June 25, 2026

STATEMENT FOR THE RECORD
DAVID R. SHEDD

Western powers are slowly awakening to one of the greatest threats facing the free world: China's unprecedented campaign of industrial espionage. The implications of this event cannot be understated. Across history, industrial revolutions have inevitably transformed global orders. New technology brings new forms of power. In today's age, emerging technologies such as advanced telecommunications, artificial intelligence (AI), quantum computing, and hypersonic weapons could very well determine the global hierarchy of the 21st century. In this new world, zeros and ones (digital code) can prove just as crucial, and therefore valuable, to determining wars as artillery shells or soldiers with M-16s were in previous engagements.

While the United States was bogged down over the first 20 years of this century disrupting international terrorists, its rival across the Pacific – the People's Republic of China – has undertaken a highly orchestrated, "whole-of-society" approach to stealing secrets that will ultimately allow it to *leapfrog* nations like the US in developing these key technologies. To China, every commercial, scientific and academic sphere in the US is a target – from advanced aerospace technology to self-driving systems, to even agricultural seeds. In the eyes of Beijing, as outlined in the Xi's "Made in China 2025" strategic plan, capturing all markets will enable the CCP to assume its "rightful place" a top a new world economic order. It will also even the score of the nation's perceived "Century of Humiliation," when Western powers trampled over the Middle Kingdom during the 19th and 20thcenturies.

China's economic and military rise in the last 25 years is arguably unprecedented in history, in terms of both scale and material gain. China joined the World Trade Organization (WTO) and entered the global economic system in 2001. It was at that point Beijing's campaign to hijack the West's crown jewels of commercial secrets kicked into high gear. Per the CCP's high command, this campaign of theft combined with increased foreign investment would transform China from an economic backwater to an economic superpower. It worked. As measured by gross domestic product (GPD) growth, the country went from being a 1.3 trillion-dollar economy in 2001 to a nearly 21 trillion-dollar economy as of 2025.

Many China-focused analysts have sought to explain China's phenomenal economic ascent. Some have chalked up its success to its command-and-control economy, the comparative advantage of a Marxist-Leninist regime in terms of long-term planning and marshalling state resources, while others have focused on China's stranglehold as the manufacturing center of the world, making it the lynchpin of the global supply chain.

There is a much more credible explanation when it comes to the larger story of how China has orchestrated its state resources to launch a highly strategic campaign – relying on traditional forms of espionage and novel forms largely alien to Western security services – to steal the commercial and technological secrets. The PRC's epic campaign of industrial espionage is a key variable explaining China's rapid economic ascent and military buildup. And that campaign has not stopped.

Looking at China's rise over the past 25 years, the breadth and variety of China's industrial theft is truly astonishing. China has stolen blueprints, know-how, and data from the West on everything from advanced aerospace technology to critical telecommunications. It has compiled genetic data on millions of people around the world, with the aspiration of giving its biotech industry a decisive advantage over Western competitors. It has weaponized venture capital and private equity firms to obtain coveted and sensitive technology from startups in Silicon Valley. The PRC/CCP routinely deploys bad-faith tactics, such as sponsoring tech start-up competitions or invite guest speakers to seminars to cloak the hidden aim of ultimately acquiring sensitive technology and IP it could not obtain legally.

Taking advantage of America's open academic environment and research institutions, it has collaborated with and recruited scientists, engineers, and software programmers. These experts later provided China with critical advantages in field such as AI, quantum computing, advanced light detection and ranging – LIDAR – remote sensing technology, electric vehicles, and green energy. These areas of emerging technology are the key battlegrounds in geopolitical rivalry and great power competition. Underscoring this new dynamic, at a late 2023 gathering in Silicon Valley, leaders of Five Eyes (the US, UK, Australia, Canada, and New Zealand) domestic spy agencies warned that "the technology secrets that are about to change the world, in artificial intelligence, biology and computing are falling into the wrong hands — stolen — in a global espionage campaign by China."

While Western governments are slowly awakening to the threat posed by China's theft of secrets, many private sector companies remain in denial of this reality. During the gathering in Silicon Valley, the head of the UK's domestic security service bluntly told the audience that nearly everyone is a target of this campaign: "If you're working today at the cutting edge of technology then geopolitics is interested in you, even if you're not interested in geopolitics." As former Attorney General Eric Holder similarly put it, "There are only two categories of companies affected by trade secret theft: those that know they've been compromised and those that don't." For CEO's and boardroom members focused on having their firm become the next *unicorn* or achieving the latest quarterly results, threats to proprietary IP, data, and corporate security have largely been relegated to the back of minds. As many are already learning, this is a mistake of epic proportions not just for the sake of their own country's national security but for their company's competitive standing in the global marketplace.

