THREAT ASSESSMENT

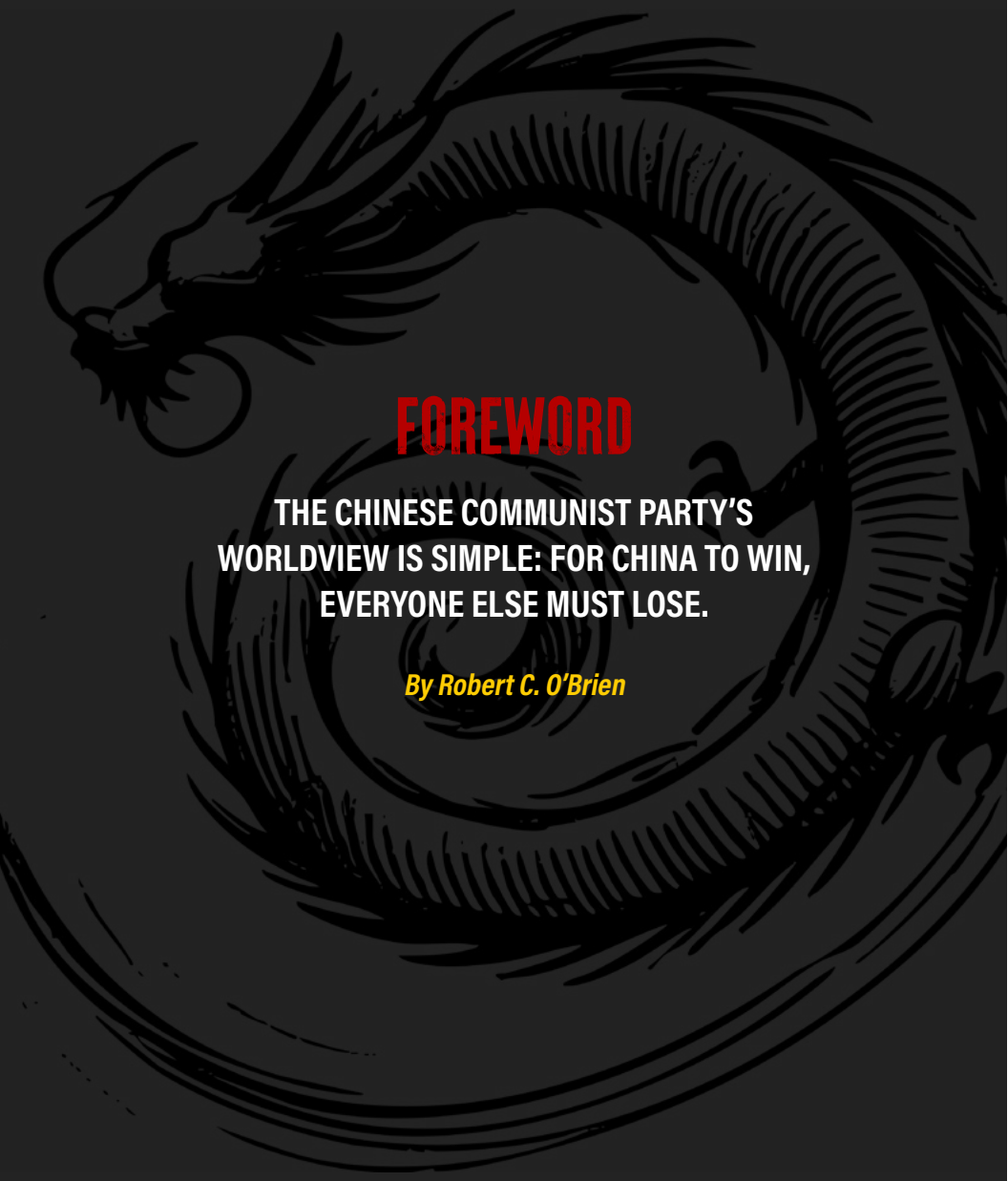
THE CCP THREAT AND HOW STATE LEADERS CAN PROTECT OUR COUNTRY AND CITIZENS

A PROJECT OF STATE ARMOR AND CITIZENS FOR FREE ENTERPRISE ACTION

STATE ARMOR

CITIZENS FOR FREE ENTERPRISE ACTION

TABLE OF CONTENTS



FOREWORD

THE CHINESE COMMUNIST PARTY'S WORLDVIEW IS SIMPLE: FOR CHINA TO WIN, EVERYONE ELSE MUST LOSE.

By Robert C. O'Brien

I.

Communist China is the most powerful adversary the United States has ever faced. Some say our country is entering a new Cold War. If this is true, it will certainly be more challenging and dangerous for America than what we faced with the Soviet Union. Under the Chinese Communist Party, or CCP, the Chinese government is plotting and growing its military might and seeking to undermine U.S. national security. Their malicious efforts and activities are not reserved only for the distant waters of the Pacific or to threaten our allies and partners overseas. China is seeking to infiltrate all aspects of America's domestic society to threaten our security and freedom. The perilous situation our nation now faces did not happen quickly. Rather, it is the result of decades of careful patience and planning on the part of the CCP.

While America squandered its post-Cold War "peace dividend," with leadership focusing instead on the global war on terror and ill-fated nation building over the past three decades, China built the world's largest military and the CCP spun a web of global influence operations. All her toil is designed to undermine free nations and to put China solely atop the international community. Already the CCP has undermined Hong Kong autonomy—next, it could seek to take democratic Taiwan by force and coercion. But the threat we face from China is not only military in nature. This is a clash that involves the whole of our societies. The most insidious and dangerous strategy the CCP is deploying is to weaken the U.S. from within. We must employ all instruments that make up national power—military, diplomatic, political, economic, trade and our industrial base—to prevail. China is certainly doing so.

Just a few years ago, China's economic rise provided hope that Beijing would one day become a reliable and cooperative partner in economic, trade and other international issues. Many in America, and throughout the West, built a strategy upon the hope that China would democratize slowly if offered the economic incentives to do so. This hope relied on a false premise and hope itself is not a substitute for a real strategy. While the U.S. and its partners offered olive branches and invited China to weave itself into the international financial order, CCP leadership in Beijing simply chose to bide their time.

Instead of investing in their people, the CCP poured billions of dollars into building a formidable and modern military. Instead of seeking trade partnerships built on mutual benefit and interdependence, the CCP stole our intellectual property and undercut our businesses. Instead of loosening their grip on power, the CCP cracked down on dissent. These tyrannical activities were designed to support the state security apparatus and to position China to one day challenge the United States and the international order which has promoted peace and prosperity for almost 80 years. This strategy has only become more pronounced under CCP Chairman Xi Jinping, who has rewritten the law to consolidate absolute power with himself.

