

Thursday, February 15, 2018
Tate Nurkin
Executive Director, Strategic Assessments, Jane's by IHS Markit
Testimony before the U.S.-China Economic and Security Review Commission
Hearing on "Implications of China's Military Modernization"

Introduction

I want to first thank the Commissioners for their invitation to participate in this hearing on the implications of China's military modernization. I think this is an important and timely topic as China's military modernization continues to build forward momentum in several capability and technology areas that have the potential to challenge U.S. military superiority in the region and affect U.S. capacity to pursue its interests and support its allies in the Indo-Pacific.

I have been asked to identify outputs and enablers of China's military modernization that pose the most consequential threats to U.S. military capabilities and to provide high-level recommendations of how best to mitigate the risks posed by these capabilities. My testimony is structured in four complementary sections.

The first section will offer a brief perspective on China's military modernization in order to frame assessments made in the rest of the testimony. Section two will discuss five linked capability areas and one enabler of modernization, focusing on providing high-level assessments of China's progress in these areas as well as why these capabilities are of particular concern. This list is not exhaustive or inclusive, but it does assess a compelling set of imminent and longer-term challenges to U.S. military superiority in the Indo-Pacific. The third section offers a series of high-level recommendations for maintaining U.S. advantage in its intensifying, accelerating and expanding military and geopolitical competition with China. The final section offers high-level additional recommendations for ensuring U.S. military superiority in its on-going competition with China.

Framing China's Military Modernization

China's military modernization is in the midst of three interlinked transitions, each in pursuit of a separate strategic objective.

The most immediately relevant and, for the United States, affecting transition is the shift in People's Liberation Army (PLA) posture from a land and territorial defense-focused anti-access / area-denial (A2/AD) force to a maritime – centric A2/AD force more capable of strategically managing the "near seas" and over time beyond.

The second transition acknowledges China's growing geopolitical influence and extra-regional interests and the need to build capacity to support and protect these interests. More frequent deployments to places like the Gulf States and ports in the Indian Ocean, along with the opening of China's first overseas military base in Djibouti all signal an ambition to project power, even in an environment in which China's most immediate military priority is targeting operational vulnerabilities of modern, high-tech militaries as part of a broader A2/AD approach. This transition in both mentality and capability is from a regionally-oriented force built to deny U.S. power projection efforts to a force capable of projecting power beyond the Western Pacific.

The third and over time possibly the most far-reaching, transition is rooted in a growing recognition that the availability and possible defense applications of novel Fourth Industrial Revolution

technologies¹, especially artificial intelligence (AI), are changing the nature of conflict and military capabilities.

Over the last decade-plus, China's force has been optimized to operate in the highly-"informatized" conditions of modern warfare that emphasize connectivity, networks, increased access to information and ease and pace of communications. These capability trends will be initially augmented and ultimately, over the next approximately two decades, superseded by the introduction and refinement of advanced 'cognitive' and autonomous capabilities and advanced manufacturing techniques. Underlying technologies of the future "intelligentization" of warfare are still in the development and testing phase, but China has clearly made an early play to invest in these technologies and the promise they hold to disrupt not just future conflict, but also current trajectories of China's competition with the United States.

Assessing the current state and future importance and trajectory of China's advanced weapons systems programs requires not just an understanding of the tensions, transitions, and varying priorities discussed above, but also analysis of four critical military domain area competitions.

The undersea competition: The United States has long-dominated the undersea domain. Both improved and planned Chinese capabilities—submarines, underwater surveillance nets, unmanned underwater vehicles (UUVs) other ASW capabilities—and a looming "valley"² in the actual size of the U.S. nuclear-powered submarine fleet (SSN) versus anticipated requirements will test U.S. undersea control, likely starting the middle of the next decade.

Missile versus missile defense: China's development of more, more accurate, and longer-range anti-ship cruise and ballistic missiles could overwhelmed by multi-axis saturation. New missile defense measures are being developed to meet this threat. The iterative interaction between new strike capabilities and novel means of providing missile defense will be a central feature of the China-U.S. (and Japan and South Korea) military competition in East Asia over the next two decades.

Space versus counter-space: The global competition in space is growing more crowded and more intense—particularly between the United States and China—as the reliance on space-based assets of modern militaries (and commercial communications) increases. These assets are critical for communication, navigation, intelligence collection, surveillance, target acquisition and reconnaissance. Control of what China's 2015 Military Strategy White Paper calls the "commanding heights" of space will be nearly essential to U.S. power projection efforts and China's attempts to deny U.S. access to the Indo-Pacific and globally project power.³

The electromagnetic spectrum: In both the heavily informatized environment of warfare today and the intelligentized environments of the more distant future, the ability of platforms and systems to send and receive signals, detect, surveil, and emit across the electromagnetic spectrum is critical to operational efficacy and success. For much of the last 15 years, the United States has operated more or less unchallenged in this domain. That is changing, in part because China has developed new organizational structures, operational concepts and platforms and systems to support its electronic warfare and cyber operations.

¹ Typically described as AI, cloud computing, advanced manufacturing, robotics, information technologies, blockchain, quantum computing, big data analytics, internet-of-things, virtual and augmented reality, biomaterials, smart sensors, smart materials, neuro technologies and energy capture and storage technologies

² O'Rourke, Ronald, "Navy Virginia Class (SSN-774) Class Attack Submarine Procurement: Background Issues for Congress," *Congressional Research Service*, October 24, 2017, 11–12. <https://fas.org/sgp/crs/weapons/RL32418.pdf>

³ USNI, "Document: China's Military Strategy," May 26, 2015, <http://news.usni.org/2015/05/26/document-chinas-military-strategy>.

Balances and imbalances in and across these competitions are critical to stability and security in the Western Pacific and to the capacity of the United States and its allies to pursue their interests in the region. They will also help shape the future of China's military modernization and its prioritized capability development.

Priority Threats to U.S. Military Capabilities and U.S. Ability to Sustain and Advance Security Interests

With this context in mind, it is clear that China's military modernization is driving new and intensifying challenges to the U.S. military and its capacity to project power to the Indo-Pacific and pursue U.S. security interests in the region. The capability areas discussed below are all at the top of an expansive list of specific capabilities that pose particularly robust threats to the U.S. military and U.S. military advantage.