China uses a multi-pronged approach to execute its relentless theft campaign, relying upon a decentralized collection method that is ultimately guided by broader strategic goals as articulated in the strategic plan known as "Made in China 2025," CCP Chairman Xi Jinping has now extended this blueprint to 2030 due to its initial success since 2015. Ironically, one of the prongs of CCP-driven IP harvesting is the profit motive. Traditionally, state actors would target and steal classified information on a government-to-government level. Government intelligence officers would typically recruit a "spy," in other words an agent/source, with access to classified information from another government to provide them secrets to help inform their national security makers and warfighters.

While old fashioned spying of this kind is certainly not dead, the PRC has undertaken a new and largely revolutionary approach to collecting critical information, reflecting a fusion of state and economic interests. No longer are diplomats just "recruited" at cocktail parties. Corporate C-Suite members, professors, academic researchers … all are fair game to Beijing. Economic theft has become state policy and leaders in Beijing have no moral scruples about doing what it takes to ensure they win. Seeking dominance with cyber capabilities, nothing is off limits to Beijing's IP vacuuming operations.

Indeed, what has made the PRC's intelligence machinery so effective is the way it has used every means at its disposal against the West. Their information collection capabilities, led by the PRC's massive Ministry of State Security (MSS) is an "all at once"- blending cyber, human intelligence, academic research, and commercial investments to achieve its larger strategic goals. All while, the PRC/CCP merely gives off the appearance, as best they can, of being a complying WTO member when it comes to the current international economic and financial order that West abides by. While brazenly stealing trade secrets from the West, the PRC has at the same time maintained an aggressive diplomatic charm offensive highlighted by the late 2023 visit of Chairman Xi to business leaders in San Francisco last year. 'All is well,' the message essentially underscored. 'Rest easy and continue to do business with China.' Despite the most optimistic of hopes by the US and its allies for continued globalization and integration of China into the global economy, however, the reality is on a collision course with raw power politics and Beijing's aspirations for a new global order achieved by its domination of critical technologies. Short-term profits can come with long-term, unexpected costs.

The challenge to the West facing this threat is that its traditionally structured security apparatuses are ill-suited to combating this unique and modern threat. The FBI has decades of practice uncovering an official Russian intelligence officer trying to recruit a government official. But the question an equally relevant requirement today is how does the FBI approach a partially owned Chinese firm seeing a perfectly legal commercial acquisition of a start-up developing cutting edge self-driving technology or a Chinese national purchasing a swath of land directly outside a US military base? The West's legal & regulatory frameworks are also lacking. Staffs and required capabilities are underfunded and overtaxed often making the prosecution of trade theft cases difficult even when the evidence is overwhelming. As former US Senator and now Secretary of State Marco Rubio so succinctly put it, American companies are committing in effect "corporate suicide" by not fully considering the long-term consequences of fueling Chinese economic superiority.

In many ways this has been a unilateral war waged by China against the US and West. Beijing has played off the naiveté of the leaders in Washington and Brussels, weaponizing their strengths – a liberal and globalized economic order – in a judo-like manner to its own advantage. While direct confrontation

in a military sense is not inevitable, this commercial war, one fought largely in the shadows, is well underway.

The potential for a "hot war" between the US and China is not some abstract idea. As each day passes, the likelihood of a direct confrontation over Taiwan builds. Chairman Xi of China has already asserted that the CCP would "reunite" with the island by 2027. American commanders have predicted this could come sooner. A major power war between the US and China would be unlike anything the world has ever seen. The American homeland itself would likely be targeted. New technologies will inevitably be deployed, likely with lethal effect.

What is to be done?

Recognizing the threat is only the first albeit vital step. The US must adopt a new conception of economic security, one suited to a world in which industrial power and national power are inseparable.

No less than seven steps should be taken by the United States to regain the initiative to protect the foundations of American power:

• **Protect the crown-jewel technologies of the 21st century**—adopt a living national Crown Jewels Doctrine to protect AI model weights, semiconductor architectures, quantum tools, and hypersonic research with nuclear-level safeguards.

• **Modernize legal deterrence**—reform the definition of economic espionage, revive the Department of Justice's China Initiative, and ensure legal penalties match the scale of national-security harm.

• **Secure the nation's physical and digital perimeter**—conduct a national security audit of critical infrastructure and move from today's patchwork defenses to an integrated 21st-century perimeter.

• **Shield the innovation pipeline**—reform research security across universities and national labs, require disclosure of foreign affiliations, and ban partnerships with PLA-linked institutions.

• **Cut off the capital lifeline**—close loopholes that allow U.S. investment and pension funds to accelerate China's military-industrial base.

• **Harden the corporate front lines**—require companies to treat their R&D and intellectual property as national-security infrastructure.

• **Make economic security a national imperative**—establish a White House–led Economic Security Council to unify policy across export controls, investment screening, research protections, and cyber defense.

Only a sustained, whole-of-nation effort on the part of US will shift the United States from having a fragmented defense approach to going on the offense in the defining geopolitical contest of the 21st century.

It is not too late to take bold actions against the PRC's great heist of western technology, know-how, and data but time is not on our side.