MARK MONTGOMERY

Senior Director
FDD's Center on Cyber and Technology Innovation

Senior Fellow
Foundation for Defense of Democracies

Washington, DC
February 9, 2023

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

Introduction

Chairman Gallagher, Ranking Member Khanna, and other members of the subcommittee, thank you for inviting me here today.

The United States Department of Defense (DOD), with the support of both Congress and the U.S. defense industrial base, has built the most powerful military force in the world. The United States has unmatched power projection capability, the ability to establish air and maritime dominance far from our shores, the resources to execute large scale ground maneuver operations, and the ability to conduct brigade-level amphibious operations. But despite all this, the United States will not be ready to deter and defeat America's most capable adversary — China — in the demanding technological environment we will face in the next five years.

This testimony will first discuss the People's Republic of China's build-up and the advantages it has in a Taiwan conflict, mainly geographic. Next, the testimony will address the five key steps the DOD/U.S. military as a whole must take to restore the balance of power. Third, the testimony will highlight four steps this subcommittee can take within its jurisdiction to facilitate the DOD-wide effort.

The Chinese Challenge

The United States has relied heavily on precision-guided munitions at range, large-scale military mobility and sustainment capacity, trained and empowered non-commissioned officers, and expansive intelligence collection and analysis capabilities to deter and, if needed, defeat adversaries. But our adversaries, particularly the Chinese, are investing in similar weapons and sensor systems, using emerging technologies to attempt to neutralize America's operational superiority and reduce the ability of U.S. forces to rapidly detect, track, and kill the adversary.

The Chinese military's capability and capacity growth has been meteoric. The Chinese Communist Party (CCP) was embarrassed by the military's relative impotence during the Third Taiwan Straits crisis of 1995-1996, when two U.S. carrier strike groups operated with impunity in the waters immediately off China's coast. The CCP has spent the past 25 years addressing that problem — building a military force designed specifically to place U.S. air and maritime operations at risk within the first island chains and soon will have the same impact within the second island chain. These Chinese investments in advanced technologies targeted observed U.S. weaknesses, such as the missile defense of ships and airfields, looking to create asymmetric advantages for Chinese forces. The Chinese also spent aggressively on technology that would marginalize existing U.S. advantages, such as military mobility and precision targeting. While the United States labeled China as the "pacing threat," the Chinese acted to develop and procure weapons as if the United States was actually *their* "pacing threat." Not surprisingly Chinese actions outperformed American rhetoric.

It is likely that current Chinese war plans will include a comprehensive pressure campaign that uses these emerging technologies to try and blind U.S. intelligence networks and silence our ability to communicate with forward forces, employ malicious cyber activity to weaken our critical infrastructure in order to both paralyze our military mobility and logistics enterprises and

bring America's economy to a standstill, and conduct a disinformation campaign to try and freeze national security decision making. The Chinese objective would be to deliver a strong signal to U.S. leaders about the vulnerabilities in our systems, ensuring the United States does not come to the support of its allies and partners.

This emerging technology challenge is complicated by a number of issues this committee cannot directly solve. The first is geography. The United States is trying to deter conflict in Taiwan and in the East or South China Seas, areas within 100 miles of Chinese ports and airfields but 8,000 miles from the U.S. West Coast. Second, China is also likely to have a "first mover" advantage — as an authoritarian regime with rapacious designs, they are much more likely to strike the first blow in a conflict. Finally, China maintains a strong advantage in the "gray zone," able to conduct operations that push the bounds of international law, lack transparency, and slowly, sometimes imperceptibly, establish advantage. While we cannot fix these problems directly, we need to acknowledge them.

Despite all these challenges, the United States can retain its military-technological superiority and, in the process, overcome China's asymmetric advancements, thus maintaining America's ability to project power and impose cost and ensuring the United States supports its allies and partners and the stability of the region. This effort will require targeted investments in multiple areas where the United States can develop and deploy new capabilities in ways that China will struggle to match.