Artificial Intelligence (AI)

China has aggressively invested in and pursued the development of AI as a means of ensuring economic growth and demonstrating and furthering national science and technology development. The result is that China is becoming a new center of gravity for AI research, even if China has not yet fully-closed the gap on U.S. leadership in the field.

Indicators of the growing prominence and scale of China's AI research are widespread. And while concerns about the quality of some of this high quantity of research and the nature of the citations are legitimate and dampen to a degree China's overall impact on international AI research, the broader point of China's growing influence holds. As Kai Fu-Lee, a Taiwanese-born AI researcher, former head of Google China, and current Chairman and Chief Executive Officer of Sinovation Ventures, effectively summarized: "It is indisputable that Chinese authors are a significant force in AI and their position has been increasing drastically in the past five years."⁴

In the defense and security context, China's military and political leadership appreciate that the PLA is at the start of changes that could transform warfare and the nature of the capabilities required to detect adversaries, deter and dissuade conflict and diminish, degrade and defeat adversaries. China's commitment to and progress in developing AI for national security and defense objectives is seen at multiple levels, including:

Policy Statements and Investments: The State Council's July 2017 release of the three-stage Next Generation Artificial Intelligence National Development Plan provided a direct and forceful indication of the overall importance the Chinese government is placing on China becoming the global leader in AI development and applications by 2030.⁵ The relatively short timeline of the plan—by comparison the Made in China 2025 plan also includes three stages covering a period from 2015 to 2049—underscores current perceptions of the health and competitiveness of China's AI research and industry efforts. The plan's third phase—which runs from 2025-2030—in particular, includes discussion of military and national security applications of AI.⁶

Autonomous Unmanned Systems Development: In June 2017, China Electronics Technology Corporation (CETC) successfully executed a world record test of 119 networked drones,

⁴ Markoff, John and Rosenberg, Matthew, "China's Intelligent Weaponry Gets Smarter," *New York Times*, February 3, 2017. <https://www.nytimes.com/2017/02/03/technology/artificial-intelligence-china-united-states.html>.

⁵ China Copyright and Media, "A Next Generation Artificial Intelligence Development Plan," July 20, 2017, <https://chinacopyrightandmedia.wordpress.com/2017/07/20/a-next-generation-artificial-intelligence-development-plan/>.

⁶ State Council of the People's Republic of China, "The State Council on the Issuance Notice of the New Generation of Artificial Intelligence Development Plan," July 20, 2017, http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm

demonstrating China's growing competence in a capability area that will be critical to future conflict and also highlighted the power of the intersection between AI and unmanned systems—discussed in more detail below.

Other Military Applications: In an August 2016 statement to *China Daily*, Wang Changqing of the China Aerospace and Industry Corporation, claimed that China's "future cruise missiles will have a very high level of artificial intelligence and automation . . . They will allow commanders to control them in real time manner, or to use a fire-and-forget mode, or even to add more tasks to in-flight missiles."⁷ This last function in this list indicates a missile with a cognitive capability to make targeting and navigation adjustments mid-flight absent human guidance or intervention based on its own autonomous reading of the operational situation.

China's investment in AI is at the top of the list of concerns for the United States because it presents China an opportunity to shift the nature of the competition itself. Rather than competing in capability areas in which the United States holds (and is likely to continue to hold) a relative advantage. China views AI investment as a means to get ahead of the U.S. in a new competitive environment that will have profound implications for future conflict.

And to be clear, while the United States currently retains overall global leadership in artificial intelligence, especially in core concepts, the prospect of China catching and subsequently surpassing the United States in military applications of AI technologies over the next decade – plus should not be discounted or dismissed. U.S. advantage will be tested, especially given the impressive range of levers and advantages that buttress and advance China's AI development, such as:

- An active AI research and academic community
- The scale of data available to China's high-tech companies and researchers, which subsequently informs AI application development and deployment
- A dynamic, opportunistic, and highly-competitive indigenous high-tech market environment and entrepreneurial culture. China's high-tech giants are competing to stay relevant in a market that demands rapid innovation and deployment of new commercial applications of AI
- Connections to Silicon Valley and the U.S. high-tech community, both through Chinese high-tech companies establishing research centers in the area and connections to individual leaders and scientists
- Talent recruitment, especially the repatriation of Chinese nationals from the U.S. high-tech industry and academic institutions
- The lure of China's commercial market for U.S. and Western firms and capacity to force U.S. companies to share data collected in China and to form joint ventures that provide China a mechanism for technology and knowledge transfers
- Top-down policy initiatives, funding, and incentives

The U.S. Department of Defense (DoD) sees China's development of AI as a real and urgent challenge and understands the need for vigilance in the development and protection of AI technologies.

Indeed, the DoD's Third Offset Strategy, an approach to achieving and sustaining U.S. superiority in military technology and capabilities, lists five types of AI capabilities as primary priorities for development: Autonomous deep learning systems, human-machine collaboration, assisted human

⁷ Lei, Zho, "Next Generation of Missiles to be Highly Flexible," *China Daily*, August 19, 2016. http://www.chinadaily.com.cn/china/2016-08/19/content_26530461.htm.

operations, advanced human-machine combat teaming and network-enabled, cyber-hardened autonomous weapons.⁸

In addition, former Deputy Secretary of Defense Robert Work touched on the potential risks to U.S. forces of adversaries, especially China, gain an advantage in algorithm-driven combat in a May 2017 speech to the U.S. DoD Applied Physics Lab: “Surprise is going to be endemic because a lot of the advances that the other people are doing on their weapons systems, we won’t see until we fight them. And if they have artificial intelligence then that’s better than ours, that’s going to be a bad day.”⁹

Unmanned Systems

China’s unmanned systems sector has experienced impressive growth since 2010, especially in military unmanned aerial vehicles (UAVs) where China’s defense and private sector have both demonstrated an impressive capacity to produce new designs and capabilities quickly.