Recent history demonstrates that under Xi Jinping and the CCP, China is not interested in becoming a thriving economic partner. Instead, Beijing seeks to upend the entire global order to place itself at the top. In Xi Jinping's eyes, for China to win, everyone else must lose.

China has committed to spending trillions of dollars under the "Made in China 2025" initiative. Their goal is to achieve global domination of high-tech industries in robotics, advanced information technology, aviation, electric vehicles, quantum computing, artificial intelligence and autonomous systems. Beijing is aggressively subsidizing national champion firms to support these goals. Chinese firms are flagrantly disregarding international laws and norms to achieve their goal.

These challenges are closer to home than most think. Chinese technology, including their microchips, telecom equipment, displays, and other technologies, have saturated the American market and infiltrated our critical infrastructure. This technology has become embedded within our transportation infrastructure, our industrial sector, our machinery, our digital systems, our cybernetwork, and our homes waiting to cripple American society should tensions ignite. Chinese owned firms are purchasing American farmland, posing a serious threat to our domestic food supply. Chinese state-owned apps such as TikTok steal American data and feed vitriolic propaganda to our young people unabated. China gladly serves up fentanyl to the cartels and drug traffickers to poison our people from across our own border. China's ambitions have become clear: undermine the West at any cost. Those ambitions must be addressed head on. U.S. vulnerabilities are not only a federal problem but also a national problem that requires a coordinated response at the state and local level.

The United States, including state and local officials, can and must meet this existential challenge with the determination to protect our way of life, our territory, and our citizens. We are living in dangerous times, facing perhaps the most serious geopolitical threat since 1938. U.S. leadership at all levels must take this threat seriously and prepare now to ward off a complete crippling of our way of life.

Ambassador Robert C. O'Brien was the 27th U.S. National Security Adviser from 2019-2021.

THE STORMY SEAS OF A MAJOR TEST

GENERAL SECRETARY XI JINPING HAS SIGNALED WILLINGNESS TO SEIZE TAIWAN REPEATEDLY – EVEN IF DOING SO REQUIRES FORCE. XI SEES AN ADVANTAGE IN COMPOUNDING CRISES SPURRED BY WARS UNDERTAKEN BY ITS ALLIES ON MULTIPLE CONTINENTS – CRISES THAT RUN THE RISK OF EXHAUSTING THE UNITED STATES AND SETTING THE TABLE FOR A POSSIBLE MOVE ON TAIWAN.

By Matt Pottinger

II.

If just one lesson could be drawn from Russia's invasion of Ukraine, it could be this: Deterrence would have been a lot cheaper than war. Yet democracies seem to be getting worse at deterrence. The record of the past two years—Vladimir Putin's assault on Ukraine, the Hamas attack of Israel sponsored by Iran and its proxies, and North Korea's resumption of testing of intercontinental ballistic missiles—is marred with failures and signs of trouble.

Looming on the horizon is the specter of a conflict more consequential than all of these flashpoints combined. Secretary Xi Jinping has vowed to "reunify" Taiwan with mainland China through force of arms if necessary. Indeed, Xi's public statements about a coming "great struggle" against China's enemies provide a window into his intentions – one the world would be unwise to ignore.

More than once, Xi has described unification with Taiwan as a prerequisite for achieving his broader objectives for China on the world stage, a vision he calls "the Chinese dream for the great rejuvenation of the Chinese nation." In a 2019 message to "Compatriots in Taiwan," he said: "The rejuvenation of the Chinese nation and reunification of our country are a surging popular trend. It is where the greater national interest lies, and it's what the people desire." Xi is equating a failure to annex Taiwan with a failure to enact his overarching goals as China's leader.

Although he has been less concrete publicly about a timeline, Xi has exhibited an impatience that distinguishes him from his predecessors. "The issue of political disagreements that exist between the two sides must reach a final resolution, step by step, and these issues cannot be passed from generation to generation," Xi told a Taiwanese envoy in October 2013.

Xi knows this may require war. In key speeches over the past few years, he has admonished his party and its armed wing, the People's Liberation Army, to prepare for a major conflict. "In the face of major risks and strong opponents, to always want to live in peace and never want struggle is unrealistic," Xi said in his November 2021 speech to the Sixth Plenum of the 19th Party Congress in Beijing. "All kinds of hostile forces will absolutely never let us smoothly achieve the great rejuvenation of the Chinese nation. Based on this, I have repeatedly stressed to the entire Party that we must carry out a great struggle."

For Xi, Washington is the adversary. "Western countries headed by the United States have implemented containment from all directions, encirclement and suppression against us, which have brought unprecedented severe challenges to our country's development," Xi said in a March 2023 address. That speech was one of four made by Xi that month in which he underscored the need to prepare for war.

This all comes as China has become the primary economic and diplomatic sponsor of a new "Axis of Chaos" of revanchist autocracies, including Russia, Iran, North Korea and Venezuela. Xi sees an advantage in compounding crises spurred by wars undertaken by its allies on multiple continents—crises that run the risk of exhausting the United States and setting the table for a possible move on Taiwan. Indeed, Xi makes clear the world is reaching a historic turning point. "Since the most recent period, the most important characteristic of the world is, in a word, 'chaos,' and this trend appears likely to continue," Xi said in 2021. "The times and trends are on our side."

In light of all of this, the world should regard gravely Xi's exhortation, contained in his "work report" to the 20th Party Congress in October 2022, that the Chinese Communist Party must prepare to undergo "the stormy seas of a major test."

Washington cannot prevent war alone. State leaders have a major role to play in disproving Xi's belief that the West is in inevitable