Challenges and Recommendations for the HASC

There is a great deal that Congress and the Armed Services Committees can do to address the challenges posed by China. My colleague at FDD, Bradley Bowman, and I have written that recent war games have made clear that we need to: (1) increase procurement of long-range weapons to strike Chinese ships;[1] (2) develop and deploy cruise, ballistic, and hypersonic defense capabilities throughout U.S. basing in the Pacific; (3) pre-position munitions in Taiwan for their use in a contingency as we will not be able to resupply easily in a crisis (as we have in Ukraine); (4) resource and position Deployable Air Base Systems, so air assets can rapidly move around the theater;[2] and (5) train and exercise with Taiwan air and maritime forces. All of these actions — which need to be executed by other subcommittees of the HASC — will increase deterrence and, if a war comes, improve chances for success and reduce U.S. casualties — all at a fraction of the current defense budget.

Procuring Long Range Anti-Ship Missiles. In most unclassified wargames I have played, the U.S. forces required 1,000-1,200 of these weapons to allow U.S. airmen to stay at a relatively safe range and destroy the Chinese Navy. Unfortunately, the current U.S. inventory contains less than 250 of these missiles, and the Department of Defense has been comfortable procuring

[1] Bradley Bowman and Rear Adm. Mark Montgomery (ret.), "America's arsenal is in need of life support," *Defense News*, October 12, 2022. (https://www.defensenews.com/opinion/commentary/2022/10/12/americas-arsenal-is-in-need-of-life-support)
[2] Rear Admiral Mark Montgomery (ret.) and Bradley Bowman, "Washington is waking up on weapons for Taiwan," *Defense News*, December 19, 2022. (https://www.defensenews.com/thought-leadership/2022/12/19/washington-is-waking-up-on-taiwan)

between 38 and 88 of these a year for the past five years. At this rate the department would reach 1,200 missiles by 2035-2050, which is a bit late for comfort.[3] Additionally, these weapons are currently only launched from Air Force B-1s, which have poor readiness, and Navy F-18s, which are tied to aircraft carrier presence. The Air Force has been very slow in working to make the B-52 capable of launching these missiles. Sinking ships in a Taiwan Strait contingency must be a priority for the U.S. Air Force.[4] The Navy is also considering placing these missiles on P-8 surveillance aircraft. The HASC should continue its efforts to maximize missile production while strongly encouraging the services to expedite installation of missile launch compatibility on B-52s and P-8s.

Developing and Deploying Cruise, Ballistic, and Hypersonic Missile Defenses. One of the most salient lessons from the invasion of Ukraine is the impact of Russian cruise and ballistic missiles on Ukrainian critical infrastructure and the significant air defense capacity required to deter them. While the United States has both sea based and land based ballistic missile defense capabilities and has sufficient sea-based cruise missile defense capabilities, U.S. forces have significant gaps in protecting against cruise missiles attacking land-based targets and against all forms of hypersonic missiles.

In defending against cruise missiles targeting U.S. airfields, prepositioned equipment, ports, and logistics systems, the U.S. Army has failed to develop a follow-on mid-range air defense system to replace the Hawk systems, which were retired nearly 30 years ago. The Army has struggled to deliver the Indirect Fire Protection Capability (IFPC) system, which is now years late, and the Army refuses to consider procuring the National Advanced Surface to Air Missile System (NASAMS) that we have provided to Ukraine for the same mission and the National Guard deploys to protect you here in the National Capital Region. As a result, our airfields and logistics sites in the Pacific are left insufficiently protected against cruise missile threats.

The development of U.S. offensive hypersonic capabilities is starting to pace those of China and Russia. However, the development of U.S. hypersonic defensive countermeasures lags Beijing and Moscow's offensive efforts. The Missile Defense Agency (MDA) is still in the early stages of developing hypersonic defense systems — probably leveraging the Glide Phase Interceptor work — and the MDA will need to be both aggressive and lucky to pace Chinese offensive capability development. It would be especially worrisome and destabilizing if a "first mover" authoritarian state were to develop significant offensive hypersonic capacities before the United States and its allies had hypersonic defense capabilities.