China’s unmanned surface vehicles (USVs), unmanned underwater vehicles (UUVs), and unmanned ground vehicles (UGVs) programs are not as mature as its UAV programs, but notable progress in USVs, in particular, has occurred. At the 2017 International Ocean Science and Technology exhibition in Qingdao, China Aerospace Science and Technology Corporation (CASC) outlined its plans for a new family of four USVs aimed at addressing a range of maritime security and naval requirements and gaps to include high-speed patrol, hydrographical survey, ASW, fleet defense, surface warfare and surveillance.¹⁰

Across all categories of unmanned systems, these highly flexible and multi-mission capabilities present a particularly diverse set of strategic and operational challenges for the U.S. military:

Transition to “Intelligentized” Warfare: Swarms of AI-infused drones are likely to be a particularly prominent feature of the future battlefield, enabling groups of linked and autonomous drones to communicate with one another—absent control from platforms, systems or personnel—to carry out a specific mission. Each drone in the swarm may have a different role—for example, some may be equipped with surveillance payloads, others may carry weapons or electronic warfare capabilities, and others may be expendable, included in the swarm only to ‘light up’ adversary air defenses so that they can be targeted by other drones in the swarm or by other assets launching stand-off weapons. Redundancy is built into the swarm allowing for self-healing and adaptation, complicating efforts to defend against them. As a CETC engineer noted to state-owned media after the June 2017 test, UAV swarms will become “a disruptive force” that will “change the rules of the game.”¹¹

Because current operational concepts around drone swarms envision hundreds rather than dozens of individual systems in a swarm and because these swarms are resilient, redundant, self-healing and adaptive, capable of carrying out multiple missions or even altering the mission mid-flight, they present challenges to traditional concepts of air defense, in particular.

⁸ Remarks by Deputy Secretary of Defense Robert Work at the Center for New American Security Defense Forum, December 14, 2015. <https://www.cnas.org/publications/transcript/remarks-by-defense-deputy-secretary-robert-work-at-the-cnas-inaugural-national-security-forum>.

⁹ Freedberg, Sydney J., “War Without Fear: DEPSECDEF Work on How AI Changes Conflict,” *Breaking Defense*, May 31, 2017. <https://breakingdefense.com/2017/05/killer-robots-arent-the-problem-its-unpredictable-ai/>.

¹⁰ Wong, Kelvin, “CASC Unveils Next Generation USV Concepts,” *Jane’s International Defense Review*, 20 September 2017, https://janes.ihs.com/Janes/Display/FG_646729-IDR.

¹⁰ Wong, Kelvin, “CASC Unveils Next Generation USV Concepts,”

¹¹ Tate, Andrew, “China Launches Record-Breaking UAV Swarm,” *Jane’s Defense Weekly*, 21 June 2017, <https://janes.ihs.com/Janes/Display/jdw66273-jdw-2017>.

At an operational level, the sheer number of assets and their capacity to, in advanced concepts of future conflict, dynamically re-task could overwhelm and confuse existing air defense systems, especially if some of these systems are jamming the communication, navigation and targeting communications buttressing air defense systems. At a more strategic level, low cost drone swarms could further intensify U.S. DoD concerns about the cost-curves associated with air and missile defense. According to *Popular Mechanics*, “a few \$45,000 anti-air missiles are a cost-effective way to shoot down an \$18 million Reaper, but firing that same anti-air missile at a smaller, commercial drone isn’t as effective, especially when there are still 102 other drones flying the same mission at the same time.”¹²

Military Modernization and Domain Area Competitions: Unmanned systems, both in isolation and as part of larger multi-domain networks (i.e., land, air, surface and undersea), will support all three of China’s military modernization objectives identified above. UAVs, USVs and UUVs will be used for a range of missions: ISR, mine countermeasure operations, strike missions, electronic warfare, environmental monitoring, installation and force protection and command, control and communications function. China’s next generation of USVs will also reinforce China’s efforts to defend islands and installations in contested maritime boundary areas

Commentary accompanying CASC’s announcement of its new USV concepts is indicative of a growing recognition within the PLA that unmanned systems are indispensable to future maritime domain operations. As a CASC spokesman noted during the introduction of the D3000, “Over the next decade, we also expect to see the introduction of small to medium-sized USVs operating alongside manned platforms, particularly in leading navies, as the concept of mixed manned and unmanned fleets matures.”¹³ In this environment, demand for “autonomous ships, which offer a way to deliver increased operational capability without sending human crew into harm’s way, while at the same time reducing operating and build costs”¹⁴ will increase both within China and in the international market.

China’s ability to compete in the undersea competition by providing more, relatively inexpensive assets to help monitor the undersea domain and meet the challenge of U.S. increased investment in UUVs.¹⁵ China’s UUV and USV development will offer a new means of enhancing China’s ASW and even, over time, potentially offering a new offensive capacity as well. They will also likely play a role in the future development of China’s Great Undersea Wall of sensors in the Western Pacific being developed by China State Shipbuilding Corporation (CSSC) to help deny the U.S. and allied undersea assets access to the close-in undersea areas.

Geopolitical Relationships: China has become a viable defense exporter in many sectors in the last decade, especially in the export of its military UAVs, including the Wing Loong I, CH-3, and Ch-4.¹⁶ to states such as Saudi Arabia, Iraq, UAE, Egypt, Jordan, Kazakhstan, Turkmenistan, Nigeria, Pakistan, Myanmar and Bangladesh.

¹² Atherton, Kelsey D., “Pentagon’s new drone swarm heralds a future of autonomous war machines,” *Popular Science*, 10 January 2017, <https://www.popsci.com/pentagon-drone-swarm-autonomous-war-machines>.

¹³ Wong, Kelvin, “China’s CASC unveils D3000 unmanned oceanic combat vessel concept,” *Jane’s International Defense Review*, September 18, 2017, https://janes.ihs.com/Janes/Display/FG_645421-IDR.

¹⁴ Wong, Kelvin, “China’s CASC unveils D3000 unmanned oceanic combat vessel concept,” *Jane’s International Defense Review*, 18 September 2017, https://janes.ihs.com/Janes/Display/FG_645421-IDR.