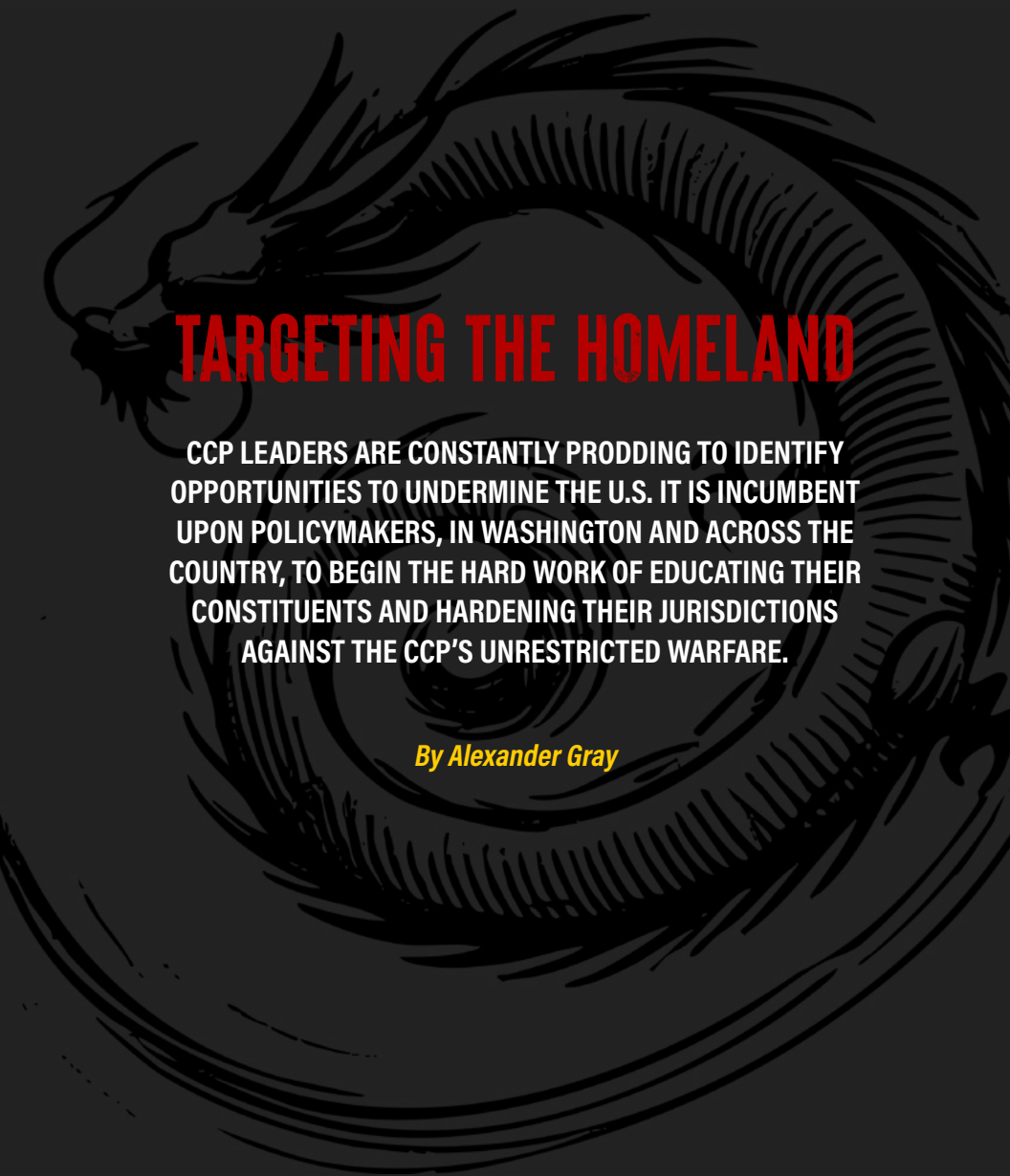
decline—and thus in deterring war. They can do so by blocking Beijing's access to American technology, capital, talent and data, and by reducing U.S. reliance on China.

Addressing Beijing's access to U.S. institutions of higher education via research partnerships is a good start. States should also consider blocking China's purchases of farmland neighboring sensitive military sites. Leaders of state pension systems can consider reevaluating investments into China.

The clock is ticking. Beijing is underwriting the countrywide synthetic drug crisis by producing nearly all fentanyl precursors. Chinese criminals are now the money launderers of choice for the cartels. Chinese influence operatives penetrate state capitals across the country. The list continues.

Unmistakable strength is the key to persuading China to refrain from setting off a geopolitical catastrophe over Taiwan. This is what kept the Cold War cold in the last century. This is what can keep Xi from rolling the iron dice of war in this one. State leadership must accept their role in preventing global conflict.

Mr. Pottinger is a Former Deputy National Security Advisor of the United States. He previously served as senior director for Asia, where he led the administration's work on the Indo-Pacific region, in particular its shift on China policy.



TARGETING THE HOMELAND

CCP LEADERS ARE CONSTANTLY PRODDING TO IDENTIFY OPPORTUNITIES TO UNDERMINE THE U.S. IT IS INCUMBENT UPON POLICYMAKERS, IN WASHINGTON AND ACROSS THE COUNTRY, TO BEGIN THE HARD WORK OF EDUCATING THEIR CONSTITUENTS AND HARDENING THEIR JURISDICTIONS AGAINST THE CCP'S UNRESTRICTED WARFARE.

By Alexander Gray

III.

Unlike previous Great Power rivals the U.S. has faced, the People's Republic of China under the Chinese Communist Party, or CCP, control has married significant economic and industrial capacity with an advanced and growing military, deep financial ties to the U.S. and its allies, and an authoritarian ideology that the party aggressively seeks to export globally. The Chinese government's pursuit of power ensures the U.S. and the CCP will be engaged in an extended competition for global dominance in the decades to come.

The rivalry between the U.S. and the People's Republic of China, or PRC, under the CCP is likely to directly impact Americans in ways that have become alien since the end of the Cold War. Following the collapse of the Soviet Union and the Sept.11 terrorist attacks, Americans became acculturated to viewing armed conflict as low-casualty, relatively sterile affairs viewed on television and affecting far-away populations. The reality of potential conflict with the PRC, whether over Taiwan, the South China Sea or any number of potential flashpoints, is that it will not be confined to distant theaters. China is determined to bring a potential war, particularly a protracted one, to the American people.

CCP leaders are constantly prodding to identify opportunities to undermine the U.S. Writing in 1999 in "Unrestricted Warfare: Two Air Force Senior Colonels on Scenarios for War and the Operational Art in an Era of Globalization (超限战)," Senior Chinese Colonels Wang Xiangsui and Qiao Liang take stock of perceived American weaknesses in a potential conflict with the United States. They write of a new kind of conflict in which "all the boundaries lying between the two worlds of war and non-war, of military and non-military, will be totally destroyed, and it also means that many of the current

principles of combat will be modified, and even that the rules of war may need to be rewritten." They note the vulnerability of the U.S. homeland, specifically to economic coercion and even biological attacks and lay out a series of spheres in which the U.S. has failed to focus sufficient attention. Twenty-five years and voluminous examples later, the United States should take the CCP at its word and understand that a potential conflict with China would indeed be "unrestricted" and the U.S. homeland would not be off limits.

Presidents Joe Biden and Donald Trump have released National Security Strategies naming China as the preeminent threat to U.S. national security. The 2017 National Security Strategy under President Trump says China seeks "to shape a world antithetical to U.S. values and interests." Similarly, the 2022 National Security Strategy under President Biden identifies China as "the only competitor with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do it."