There are also several revamped technologies that need to be brought into the air defense fight. Upgrading the outdated E-3 Sentry Airborne Early Warning and Control System (AWACS) aircraft to the new E-7 Wedgetail is a much-needed step. The department should also consider medium- and high-altitude persistent aerostats (dirigibles and balloons) with installed air defense

[3] Bradley Bowman and Rear Adm. Mark Montgomery (ret.), "America's arsenal is in need of life support," *Defense News*, October 12, 2022. (https://www.defensenews.com/opinion/commentary/2022/10/12/americas-arsenal-is-in-need-of-life-support)

[4] Bradley Bowman and Lt. Gen. Michael A. Loh, "Guarding Contested Skies," *Foreign Podicy*, January 27, 2023. (https://www.fdd.org/podcasts/2023/01/27/guarding-contested-skies); Bradley Bowman and Lt. Gen. Richard G. Moore, "Building the Air Force the U.S. Needs," *Foreign Podicy*, October 11, 2022. (https://www.fdd.org/podcasts/2022/10/10/building-the-air-force-the-us-needs)

radars for the defense of both Guam and the homeland. These are technologies the United States has excelled at but has been slow to exploit.[5]

Pre-positioning Munitions in Taiwan for Taiwan. Another important lesson from recent wargaming is the difficulty in re-arming Taiwan during a conflict. This is in stark contrast to Ukraine, where land borders with Poland, Slovakia, and Romania have facilitated re-arming and re-supply. In the case of a Chinese blockade or invasion of Taiwan, it will be nearly impossible to resupply Taiwan. Instead, this will require pre-positioning key munitions in Taiwan that the United States might want to transfer to Taiwan in a crisis, such as anti-armor missiles, air defense missiles, anti-ship missiles, and mines. Just such an effort was authorized in the FY 2023 National Defense Authorization Act, but no funding was appropriated to execute this task. Pre-positioning of munitions in Taiwan should be prioritized for appropriation in FY 2024 budgets.

Resourcing and Positioning Deployable Air Base Systems (DABS). The USAF Agile Combat Employment (ACE) operational concept is a key element in building resilience into regional U.S. air power capabilities. The concept relies on utilizing numerous airfields distributed throughout the theater — in Japan, Australia, the Marianas, the Compact States, and possibly the Philippines — in order to complicate Chinese targeting opportunities, from both military and political perspectives. To support this concept, the Air Force needs to expedite the procurement of thirty or more DABS for the Pacific theater — each system includes maintenance, runway repair, munitions handling, and air traffic control equipment. Despite Congress identifying this issue as early as 2018, the Air Force has struggled to procure sufficient Pacific positioned DABS units.

Training and Exercising with Taiwan Forces. The United States has not exercised with the Taiwan air and naval forces in theater in nearly 40 years. This failure to train together has left U.S. and Taiwan forces at the lowest level of operational partnership — "deconflicted" — which basically means your forces stay over there and our forces will stay located over here. To effectively counter Chinese military moves, the United States and Taiwan need to raise their level of operational partnership to "coordinated" or even "integrated." This will take significant operational exercises, table-top drills, and wargaming — all of which were authorized and directed in the FY 2023 NDAA after years of "sense of Congress" statements that such work was needed. Given the previous Department of Defense reluctance to conduct such bilateral exercises, Congress will have to carefully oversee and manage the department's efforts.[6]

---

[5] Bradley Bowman, Maj. Lauren Harrison, and Ryan Brobst, "Between E-3 And Eyes In Space, The Air Force Needs A Bridge, Now," *Breaking Defense*, October 5, 2021. (https://breakingdefense.com/2021/10/between-e-3-and-eyes-in-space-the-air-force-needs-a-bridge-now); Bradley Bowman and Rear Adm. Mark Montgomery (ret.), "Time To Wedge The E-7A Wedgetail Into The US Air Force Fleet," *Breaking Defense*, October 25, 2021. (https://breakingdefense.com/2021/10/time-to-wedge-the-e-7a-wedgetail-into-the-us-air-force-fleet); Bradley Bowman and Rear Adm. Mark Montgomery (ret.), "If The Air Force Buys The E-7A Wedgetail, What's Next?," *Breaking Defense*, October 26, 2021. (https://breakingdefense.com/2021/10/if-the-air-force-buys-the-e-7a-wedgetail-whats-next); Bradley Bowman and Maj. Brian Leitzke, "Let the Air Force let go of the E-3 'Sentry'," *Breaking Defense*, July 29, 2022. (https://breakingdefense.com/2022/07/let-the-air-force-let-go-of-the-e-3-sentry)