¹⁵ Pomerleau, Mark, “DOD Plans to Invest \$600M in Unmanned Underwater Vehicles,” *Defence Systems*, February 4, 2016, <https://defensesystems.com/articles/2016/02/04/dod-navy-uuv-investments.aspx>.

¹⁶ Grevatt, Jon, “Indonesia Looks to China for Combat UAVs,” *Jane’s Defense Weekly*, 28 July 2017, https://janes.ihs.com/Janes/Display/FG_600842-JDW.

The main benefit of these export sales for China is not about funding streams. Rather, they serve as a mechanism to deepen industry and then geopolitical relationships with states that either sit atop key energy and resource reserves or can serve as a hedge against India. Add to this China's recent efforts to sell unmanned aerial vehicles into Southeast Asia and at least one state with an active claim in the South China Sea. In late July 2017, *Jane's Defense Weekly* reported that Indonesian officials have outlined a program to procure UCAV from China. The exact requirement is still being finalized, but features six UCAV units each consisting of three batteries. More recently, the Wing Loong I and II were both displayed at the Singapore Air Show, Asia's largest airshow, in February of 2018, as a means of engaging other Southeast Asian states in order to influence behaviors, policies and perspectives.¹⁷

Counter-Space Capabilities

China's focus on AI and to a degree unmanned systems constitutes a risk to the United States because it presents a pathway for China to create military advantage by beating the United States to the commanding heights of cognitive warfare by the start of the 2030s. In the shorter-term, though, China's military modernization represents more immediate challenges through weapons systems that target the command, control, communication, computers, intelligence, surveillance, target acquisition and reconnaissance (C4ISTAR) vulnerabilities inherent in modern, highly-connected militaries.

The modern "informatized" operational military environment is largely defined by the importance of networked forces being able to communicate with one another to enable C4ISTAR tasks. These communications can take place through many mechanisms and across many domains, including through satellites based in space.

The United States has an extensive and resilient space-based infrastructure and relies on this infrastructure and the advantages it confers to bring to bear the full weight of its power projection and warfighting capabilities throughout the world. China's A2/AD modernization acknowledges the strength of the U.S. military and of its space-based architecture. It also understands that U.S. reliance on space assets constitutes a strategic and operational vulnerability to be exploited.

The result has been a diverse counter-space program with demonstrated capabilities in four categories of counter-space weapon:

- Direct Ascent Anti-Satellite (ASAT) Weapons
- Co-Orbital ASAT weapons
- Directed energy weapons
- Cyber hacking that can disable satellites for several minutes or perhaps longer.¹⁸

Air Force Major General Nina Armagno summarized the outcome of the existence of these weapons by warning that "Russia and China, by the year 2025, will be able to hold at risk every one of (U.S.) satellites in any orbit."¹⁹ This despite continued efforts to develop new technologies and operational concepts, such as disaggregation and development of microsatellites, to mitigate risk and

¹⁷ Wong, Kelvin, "China's Wing Loong UAV family makes Southeast Asian debut", *Jane's Defence Weekly*, February 5, 2018, http://www.janes.com/article/77587/singapore-airshow-2018-china-s-wing-loong-uav-family-makes-southeast-asian-debut?utm_content=buffer29d0&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

¹⁸ U.S.-China Economic and Security Review Commission, "China's Space and Counterspace Programs," *2015 Report to Congress*, November 2015, http://origin.www.uscc.gov/sites/default/files/annual_reports/2015%20Annual%20Report%20to%20Congress.PDF.

¹⁹ Lambakis, Steve, *Foreign Space Capabilities: Implications for U.S. National Security*. Report, pg. 43. <http://www.nipp.org/wp-content/uploads/2017/09/Foreign-Space-Capabilities-pub-2017.pdf>.

vulnerability of U.S. space-based infrastructure. A particularly successful Chinese counter-space campaign could degrade or deny U.S. access to space and ensure U.S. forces could not effectively “see,” “sense” or “hear,” much less navigate, target and communicate. Asymmetric denial of U.S. space assets is the ultimate game-changer and game-leveler in military capabilities.

The Strategic Support Force, Integrated Network Electronic Warfare and the Electro-Magnetic Spectrum

China’s counter-space capabilities and, in part, its burgeoning unmanned systems capability are part of a broader suite of capabilities—to include cyber capabilities, specialized platforms, and directed energy weapons—designed to gain ascendancy in the electro-magnetic spectrum and electronic warfare.

Former Chief of Naval Operations Admiral Jonathan Greenert described the importance of the electromagnetic spectrum in 2016:

“The electromagnetic spectrum is an essential—and invisible—part of modern life [military and civilian]. Our military forces use wireless computer networks to coordinate operations and order supplies, use radars and sensors to locate each other and the enemy, and use electronic jammers to blind enemy radars or disrupt their communications. With wireless routers or satellites part of almost every computer network, cyberspace, and the electromagnetic spectrum now form one continuous environment.”²⁰

China’s efforts to gain advantage in this competition in the electromagnetic spectrum and in the closely linked cyber and space domains have involved the development of new organizational structures, operational concepts and military capabilities, all of which combine to pose a more coordinated and robust threat to U.S. and allied military capabilities and potentially to undermine U.S. ability to pursue its interests in the Indo-Pacific.

In November of 2015, China established the Strategic Support Force (SSF) as a military service level organization reportedly “equal in standing to China’s army, navy, air force and missile service.”²¹ The SSF reportedly combines three former PLA cyber, EW and intelligence services components and is responsible for coordinating and executing electronic warfare, space / counter-space and cyber warfare activities.²²

The establishment of SSF accelerates China’s challenge to the United States in the electromagnetic spectrum and “reflects the on-going Chinese effort at being able to establish ‘information dominance.’”²³ It is also central to China’s efforts to achieve more fully execute operations associated with the concept of “integrated network electronic warfare”²⁴ (INEW). According to Michael Raska, Assistant Professor at the S. Rajanatham School of International Studies in Singapore,

²⁰ Wilson, J.R., “Today’s battle for the electromagnetic spectrum,” *Military and Aerospace Electronics*, 27: 8. <http://www.militaryaerospace.com/articles/print/volume-27/issue-8/special-report/today-s-battle-for-the-electromagnetic-spectrum.html>.