Governors and local officials must come to grips with this threat, too, and our officials must collectively evaluate China's threat to Americans at the state and local level. In March of this year, President Biden's National Security Adviser, Jake Sullivan, sent a letter to Governors outlining PRC threats to critical infrastructure and called partnerships with state, local, tribal, and territorial governments "critical" to countering these threats. Back in 2020, President Trump's Secretary of State, Mike Pompeo, said "competition with China is not just a federal issue" and called states to collective action. China's understanding of the inherent vulnerabilities created by America's decentralized system of government has only grown in the quarter-century since the publication of "Unrestricted Warfare." Now is the time for U.S. policymakers and engaged citizens to similarly take stock of those potential weaknesses and act accordingly.

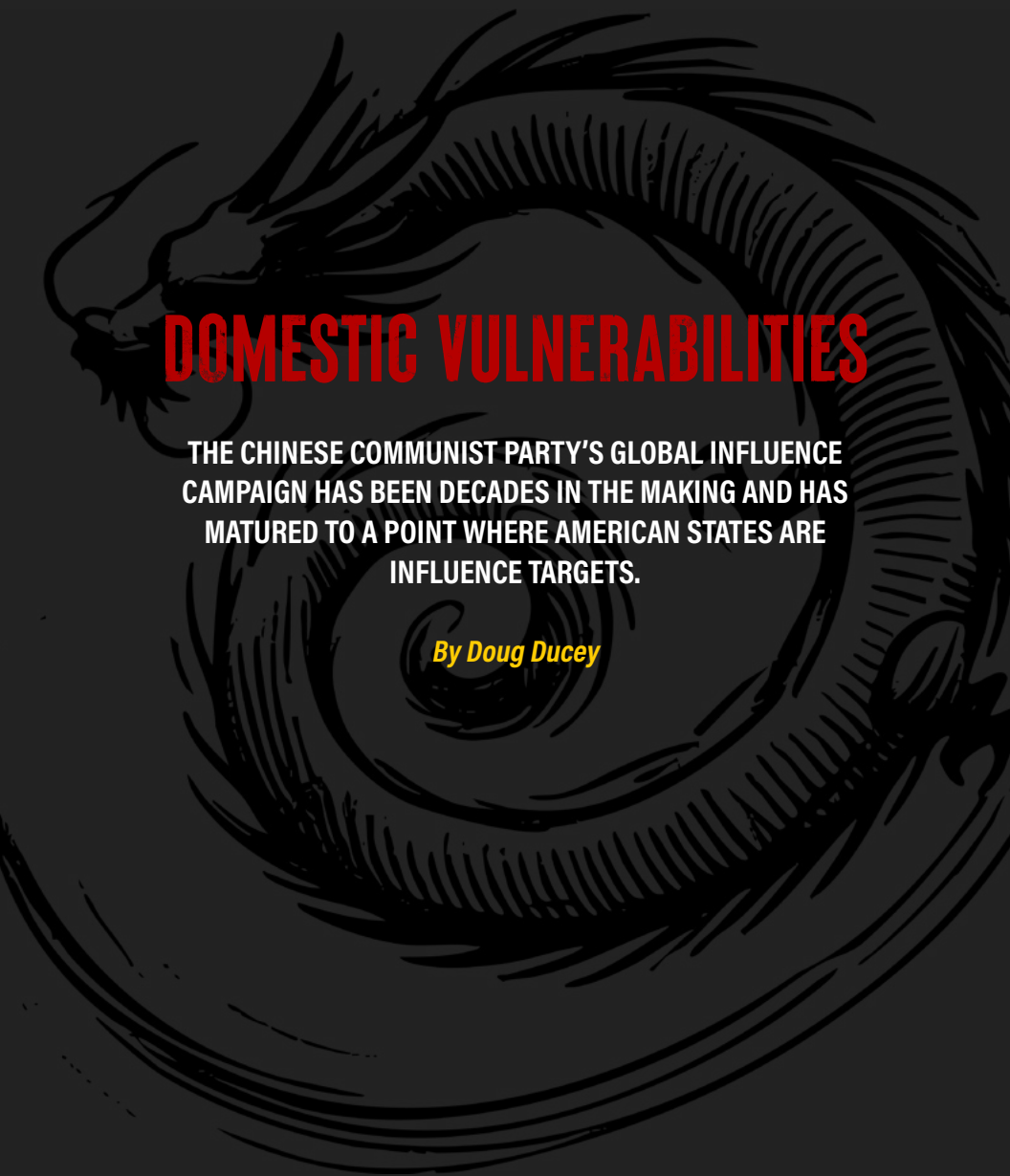
U.S. states and localities have long been particularly susceptible to Chinese influence operations in peacetime and, in a potential

wartime scenario, a wide array of potential CCP coercive measures. In peacetime, these range from utilizing the "Thousand Talents Program" to transfer sensitive technologies from U.S. universities to the PRC, using "Confucius Institutes" and similar institutions to promote CCP ideological objectives on campuses, deploying CCP agents to harass and intimidate campus voices opposed to the regime's authoritarianism, and manipulating sister city relationships and other cooperative initiatives to subvert or compromise state and local officials.

In wartime, CCP depredations facing states and localities could include cyberattacks on critical infrastructure, producing significant damage to civilian populations. These attacks could also include disruption of the food supply facilitated by CCP control of key pieces of agricultural land across the U.S., and traditional sabotage operations directed at key pieces of federal, state and local infrastructure. With the federal government distracted by an ongoing conventional conflict of unprecedented scale and scope, states and localities will be forced to address these challenges with limited federal resources and without a tradition of proactive measures addressing the CCP threat.

Such unprecedented challenges will fall heavily on the shoulders of state and local officials, many of whom are unaware of the CCP threat or the unique nature of CCP warfighting doctrine that will likely bring any potential conflict directly to their doorsteps. It is incumbent upon policymakers, in Washington and across the country, to begin the hard work of educating their constituents and hardening their jurisdictions against the CCP's unrestricted warfare. Without concerted, thoughtful action in peacetime by governors, legislators, mayors and city councilors, vast swathes of America will remain deeply vulnerable to China's predations in the event of conflict.

Mr. Gray is a senior fellow at the American Foreign Policy Council. He served as chief of staff of the White House National Security Council from 2019-2021.



DOMESTIC VULNERABILITIES

THE CHINESE COMMUNIST PARTY'S GLOBAL INFLUENCE CAMPAIGN HAS BEEN DECADES IN THE MAKING AND HAS MATURED TO A POINT WHERE AMERICAN STATES ARE INFLUENCE TARGETS.