[6] Bradley Bowman and Rear Adm. Mark Montgomery (ret.), "Standing With the Free People of Taiwan," *Foundation for Defense of Democracies*, December 15, 2020. (https://www.fdd.org/analysis/2020/12/15/defending-forward-standing-with-the-free-people-of-taiwan)

Specific Challenges and Recommendations for the CITI Subcommittee

In this Cyber, Information Technologies, and Innovation (CITI) subcommittee, there are equally important steps that need to be taken to ensure U.S. forces are ready to deter and defeat America's adversaries in the demanding technological environment we will face in the next five years. At a minimum, this subcommittee should work to: (1) improve the cyber and information resilience of the military and the nation; (2) assess and strengthen the readiness and structure of U.S. Cyber Forces; (3) enable an environment where innovation is encouraged and risk is accepted; and (4) help allies and partners maintain interoperability with U.S. forces as they modernize.

Improve our Cyber and Information Resilience. In a contingency or conflict with China, U.S forces must maintain their ability to detect and track adversaries, communicate among forces, and mobilize and sustain forces. China's opening moves in any crisis or conflict, either to deter U.S. action or to defeat U.S. efforts, will be aimed at limiting or eliminating: the U.S. military's ability to sustain its operations logistically; the U.S. ability to see, track, and locate Chinese forces; and the capability of U.S. military leaders to command and control forces. Unable to communicate, deploy, or resupply, U.S. forces will be paralyzed. To avoid this situation, the U.S. military needs to build resilience, including through redundancies, across every link and node of its operations — from sensors to attack platforms, in information architecture and networks, across command-and-control systems, and at a pace commensurate with the threat. In addition to this cyber hardening, the United States will need to acquire large numbers of low-cost and expendable platforms that would support surveillance, communications, logistics, and strike — especially during the opening days of a campaign. This subcommittee can and should have a significant say in investments that protect the resilience of the military cyber and information enterprise.

This resilience will have to extend into our national critical infrastructure — the transportation systems, electrical power systems, water systems, financial systems, and other sectors that enable the mobilization and resupply of U.S. forces. Building such a resilience is a more burdensome process as it requires the development of a public-private collaboration that has not succeeded despite 20 years of government efforts. It is estimated that 85 percent of the national critical infrastructure is owned and operated by private sector or state and local utilities, not the federal government. This creates a defense challenge that is much more complex than traditional warfare areas, such as anti-submarine warfare or air defense, where all the assets are owned and operated by the U.S. military. The responsibility for this collaboration extends across multiple federal agencies and congressional committees, but this subcommittee can ensure that key elements of the public-private partnership are being addressed, such as establishing a cyber threat information collaboration environment (CTICE). This CTICE would consist of technical tools for information analytics and a portal through which relevant government and industry parties can submit and access cyber threat information from different sources across the federal government, including the intelligence community, with the requisite clearances and permissions. This subcommittee's former chairman, Rep Jim Langevin, attempted to champion just such legislation last year.

Assess and Strengthen U.S. Cyber Forces Readiness and Structure. Over the past decade, this subcommittee has provided extensive guidance and oversight to the development and employment of U.S. cyber forces. Despite this attention and inspired leadership from the U.S. Cyber Command, U.S. cyber forces are inconsistent in organization, readiness, and training across the military services. Additionally, the size of each service contribution to the cyber mission forces has not changed appreciably since the original agreements in 2012, despite significant changes in the cyber threat. As a result, the United States is not optimized for conflict with a Chinese adversary, which created a single military component in its Cyber Support Force back in 2016. This Chinese effort is improving in capability and already has a significantly (up to 10 times) larger capacity.

This subcommittee should address the challenges to U.S. cyber force posture across three issues: force readiness, structure, and operations. In the cyber force readiness area, the subcommittee should assess the inconsistent readiness of service cyber forces in light of the recently delivered cyber force structure review. The subcommittee should also evaluate the utilization and performance of the Pentagon's special hiring authorities for cyber professionals.