²¹ Gertz, Bill, “Chinese Military Revamps Cyber Warfare, Intelligence Forces”, *Washington Free Beacon*, January 27, 2016, <http://freebeacon.com/national-security/chinese-military-revamps-cyber-warfare-intelligence-forces/>

²² Gertz, Bill, “Chinese Military Revamps Cyber Warfare, Intelligence Forces”, *Washington Free Beacon*, January 27, 2016, <http://freebeacon.com/national-security/chinese-military-revamps-cyber-warfare-intelligence-forces/>

²³ Gertz, Bill, “PLA’s new Strategic Support Force remains an enigma”, *Washington Free Beacon*, December 18, 2017, <http://freebeacon.com/national-security/asia-times-plas-new-strategic-support-force-remains-enigma/>

²⁴ Raska, Michael, “China’s evolving cyber warfare strategies”, *Asia Times*, 8 March 2017, <http://www.atimes.com/article/chinas-evolving-cyber-warfare-strategies/>

“In Chinese strategic thoughts, INEW has a holistic representation that combines coordinated use of cyber operations, electronic warfare, space control and kinetic strikes designed to create ‘blind spots’ in adversary C4ISR systems.”²⁵

And this effort is being supported by more, more robust and more prominently featured capabilities. *Xinhua* reporting on the July 2017 PLA parade in Inner Mongolia marking the 90th anniversary of the PLA’s founding highlighted the presence of “16 items of the PLA’s latest electronic warfare equipment that can disrupt enemy radar and communication in air defense and field battles.”²⁶ Among those 16 items were “two models of electronic reconnaissance vehicles, a Y-8 electronic jamming aircraft and a group of military drones that can ‘paralyze and suppress’ enemy early-warning and command communications systems.”²⁷ China has also used directed energy systems to jam platform or system signals or dazzle (i.e., inhibit the capacity of radars or sensors to ‘see’) platforms and systems.²⁸

The confluence of capabilities, concepts and structures is taking place at a time in which the DoD is coming to terms with potential vulnerability in the electromagnetic spectrum after two decades of under-appreciation of the potential for intense and affecting competition in this area. According to Dr. William Conley, the Deputy Director of Electronic Warfare in the Office of the Undersecretary of Defense for Acquisitions, Technology and Logistics “the foot is fully on the gas pedal”²⁹ within DoD to make up for “twenty – five years of inattention” to electronic warfare.³⁰

Maneuverable Reentry Vehicles (MaRVs): Anti-Ship Ballistic Missiles and Hypersonic Glide Vehicles

MaRV-equipped weapons provide many advantages over traditional ballistic missiles, most notably their ability to maneuver toward their target, potentially taking an irregular or unpredictable path and providing the missile a better opportunity to defeat even the most advanced missile defense systems. In addition, the maneuverability of the warhead enables MaRV-equipped ballistic missiles to hit moving targets.

China’s DF-21D and DF-26 anti-ship ballistic missiles (ASBMs) are thought to be equipped with MaRV warheads.³¹ Much has been written about these systems and their capacity to target U.S. aircraft carriers at long ranges and thereby hold at risk the primary engine of U.S. power projection. These systems are currently deployed, but also vulnerable to U.S. counter-measures against the systems’ reconnaissance –strike complex.

China’s MaRV programs also include its hypersonic glide vehicle (HGV) program, which revolves around the HGV known as the DF/ZF. China has completed seven tests – six successful—of its HGV programs. HGVs are able to travel at speeds above Mach 5 and maneuver to their targets and, as such, are seen as being able to dramatically alter the missile versus missile defense competition.

²⁵ Raska, Michael, “China’s evolving cyber warfare strategies”, *Asia Times*, 8 March 2017, <http://www.atimes.com/article/chinas-evolving-cyber-warfare-strategies/>

²⁶ “China displays electronic warfare equipment at Army Day parade”, *Xinua*, July 29, 2017, http://www.xinhuanet.com/english/2017-07/30/c_136485220.htm

²⁷ “China displays electronic warfare equipment at Army Day parade”, *Xinua*, July 29, 2017, http://www.xinhuanet.com/english/2017-07/30/c_136485220.htm

²⁸ Lin, Jeffrey, and P.W. Singer. “Here’s how China is battling drones,” *Popular Science*. March 28, 2017. <http://www.popsci.com/chinas-new-anti-drone-weapons-jammers-and-lasers#page-2>.

²⁹ Conley, Dr. William, “State of Electronic Warfare in the DoD,” speech at the Mitchell Institute of Aerospace Studies, June 22, 2017, https://www.youtube.com/watch?v=qR_PPGDnejo.

³⁰ Conley, Dr. William, “State of Electronic Warfare in the DoD,” speech at the Mitchell Institute of Aerospace Studies, June 22, 2017, https://www.youtube.com/watch?v=qR_PPGDnejo.

³¹ Fisher, Richard D, “US officials confirm sixth Chinese hypersonic manoeuvring strike vehicle test,” *Jane’s Defense Weekly*, November 26, 2015.

China is still developing HGV maneuverability and the capacity to communicate with the system at such high speeds. It is not expected to come into service for several more years, perhaps not until the late 2020s.

China's main motivation for its program is clear, most notably to counter-act the diminishing effect it believes ever-advancing U.S. missile defense capabilities are having on its strategic and conventional deterrent. China also seeks to match U.S. development of hypersonic weapons being made through the U.S. Prompt Global Strike program.

The success and, critically, continued prioritization of China's MaRV programs, especially HGVs, pose a short and medium-term risk to U.S. military capabilities and regional interests in three ways.

Holding at Risk Critical U.S. Capabilities: A more mature ASBM capability equipped with maneuverable warheads could hold at risk the U.S. Navy's surface fleet and carrier battle groups, a significant component of current U.S. capacity to project power in the Indo-Pacific and meet the PLA's on-going transition to a more maritime posture. The combination of the hypersonic speeds and maneuverability of HGVs would eliminate the reliability of existing missile defense systems. Absent effective deployment of low cost of shot missile defense measures capable of hitting both ASBMs and HGVs—electromagnetic rail guns, hyper-velocity weapons and directed energy, for example—or deterring, dissuading or stopping the launch of these weapons in the first place—to include 'left of launch' interventions—China's MARVs will significantly erode the U.S. ability to protect assets and allies in the Indo-Pacific.