By Doug Ducey

IV.

The United States is on the verge of succumbing to Beijing's master plan to render America, along with the rest of the world, dependent on technologies controlled by the Chinese Communist Party, or CCP. The plan has progressed by exploiting seams between the public and the private sector, and between the federal government and U.S. states. State governments are now uniquely well-positioned to increase protections their constituents—and prevent the CCP's plan from succeeding.

The CCP's aim is to supplant the United States as the world's leading superpower, and China's leadership believes our federal system can be exploited for their gain. As the former chief executive of one of the largest, fastest growing, and most economically diverse states in America, I've found myself alarmed by the degree to which the CCP has tried to gain a foothold at the state and local level, and by the lack of information that federal authorities have shared with state leaders about the threats they face. Sadly, during my eight years in office, this issue was rarely a topic discussed by our partners in the federal government. Federal-state information sharing must improve if we're to thwart the ambitions of the Chinese Communist Party, and state executives must adopt comprehensive policies and procedures to protect their states.

In my time outside public office, I've had the opportunity to work closely with experts who've spent decades analyzing the CCP's military buildup and global influence operations. Presented with

the full scope of all the CCP's activities in states across America, I asked, "Why aren't governors made aware of these threats?" As the Chairman of the Republican Governors Association, we frequently hosted meetings where governors could compare notes and discuss policy matters in their respective states. Not once during eight years of working with my colleagues and two years running the RGA did anyone mention specific official outreach from federal officials about tangible national security concerns related to CCP state-level influence campaigns. Secretary of State Mike Pompeo's February 2020 speech to the National Governors Association stands as a lone wakeup call, but it was delivered mere weeks before the COVID-19 pandemic spread across the United States and consumed state-federal relations.

If China is targeting states, which we now know they are, then state leaders must be regularly briefed by federal law enforcement and intelligence agencies that have first-hand knowledge of the threats states face. And at the state level, we must reach out to establish a more productive relationship with federal partners and request more information-sharing. Our federal system allows states to be nimble and act quickly to steer policies in a better direction. Federal authorities should recognize both state strengths and vulnerabilities and prioritize sharing information that allows state executives to maximize their impact in protecting our nation from hostile actors like the CCP.

Fortunately, state and local leaders don't need to wait on the federal government or even state legislatures to begin to enact policies that help curtail CCP influence. One easy step is for governors to direct all agencies and employees to forego official trips to China and to refuse any gifts provided by the CCP and its state-owned companies and affiliated entities. These seemingly "kind" gestures by Chinese entities are a ruse designed to further normalize economic and political relations with state and local governments. The underlying intent, according to a 2022 memo by the Director of National Intelligence, is to allow China's government to shape policymaking through the U.S. business community, to engage in

information collection, to target officials to exploit later, to promote technological dependence, and to build partnerships that can be exploited for political propaganda and other purposes. Ethics rules should be updated to require state employees to report interactions with foreign adversaries so that influence campaigns can be tracked and thwarted.

It's imperative for elected officials and the business community to have a proper understanding of the CCP's stated mission to displace the United States' role as the world's leading superpower, and to factor that knowledge into interactions at the state and local level. If the goal is to promote state economic development, there are far better ways to benefit your state and community than by acting as an unwitting participant in the CCP's influence operations. State economic incentives that are extended to American companies and those of our friends and allies should never be extended to companies of our adversaries. Therefore, as governors develop strategies to on-shore critical production, they should direct their economic development agencies to attract foreign direct investment from trusted countries that share our values and not adversaries that are trying to engineer our downfall.

One of my proudest accomplishments during my time as governor was bringing the Taiwan Semiconductor Manufacturing Company (TSMC) facility to Arizona. In 2020, we succeeded in securing the world's largest contract manufacturer of silicon chips because we created an economic environment free of unnecessary burdens, with low costs for doing business and an effective workforce ready to contribute to a world-class operation. Not only was TSMC's presence a boon to our local economy, bringing thousands of jobs to the state, but we also helped lessen American dependence on Chinese-made semiconductor chips, and we on-shored Taiwanese chipmaking that could be disrupted if China launches a conflict in the Pacific. Supply chain bottlenecks created by the COVID-19 pandemic revealed just how dependent we are as a nation on Chinese-made products, particularly semiconductor chips, which have become vital to our technology, automotive, and healthcare industries. I

encourage all state leaders to pursue similar investments that serve both as beneficial economic development projects and to reduce our dependence on products made by hostile nations.

In addition, governors should maintain and regularly update a list of prohibited technologies to ensure state agencies and contractors are not introducing unseen risks into our state government and critical infrastructure. And local governments should be encouraged to adopt the same protocols. Even before Congress enacted a law to require divestiture of TikTok from a CCP-controlled company, most state leaders prohibited TikTok on state devices due to the danger TikTok presented to sensitive state data. But TikTok is only one piece of compromised software that states need to ward off – there are plenty of other instances of software and hardware that states must avoid. Governors as politically diverse as Texas' Greg Abbott and Wisconsin's Tony Evers have already implemented a list of prohibited technologies. These lists should be monitored and updated as new information reveals the risks associated with adversary technologies.

Most importantly, there is now an effort underway to raise greater awareness of how state leaders can solve the new set of problems in front of us. Comprehensive state solutions exist, and it's now a matter of adopting and implementing policies to protect our states. The CCP continues to unnecessarily escalate tensions with Taiwan and other neighbors, threatening a conflict that would disrupt the entire world order. State leaders must move swiftly to address our greatest weaknesses to secure our homeland and enhance domestic resilience, even if the federal government has failed to take a leading role. The coronavirus pandemic taught us that states are on the front lines of global crisis response, and that our federal system is one of our greatest strengths as a nation if leaders leverage their powers appropriately. We must not allow the Chinese Communist Party to continue exploiting American federalism to their own benefit, and instead we must use our unique and dynamic system to secure our country against the greatest threat we face.

Finally, the sections that follow provide a briefing about five critical threat areas that I would want to be briefed on as a state leader. They are the danger of technological dependence, threats to land and critical infrastructure, exploitation of American universities, influence operations and elite capture, and how state funds are used to finance China's military buildup and human rights abuses. The experts who wrote these sections detail the problem and point to concrete solutions.

State leaders must quickly get the ball rolling with the solutions at hand to secure our states against foreign adversaries. Enacting the solutions laid out below will make a tremendous start. State leaders should also direct their policy and legal teams to develop new and innovative solutions in this emerging area that will define our ability to secure our nation. Our 50 laboratories of democracy make an unbeatable machine of policy innovation. It's time we unleash them on one of the 21st century's greatest challenge: securing our homeland against the threat of Communist China.