In the force structure area, the subcommittee should assess if the force design of Cyber Mission Force, conceived more then 10 years ago, can effectively produce forces for 21st century warfare, or if more dramatic solutions, such as an independent Cyber Force, should be considered, as was recently done with the Space Force. The committee should also look at the structure and responsibilities of the newly created Assistant Secretary of Defense for Cyber Policy and determine from what additional authorities the office would benefit.

In cyber force operations, the subcommittee should ensure that the principles laid out by the Congress in Section 1632 of the FY 2019 NDAA — supporting "defend forward" operations and increasing the level of U.S. efforts to impose costs on adversaries in cyberspace — are being adhered to. Additionally, the subcommittee should assess and encourage the development of both the offensive and defensive cyber capabilities of certain allies and partners, including Taiwan.

Enable an Environment to Innovate. The United States has learned some important lessons from the conflict in Ukraine, and the Department of Defense should be working to apply these same lessons in dealing with the defense industrial base. For example, the Ukrainians needed anti-ship cruise missiles to limit Russian Navy operations in the Black Sea. With no program of record available for a land-based Harpoon missile launching system, the Ukrainians had to work with Boeing, the Danish Army, and the U.S. Navy to "MacGyver" a cobbled together launcher system. Taiwan has asked for a similar land-based Harpoon system and was approved for purchase in 2020, but delivery of a "new design" system is not expected until 2027 or later. Clearly a similar "MacGyver" approach can and should be taken by Boeing and the U.S. Navy to ensure that a key partner has the weapon systems needed to deter Chinese action sooner than seven years after they ordered it.[7]

[7] Rear Admiral Mark Montgomery (ret.) and Bradley Bowman, "How 'MacGyver' magic can get Taiwan its Harpoon defenses faster," *Defense News*, December 7, 2022. (https://www.defensenews.com/opinion/commentary/2022/12/07/how-macgyver-magic-can-get-taiwan-its-harpoon-defenses-faster)

Similarly, Ukraine is desperately seeking air defense solutions for the Russian cruise missile challenge. As the Ukrainians ran out of Soviet-era missiles for their BUK-M1 launchers, they again worked to pull together a non-standard solution. The United States provided RIM-7 Sea Sparrow missiles that the Ukrainians rapidly integrated with their radar and fire control systems. This is especially impressive given the U.S. Army's 10-year-long unsuccessful struggle to build a similar medium-range air defense system from the ground up. The subcommittee should work to encourage a little more "MacGyver" and a little less "Valley of Death."

Help Allies and Partners Develop and Maintain Interoperability with U.S. Forces. The United States often modernizes its forces, including investments in software and command, control, and communications systems without sufficient consideration for the gap it creates in capabilities with our allies and partners which eventually lead to challenges conducting coalition operations. A number of issues can inflame this gap, including insufficient defense spending by partners and U.S. security (classification) concerns. The United States must address these challenges if it is to capitalize on one of its most enduring asymmetries against China — its network of alliances and partnerships. This is particularly true as the United States begins developing and fielding the Joint All Domain Command and Control (JADC2) architecture. This JADC2 system will clearly need a multilateral capability for key partners to participate in, including Japan, Australia, and eventually Taiwan, and in doing so, the U.S. will need to accept far greater risks in information sharing and transfer of technologies.

Conclusion

The United States and its allies and partners may not be on the right track to be ready for a conflict with China in the next five years, but they certainly can be, and this committee can help make that so. Targeted investments by the whole committee in anti-ship munitions, missile defense capabilities, prepositioned gear in Taiwan, air asset deployment capabilities, and exercising with Taiwan forces, will restore the U.S. ability to maneuver forward and reduce U.S. casualties — and all at a fraction of the current defense budget. This subcommittee can work to improve the cyber resilience of the military and the nation; bolster the capacity of the U.S. cyber forces; enable an environment where innovation is encouraged; and keep our allies and partners on step with us. All of these efforts will restore our ability to deter malicious Chinese efforts in the Western Pacific and — if deterrence fails — defeat Chinese aggression.