Destabilizing Regional Security: HGVs constitute a particularly destabilizing weapon, upsetting traditional expectations of both nuclear and conventional deterrence and serving to weaken regional security mechanisms. The perception of HGVs as being "unstoppable"³² and able to defeat current missile defense systems—even if there may be means to respond to HGVs in the future—create inducements and incentives for preemptive strikes, a particular anxiety in times of heightened bilateral U.S.-China tension coupled, as has happened since the mid-2000s, with Chinese assertiveness along its Asian periphery in the South China Sea and East China Sea, in particular.

Falling Behind: China has made demonstrable progress in its hypersonics research in the last decade. In addition to the seven tests of the DF/ZF HGV, China has built the world's largest hypersonic testing wind-tunnel and has made progress in ramjet and scramjet engines for a hypersonic cruise missile.³³ There is a growing expectation within the U.S. defense and security communities of future production and deployment by the end of the next decade.

As a result, the United States and its technologically competent defense partners, have little choice but to match and, if possible, regain superiority in hypersonic platform capability. As former Acting Assistant Secretary of Defense Alan Shaffer noted, "We, the United States, do not want to be the second country to understand how to control hypersonics."³⁴

But there is some indication that this may, in fact, be what is happening, due both to advancement of China's program and a perception that the United States, much like with electronic warfare capabilities, has not been attentive in maintaining its advantage. In January of 2018, Air Force

³² Freedberg, Sydney J. "Speed Kills: The Case for Hypersonic Weapons," *Breaking Defense*. June 3, 2014, <https://breakingdefense.com/2014/06/speed-kills-the-case-for-hypersonic-weapons/>

³³ Norris, Guy, "China Reveals Key Test Progress On Hypersonic Combined-Cycle Engine," *Aviation Week*, 10 April 2017, <http://aviationweek.com/technology/china-reveals-key-test-progress-hypersonic-combined-cycle-engine>.

³⁴ Machi, Vivienne, "Future Weapons: Rivals Push Pentagon to Boost Funding for Hypersonics Research," *National Defense*, June 26, 2017, <http://www.nationaldefensemagazine.org/articles/2017/6/26/future-weapons-rivals-push-pentagon-to-boost-funding-for-hypersonics-research>.

General Paul Selva, the Vice Chairman of the Joint Chiefs of Staff, starkly claimed that “We have lost our technical advantage in hypersonics.” General Silva did qualify his statement by saying that the United States has not yet “lost the hypersonics fight”, but he also stressed that China (and Russia) have “moved out pretty smartly” on hypersonics. China, in particular, has been “willing to spend tens to hundreds of billions of dollars on its program.”³⁵ This capacity to spend more or less without meaningful constraint on programs supported and prioritized by the Chinese Communist Party (CCP) is a consistent and common enabler of science and technology success for China, especially in quantum computing and encryption and artificial intelligence.

China’s Technology Acquisition Strategies: A Key Enabler of China’s Defense Industrial Base

Narratives about China’s inability to innovate in key defense capabilities or challenge the United States and its allies in fielding exquisite technologies should be reconsidered, especially in light of China’s recent success in quantum computing and encryption, AI, hypersonic flight, networked unmanned systems and even deep sea exploration as well as general indicators of advancement of the technical capacity of China’s defense industrial base.

At the core of this success is China’s technology acquisition program, another critical aspect of China’s military modernization that, if unchecked, will constitute a challenge to U.S. ability to sustain military and technological advantage over China and other actors.

China’s technology acquisition efforts are directed, aggressive, sophisticated, multi-faceted and concentrated on an impressive array of technologies with a particular focus in 2016, according to the U.S. Defense Security Service in “electronics, aeronautic systems, and C4 technologies.”³⁶

While cyber-theft, solicitation, and espionage of various kinds are still used and highly-effective, China has also benefitted from—and, critically, *will continue to benefit from*—growing intersections between commercial and military technologies and a defense innovation environment in which products from high-tech firms and applied research institutes are frequently the catalyst for new and cutting-edge defense and security capabilities. In this environment China is pursuing several predominantly licit acquisition methods, which are now vital to China’s military modernization and, especially, efforts to develop Fourth Industrial Revolution technologies:

- Inter-governmental and academic science and technology relationships
- Use of Chinese students studying in the United States
- Delegation visits
- Exploitation of a growing range of useful open sources
- Conferences, conventions, and trade shows
- China’s dual-use space program
- Joint ventures with U.S./Western companies

An investigation of China’s inter-governmental and academic science and technology relationships highlights the scale and dimensions of the challenges the United States faces in protecting its own commercial, dual-use, and military technologies and managing the diffusion from other actors of

³⁵ Morgan, Wesley, “Selva: We have lost our technical advantage in hypersonics”, *Politico*, January 30, 2018, <https://www.politicopro.com/defense/whiteboard/2018/01/selva-we-have-lost-our-technical-advantage-in-hypersonics-503866>

³⁶ “Targeting U.S. Technologies 2017: A Trend Analysis of Cleared Industry Reporting”, Defense Security Services, September 7, 2017, http://www.dss.mil/documents/ci/2017_CI_Trends_Report.pdf. The report is careful to not name specific countries and therefore refers only to four regions, including East Asia and the Pacific. It is reasonable to assume that trends and insights regarding East Asia and Pacific region technology acquisition efforts effectively represent the trends in China’s technology acquisition program.

advanced commercial and applied research developed technologies that also have military and security purposes.

According to a January 2017 statement released by China's Ministry of Science and Technology (MOST), China has S&T relationships with 158 "countries and regions," including inter-Governmental science and technology accords" with 111 of these countries and regions. MOST asserted that these agreements allow for China to "integrate into the global network of scientific and technological innovation"³⁷ and, therefore, they are an input into China's civil-military fusion efforts that facilitate technology transfer from commercial and civil enterprises to China's defense industrial base.