Governor Doug Ducey served as the 23rd Governor of Arizona from 2015-2023.

THE THREAT OF TECHNOLOGICAL DEPENDENCE ON THE CCP

CHINESE COMMUNIST PARTY GENERAL SECRETARY XI JINPING ENVISIONS A WORLD WHERE ALL IMPORTANT TRADE ROUTES AND SUPPLY LINES RUN THROUGH BEIJING. U.S. STATES HAVE AN OPPORTUNITY TO STEP UP AND TAKE ACTION TO PROTECT AMERICANS

By Jacqueline Deal, PhD

V.

The United States is on the verge of succumbing to Beijing's master plan to render America, along with the rest of the world, dependent on technologies controlled by the Chinese Communist Party, or CCP. The plan has progressed by exploiting seams between the public and the private sector, and between the federal government and U.S. states. State governments are now uniquely well-positioned to increase protections for their constituents—and prevent the CCP's plan from succeeding.

CHINA'S PLAN IN THREE STEPS

While most Americans consider technology to be a convenience at home and a productivity booster at work, for Chinese President and CCP General Secretary Xi Jinping, technology holds the key to "the great rejuvenation of the Chinese nation" or the "China Dream." That is, Xi believes that mastering current and emerging technologies will enable China to eclipse the United States as the world's leading power.

How? Rather than engage with the world of free and competitive trade, Xi envisions a world where all important trade routes and supply lines run through Beijing. This is possible, according to the CCP, thanks to the Fourth Industrial Revolution, which has created an information economy that rewards platform and data dominance. Xi's idea is for China to be the home of the companies that monopolize critical industries and data. On behalf of the party, these companies will "win" the technology race and acquire the

resultant leverage—other states will hardly be able to stand up to a regime that knows their secrets and constitutes their sole supplier for necessary imports. This means that the CCP will effectively be able to dictate terms to exposed, dependent foreign governments and their people. A dystopian cycle will then ensue, ensuring the party's wealth and power while reducing the rest of the world's prosperity and freedom.

The CCP's three-step plan will turn this vision into a reality.

STEP ONE

First, China had to move up the value chain from merely assembling goods designed and produced elsewhere to engaging in leading-edge production. The need for such progress was identified in the early 2000s, when CCP strategists worried that, having become the world's factory, China would still be in trouble if the West ever decided to impose a technology blockade and deny it key inputs. Beijing therefore promulgated a national Medium- and Long-Term Science & Technology Development Plan outlining the industries, resources and technologies that China had to indigenize—from information technology, minerals and manufacturing to advanced energy (such as solar panels, batteries and electric vehicles), core electronic components (think semiconductors, smart systems and the Internet of Things), wireless mobile telecommunications (e.g., 5G), and drug innovation and development.

The plan's execution has involved business deals with leading companies worldwide, "talent" programs to recruit academics with relevant expertise abroad and cyber theft. Under Xi, the party turbocharged this effort by upgrading "military-civil integration" into "military-civil fusion." A longstanding policy of exploiting for military and state purposes the know-how accessible to Chinese companies, students and other nominally private-sector entities was thereby transformed to collapse the boundary between private and public. Today, Xi claims rights to the allegiance of all "sons and daughters of the Yellow Emperor" inside or outside the country,

whether or not they are Chinese citizens. The CCP wants to enlist the help of these "children" to achieve the China Dream.

STEP TWO

Having acquired critical technology, China's second step has been to foster national champions to displace foreign competitors in key sectors. The classic example is Huawei, which received tens of billions of dollars of subsidies from Beijing to undercut competitors and become the world's leading supplier of 5G telecommunications equipment, perfectly positioning the company to spy on global voice and data flows or to disrupt these flows in a crisis or a war. But Huawei is far from unique.

Other national champions have proliferated around the key industries, resources, and technologies identified back in 2006. For instance, the CCP has pursued its ambition to dominate dual-use manufacturing involving microelectronics and information technology by fostering the rise of:

- China Rare Earth Group, a conglomerate that controls nearly all the minerals necessary for high-tech manufacturing
- Drone-maker DJI
- Video camera-makers Dahua and Hikvision
- Lenovo and Lexmark in the computer and printer space, respectively
- Airport scanner-maker Nuctech
- Alibaba, Bytedance and Tencent in the social media and e-commerce space
- Semiconductor Manufacturing International Corporation, or SMIC, a chip company, and, again, Huawei, which has also quietly entered the semiconductor field

Similarly, in the advanced energy space, China has promoted CATL (batteries), BYD (batteries and electric vehicles) and Hesai (LiDAR), which are also dual-use companies now that cars are connected vehicles and sensor platforms in addition to ways of getting from here to there. And in the fields of biotech and drug

development, Chinese national champions BGI and WuXi AppTec have become world-leading companies with considerable access to foreign populations' DNA as well as the formulas for new drugs.

Across their respective industries, all these companies collect sensitive data, fulfill important functions, and have acquired near-monopolies. They have all also benefited from state subsidies and labor policies that suppress wages in China. This ensures that they are not competing with foreign peers on a level playing field, so they can win.

STEP THREE

The third step, which the CCP is now pursuing, involves reaping the rewards from having fostered, and cultivated foreign dependence on, such national champions. If this sounds like science fiction, consider what has already come out: The CCP and its intelligence apparatus secretly have access to TikTok user accounts through Bytedance, its Chinese parent company, and, according to a former employee, used this access to surveil pro-democracy forces in Hong Kong. Bytedance has also allegedly spied on journalists covering TikTok to find out which employees were talking to them.

Another example arose early in the pandemic, when the CCP used its state media outlet, Xinhua, to threaten the Trump administration and block it from investigating how Beijing handled the initial COVID-19 outbreak in Wuhan. The threat—to suspend exports of pharmaceuticals—seemed credible given U.S. dependence on Chinese medical supplies, so the administration had to stop asking questions. Most recently, the Biden administration's October 2022 move to restrict China's access to leading-edge semiconductor technology resulted in similar threats from Beijing to suspend shipments of rare earths, the critical minerals over which China holds a near-monopoly. Perhaps that is why Biden's Commerce Department failed to enforce its own semiconductor export controls, prompting concerned Congressmen to warn the White House in October 2023 that the department's fecklessness was "pushing the United States toward a national security crisis."