One of these programs, established in April 2017, is an agreement between CETC—a member of China's defense industrial base with commercial and civil interests as well—with University of Technology Sydney in Australia to establish the Australia-China Research Innovation Centre in Information and Electronics Technologies. CETC will provide \$20 million over five years for the initiative, which will engage in research programs focused on several Fourth Industrial Revolution technologies, all of which have important defense applications:³⁸

- Big data technologies (mobile sensing and communications, electromagnetic metamaterials and devices, big visual data analytics, transfer learning, and Internet of Things)
- Quantum computing and quantum communications
- AI
- Simultaneous localization and mapping, assisted robots and robots for infrastructure monitoring and maintenance
- Advanced materials and electronics (THz devices, environmental and industrial sensors and integrated circuits)

Capabilities and Technologies

China's military modernization—pursuing objectives across three transitions and seeking to alter strategic and operational balances in domain area competitions—poses complex and durable challenges to the U.S. military's capacity to operate and press U.S. interests in the Indo-Pacific. Meeting these challenges and mitigating risk from them over the next three decades requires an understanding of the nature of the conflict, gaps and vulnerabilities in U.S. capabilities and, ultimately, investment in specific capability and technology areas.

Prioritizing capabilities and (re) gaining superiority: A thorough review of recent developments across a range of advanced weapons systems of interest to both the United States and China reveals several instances in which U.S. superiority in critical technology and capability areas is being called into question. For example, in June 2017, China claimed that it had leap-frogged the United States in integrated electronic propulsion systems (IEPS).³⁹ The claim is apocryphal, and it is not surprising, nor *necessarily* worrying that China would make such claims.

What is worrying, though is when similar statements about U.S. advanced technology programs are made by U.S. defense leaders, such as Dr. Conley's and General Silva's comments referenced above (about U.S. electronic warfare and hypersonic developments respectively). Both of these comments

³⁷ Grevatt, Jon, "China Grows Its International Technology Network," *Jane's Defense International*, January 19, 2017. <https://janes.ihs.com/Janes/Display/jdin91289-jdin-2017>.

³⁸ *University of Technology Sydney*, "Joint IET Research Centre with China Electronics Technology Group Company," April 26, 2017. <https://www.uts.edu.au/about/faculty-engineering-and-information-technology/news/joint-iet-research-centre-china>.

³⁹ Jane's by IHS Markit. "Chinese navy claims lead in IEPS development," June 5, 2017. <https://janes.ihs.com/Janes/Display/jdw66061-jdw-2017>.

suggested that China (and others, including Russia) had either closed the gap or inched ahead in key technology areas in large part because they had been more aggressive and attentive to these technology areas than had the U.S. DoD, which only regained focus after the full scope of China and Russia's advancement was revealed. Indeed, Dr. Conley's exact comment was that "the foot is fully on the gas pedal"⁴⁰ within DoD to make up for "twenty – five years of inattention" to electronic warfare.⁴¹

This dynamic, which one can argue is also seen in China's advancement in AI, drone swarms and, quantum encryption, can be slowed and reversed through effectively prioritizing the most important military competitions—the undersea domain, missile versus missile defense, space and the electromagnetic spectrum are all good places to start—and comprehensively assessing the capabilities required to retain U.S. pre-eminence both now and into the future.

A list of initial capabilities features:

- Unmanned systems (UAVs, USVs, and UUVs)
- Deep magazine, low cost of shot air and missile defense capabilities (electromagnetic rail guns and / or hypervelocity guns and directed energy weapons)
- HGVs
- Reusable space launch
- Microsatellites
- Advanced position, navigation and timing capabilities, including the capability to navigate absent information from Global Positioning System satellites or other global navigation satellite systems
- Adaptive and cognitive EW
- Advanced and remote sensors

Core technologies: Maintaining advantage in these competition and capability areas will require the United States to invest in emerging supporting and enabling technologies. This list of supporting technologies is a long one, though the five technology areas discussed below are especially relevant:

- *Artificial intelligence and big data analytics:* Certainly, maintaining U.S. advantage in AI concepts and defense applications is a powerful priority for the U.S. DoD as part of an effort to lead the way toward an era of cognitive warfare, as evidenced by the five AI technology areas prioritized in the Third Offset Strategy. AI is a foundational technology for development of drone swarms, which will present vexing problems for China, just as Chinese swarms will test U.S. air defense concepts and capabilities.

But AI has several other applications for the future of military capabilities and intelligence and decision-making and for the future of U.S. competition in military capabilities with China. For example, AI applications will be core to cognitive electronic warfare capabilities designed to retain dominance of the electromagnetic spectrum, already under-development by the United States. Cognitive electronic warfare systems will enable U.S. platforms to enter into any environment with no information about adversary electronic warfare systems and independently and rapidly identify the capabilities they face and formulate countermeasures. According to Jane's C4ISR desk analysts, effective and rapid development

⁴⁰ Conley, Dr. William, "State of Electronic Warfare in the DoD," speech at the Mitchell Institute of Aerospace Studies, June 22, 2017, https://www.youtube.com/watch?v=qR_PPGDnejo.

⁴¹ Conley, Dr. William, "State of Electronic Warfare in the DoD," speech at the Mitchell Institute of Aerospace Studies, June 22, 2017, https://www.youtube.com/watch?v=qR_PPGDnejo.

of cognitive electronic warfare “will provide the United States with a decisive advantage within the critical EW [electronic warfare] domain.”⁴²

More generally, but still highly-relevant to meeting the challenges posed by China’s military modernization, AI will also support the necessary enhancement of perception and processing of information and design and execution of new approaches for both humans and machines to queue, synthesize, digest, and discern information. These new approaches are necessary cope with complex and fast – moving strategic and operational contexts that will be marked by a surfeit of available information of variable quality and timeliness arriving at increasing velocities.

- *Power and energy capture and storage:* Power limitations are a potential “long pole in the tent” for advancement of several types of U.S. military capabilities referenced above, particularly unmanned systems and electromagnetic rail guns. As the U.S. military (as well as others), ask unmanned systems to carry out more missions and carry more sensors and more powerful payloads, it will also need to develop more efficient means of powering these sub-systems and payloads while not adding size, weight or significant cost.

Energy capture and storage and propulsion technologies will also be critical for unmanned systems and other advanced platforms as they seek to balance the general need for persistence—the ability to stay on mission for longer durations at longer ranges—with the need to stay relatively low observable in operational environments that are likely to have more and more powerful sensors.

Power is also a concern for electromagnetic railguns, which require a tremendous amount of energy to operate and need to be able to store this energy to be able to fire on-demand. According to a June 2016 *Popular Mechanics* article, “The problem (with railguns) is that the only ships that will be able to generate the gargantuan 25 megawatts of power (enough to power almost 19,000 homes) required to fire the railgun are the Zumwalt-class destroyers, which will use Rolls-Royce turbine generators to produce as much as 78 megawatts of power for the ship.”⁴³

- *Information security:* China’s cyber capabilities and its successful development in quantum computing and encryption have not been touched on in much detail in this testimony. However, they are part of a strong focus on the information domain rooted both in a sense of vulnerability—amplified by information contained in the Edward Snowden leaks that showed that China was “always being hacked”—and opportunity to use cyber weapons to exploit vulnerabilities in the high-tech, highly-networked U.S. military and defense industry. China’s investment in cyber technologies and in quantum encryption, in particular, will continue, requiring a U.S. response in order to both protect U.S. information and to continue to carry out effective offensive cyber operations against China. U.S. investment in quantum encryption as well as other novel technological approaches to cyber-defense, such as blockchain, will be warranted to keep pace with China in this domain area.
- *Advanced materials:* In July of 2017, U.S. Army Chief of Staff General Mark Milley noted that the nature of future armored vehicles and main battle tanks would be determined in large

⁴² This analysis was provide both in phone discussions between the author and Jane’s C4ISR Systems team on May 23, 2017 as well as through written analysis included in primer / informational papers submitted to the author on May 20, 2017.

⁴³ Bennett, Jay. “The Future of the Navy’s Electromagnetic Railgun Could Be a Big Step Backwards,” *Popular Mechanics*. April 2, 2017. <http://www.popularmechanics.com/military/weapons/a21174/navy-electromagnetic-railgun/>.

part by the nature of the materials out of which these platforms would be constructed. According to Milley, “the real sort of Holy Grail of technologies that I’m trying to find on this thing is material—is the armor itself. If we can discover material . . . That is significantly lighter in weight that gives you the same protection, that would be a real significant breakthrough.”⁴⁴

Of course, the importance of advanced materials is not limited to ground vehicles. The ability to develop lighter weight, stronger, more dynamic materials is a fundamental element of the conceptualization and design of future military capabilities that will allow the United States to maintain its military advantage vis-à-vis China and other actors. Of particular interest are smart, nano and bio-materials that retain at scale the dynamic and customizable attributes they exhibit at the atomic or genome level. These materials can promote qualities in advanced platforms and systems like self-healing, adaptation to environments, low observability, ultra-high strength and speed, and energy capture and storage. They also can support force and platform protection through increasingly attainable capabilities such as adaptive camouflage or smart armor.⁴⁵

- *Advanced Manufacturing:* Optimizing the effects of new materials with novel properties will rely on the concurrent development of new means of manufacturing with a heightened level of precision and customization. Virtual and augmented reality manufacturing, computer aided design, additive manufacturing (also known as 3D printing), 4D printing, synthetic biology manufacturing and automation are all technologies in which the U.S. should invest in order to retain advantage in the modern military capabilities required to retain advantage in military competition with China. The combination of new, smart, nano-, and bio-materials and advanced manufacturing will not only create cost and performance efficiencies, it will also create the potential for a new industrial Design Age in which manufacturing processes and material properties will be seen as powerful enablers of constructive innovations in capabilities rather than constraints.

Additional High-Level Recommendations

Technology protection: Many of the technologies driving the future of military capabilities are also of interest to and/or being developed by the high-tech industry, applied research institutes and other non-defense industries, such as automotive, commercial aerospace, maritime and energy. While this dual-usization of emerging technologies creates salutary new pathways for innovation in defense technology, it also complicates the challenge of technology protection, especially in light of China’s aggressive technology acquisition program. Mitigating risks associated with technology transfer—intentional or otherwise—of Fourth Industrial Revolution technologies will require a cross-industry understanding of what technologies China is prioritizing and how it is pursuing these technologies.

The U.S. government can support this collaboration by establishing and facilitating cross-industry working groups and panels that will first identify key strategic technologies that should be protected and second create guidelines to help companies across all relevant industries understand and address risk in a consistent manner and better anticipate when technology theft is more likely to take place.

⁴⁴ Freedberg, Sydney, “Milley’s Future Tank: Railguns, Robotics and Ultra-Light Armor”, *Breaking Defense*, July 27, 2017, <https://breakingdefense.com/2017/07/railguns-robotics-ultra-light-armor-general-milleys-future-tank/>

⁴⁵ Nurkin, Tate, “Promise and Peril: Opportunities and challenges of disruptive technologies and innovation”, *Jane’s blog*, June 22, 2017, <https://ihsmarkit.com/research-analysis/promise-and-peril-opportunities-and-challenges-of-disruptive-technologies-and-innovation.html>

The U.S. DoD, Congress, State Department and other agencies of the Executive Branch can also enhance technology protection by working with allies, especially in the Indo-Pacific, to establish a common understanding of the threat and ramifications of China's technology acquisition approaches. This common understanding can serve as a foundation on which to deepen collaboration in the protection of critical and sensitive dual-use technologies.

Adjacent Reforms and Other Transaction Authorities: Developing novel technologies is just one step in the overall development of capabilities. The move from novel technologies to fielding a viable capability involves several other adjacent innovations in operational concepts, training, organizational structure and legal and procurement frameworks. Given the pace of innovation in technology areas of increasing importance to the U.S. DoD, continued innovation in procurement processes that allow for rapid acquisition of platforms and systems will be essential to maintaining U.S. competitiveness and sustained ability for the U.S. to project power and pursue security interests in the Indo-Pacific. Initial DoD efforts to accelerate procurement processes for certain capability types—known as Other Transaction Authorities—should be refined and expanded as should efforts to collaborate the U.S. high-tech industry.