STATES TO THE RESCUE

The United States still has strong cards to play, however, as America, its allies and friends in Europe and Asia—such as Japan, South Korea, and India—are among China's most important export destinations. If the collective West decided to incur the cost of finding alternative suppliers and ceased buying Chinese goods, the Chinese economy would suffer and technological dependence would end. Xi is trying to address this vulnerability with a policy called "dual circulation." The goal is to insulate the party from U.S. pressure by boosting domestic consumption and strengthening ties to non-Western markets. But given the policy of financial repression, this is an uncertain and necessarily longer-term proposition.

Meantime, U.S. states have an opportunity to step up and take action to protect Americans. If federal sanctions against Chinese national champions are likely to trigger the kinds of threats from Beijing that successive U.S. presidents have faced, states could nonetheless enact bans on procurement of Chinese technologies with public dollars and sometimes more broadly within their jurisdictions. Given the impracticality of suspending exports to particular localities, Beijing would be hard-pressed to retaliate. Such bans would go a long way toward weaning the country off a dangerous dependence on its number one rival.

Increased security will come with a cost states should be willing to bear—and the federal government should defray. The case of Huawei is instructive of both extreme dependence to avoid and public funding of solutions. A 2019 White House Executive Order called the threat posed by foreign adversary-controlled "information and communications technology or services" in the United States a "national emergency," citing the risks of "sabotage" and "economic and industrial espionage." The Trump Commerce Department noted that "there is reasonable cause to believe that Huawei has been involved in activities contrary to the national security or foreign policy interests of the United States." Congress then passed and the president signed the bipartisan Secure and Trusted Communications

Act, prohibiting federal funds from being used to obtain or maintain equipment from untrusted suppliers such as Huawei, and establishing a reimbursement fund for carriers to "rip-and-replace" any such equipment already installed. But since 2020, rip and replace has been stalled by charges that the federal reimbursement funding level is inadequate. Given the local interests at stake regarding sabotage and espionage, states could allocate their own funds for rip-and-replace and then sue the federal government for reimbursement.

In states with surpluses, procurement bans could be paired with incentives for innovation and manufacturing to restore U.S. competitiveness. Once reliance on cheap (or slave and child) Chinese labor has been banned, American entrepreneurs will respond to incentives to exploit technology for productivity gains. The ensuing activity will create jobs and tax revenue in states that seize this opportunity. From computers and printers, to drones, DNA sequencers, and electric vehicles, states should stop buying or reimbursing purchases of dual-use Chinese technology and start investing in U.S. alternatives. This way, they can ensure that the American Dream survives and prevails.

Dr. Jacqueline Deal is President of the Long Term Strategy Group, a defense consultancy, and co-founder of the American Academy for Strategic Education, a nonprofit that teaches courses on net assessment and China to rising national security and policy professionals. She frequently testifies on behalf of State Armor-backed legislation.

DOMESTIC VULNERABILITIES

THE CCP'S APPROACH TO TARGETING U.S. CRITICAL INFRASTRUCTURE AND LAND THROUGH CYBERATTACKS, ESPIONAGE, MALIGN INFLUENCE, AND THREATS TO FOOD AND AGRICULTURE SECURITY POSES A GRAVE AND COMPLEX CHALLENGE.

By Brian J. Cavanaugh

VI.

The Chinese Communist Party, or CCP, poses a multifaceted threat to the United States, including plans to target our critical infrastructure and land. The strategic infiltration by the CCP spans across cyberattacks, espionage, land acquisition, and pre-positioning for various malign activities. These efforts are not only aimed at undermining U.S. national security, but also at exerting influence over key sectors of our economy, such as food and agriculture, thereby threatening our ability to meet America's most fundamental needs.

During a hearing before the House Select Committee on Strategic Competition between the United States and CCP officials, FBI Director Christopher Wray issued a stark warning about the immediate risks posed by the CCP to U.S. national and economic security. Wray called the CCP's aggression the "defining threat of our generation," emphasizing that these threats are already upon us, with U.S. critical infrastructure being a key target. "The PRC cyber threat is made vastly more dangerous by the way they knit cyber into a whole-of-government campaign against us. They recruit human sources to target our businesses, using insiders to steal the same kinds of innovation and data their hackers are targeting while also engaging in corporate deception—hiding Beijing's hand in transactions, joint ventures, and investments—to do the same," Wray said. Indeed, the CCP has made it clear that it considers every sector that makes our society run as fair game in its bid to dominate on the world stage.

Cyberattacks are a primary tool in the CCP's arsenal to target U.S. critical infrastructure. The CCP employs sophisticated cyber-espionage campaigns to infiltrate networks, steal sensitive information, and disrupt operations. One notable example is the 2015 Office of Personnel Management breach, when Chinese hackers compromised the personal data of over 22 million current and former federal employees. This breach exposed sensitive information, including Social Security numbers, fingerprints and background investigation records, providing China with a treasure trove of intelligence that could be used for blackmail or the recruitment of spies.

In addition to direct cyberattacks, the CCP has been implicated in placing backdoors in hardware and software products sold to the U.S. market. Notably, the use of Huawei equipment in telecommunications and ZPMC cranes in port infrastructure has raised significant security concerns. These companies have been accused of embedding spyware in their devices, enabling the Chinese government to eavesdrop on communications and potentially disrupt critical services. This pre-positioning of malicious capabilities within critical infrastructure could cripple U.S. systems during a conflict or crisis, effectively representing a first strike capability in a time of war.

Espionage is another critical threat posed by the CCP, targeting both governmental and private sectors. The CCP uses a variety of methods, including traditional human intelligence and more modern techniques like cyberespionage, to gather information and exert influence. One high-profile case is that of Chinese national Xu Yanjun, a deputy division director at China's Ministry of State Security, who was arrested in 2018 for attempting to steal trade secrets from U.S. aviation and aerospace companies. This case highlights the CCP's focus on acquiring advanced technologies to bolster its own military and economic capabilities.

The risk posed by Chinese espionage extends beyond cyberspace to physical land acquisitions near critical U.S. installations. The CCP

is attempting to acquire land near military installations, defense industrial base facilities, telecommunications hubs, data centers, sensitive fiber pathways and electric grid assets. Such acquisitions provide strategic advantages, enabling China to conduct surveillance, gather intelligence, and potentially disrupt critical operations. For instance, in 2020, a Chinese-owned company attempted to purchase land near Laughlin Air Force Base in Texas, raising alarms about potential espionage activities. These land acquisitions represent a direct threat to national security, allowing the CCP to position itself close to sensitive sites and infrastructure.

Additionally, China's acquisition of U.S. farmland and agricultural assets poses a direct threat to American food and agriculture security. Chinese companies have been purchasing vast tracts of farmland and investing in agricultural businesses, potentially giving Beijing control over significant portions of the U.S. food supply chain. In 2013, the Chinese company Shuanghui International Holdings, now WH Group, acquired Smithfield Foods, the largest pork producer in the United States, for $4.7 billion. This acquisition not only provided China with access to U.S. agricultural resources but also raised concerns about food safety and supply chain security.

The CCP's approach to targeting U.S. critical infrastructure and land through cyberattacks, espionage, malign influence, and threats to food and agriculture security poses a grave and complex challenge. The examples provided offer a glimpse into the CCP's strategic intent to infiltrate and undermine American society at multiple levels. Addressing these threats requires a coordinated response that involves federal, state and local governments, as well as private sector vigilance.

States, being at the forefront of this new strategic threat, must take decisive action. State governments should conduct comprehensive assessments of their vulnerabilities, enhance their cyber defenses, and scrutinize foreign investments in critical sectors. Legislative measures should be enacted to protect state infrastructure from Chinese technology infiltration and to divest state pension funds

from CCP-affiliated entities. Furthermore, states should strengthen their collaboration with federal agencies and private entities to ensure a unified and robust defense against these threats.

By recognizing the scope and nature of the CCP's activities, states can implement targeted strategies to safeguard their critical infrastructure and protect their citizens. In this battle, states can provide important leadership and protection, and their proactive measures are essential to preserving national security and ensuring the resilience of American society in the face of this persistent and evolving threat.

Brian J. Cavanaugh served on the National Security Council from 2018–2021 as the Senior Director for Resilience under both Presidents Trump and Biden. He is currently the Senior Vice President of Homeland Security and Technology at American Global Strategies, a firm founded by former National Security Advisor Robert O'Brien and NSC Chief of Staff Alex Gray.

HOW OUR ENEMIES ARE EXPLOITING AMERICAN UNIVERSITIES - AND WHAT CAN BE DONE TO STOP IT

MY UNIVERSITY, THE UNIVERSITY OF TEXAS AT AUSTIN, PROVIDES TRUSTED SCIENTIFIC, ENGINEERING, POLICY AND LEGAL EXPERTISE TO THE DEPARTMENT OF DEFENSE, THE INTELLIGENCE COMMUNITY AND OTHER GOVERNMENT AGENCIES. BUT UNIVERSITIES ALSO PRESENT VULNERABILITIES THAT THE CHINESE COMMUNIST PARTY, OR CCP, CAN EXPLOIT.

By Adam Klein

VII.

In its great-power competition with the United States, the Chinese Communist Party seeks to exploit our nation's weaknesses and erode our strengths. Since World War II, America's public research universities have supplied scientific and human capital to support our nation's defense. In 1958, spurred by the Soviet Union's launch of the Sputnik satellite, Congress passed the National Defense Education Act, investing in science, mathematics and instruction in Russian and other priority languages on our nation's campuses.

America should expect no less of its great universities today. Indeed, many are already rising to the call. My university, the University of Texas at Austin, provides trusted scientific, engineering, policy and legal expertise to the Department of Defense, the intelligence community and other government agencies. Our public research universities also introduce adventurous students from around the world – including students from China—to the principles of freedom and rule of law at the heart of our American experiment.

But universities also present vulnerabilities that the Chinese Communist Party, or CCP, can exploit. Research laboratories face human- and cyber-espionage threats from Chinese intelligence services. Confucius Institutes on American campuses (now mostly closed) and outposts of American universities in China (many still open) create financial links that can compromise U.S. universities. Secretive CCP money seeks to suborn researchers in high-priority

scientific fields. Meanwhile, CCP informants intimidate Chinese students who have come to American universities to study in freedom.

State universities must mitigate these risks, but they should not stop there. Within the appropriate bounds of their academic mission, universities can also help our nation to prevail in great-power competition with the CCP.

TAKE RESEARCH SECURITY SERIOUSLY

American research universities are the world's best. Their technical prowess is an invaluable national asset—but also a vulnerability. China covets American expertise in areas with potential defense and security applications. These include artificial intelligence, semiconductors, quantum computing, materials science, aerospace, acoustics and signal processing, advanced manufacturing and biotech. But American know-how in non-defense fields is also valuable to the People's Republic of China, or PRC, and its companies, which aim to undercut and displace American competitors.

Some universities have struggled to appreciate and react to this threat. Academic culture and tenure incentives encourage academics to publish research results, rather than shielding them. Scientific researchers, unlike national-security experts, rarely see their own work as connected to geopolitical rivalries. Unfortunately, that is precisely how the PRC sees their discoveries—as a potential American advantage to be appropriated and ultimately surpassed.

The CCP threat to our universities' discoveries takes several forms. One is hacking: infiltrating computer networks to exfiltrate sensitive research findings or personal data. Universities must thus harden their cybersecurity practices, recognizing that they are a priority target. In particular, they should focus on dual-use research with potential defense applications, recognizing that this information is likely to face a high-end cyber threat.

The second threat is financial suborning of American researchers. China's "Thousand Talents Program" aims to lure leading researchers, scientists, engineers and other experts from foreign countries. Most notoriously, Charles Lieber, chair of Harvard's chemistry department, accepted hundreds of thousands of dollars in Thousand Talents funding from the Wuhan University of Technology. Lieber was later convicted of lying to federal authorities about his Thousand Talents contract and his income from China. In another case, Sung Guo Zheng, a biomedical researcher at Ohio State, was convicted of plotting to smuggle scientific developments from his federally funded lab back to China to benefit the PRC.

A third challenge is human intelligence collection, which can include recruiting witting or unwitting agents with access to sensitive research data. Classified research at universities, of course, is limited to U.S. citizens. But much of the unclassified research taking place on U.S. universities, on topics ranging from AI to semiconductors, still holds great potential value to the PRC. And students with PRC citizenship working in research labs at U.S. universities have served as clandestine intelligence collectors in the past.

This raises delicate questions. The American people have no conflict with the Chinese people—only with their government, which deprives its own citizens of their natural rights and threatens aggression against our allies, servicemembers and homeland. We should also remember that many PRC students come to our universities precisely to escape the stultifying repression on their own campuses and to experience the freedoms that America offers. In this competition between systems, allowing PRC students to experience freedom of expression is one way that we may be able to influence them.

Yet there are undeniable risks. Officers from China's Ministry of State Security task "loyal" PRC students studying at U.S. universities with monitoring other Chinese students, often through

“Chinese Scholars and Students Associations” controlled by PRC diplomatic posts in the U.S. The head of the U.S. government’s National Counterintelligence and Security Center has confirmed that Chinese students on American campuses “risk being targeted from harassment” if they depart from the “views and ideology of the Chinese Communist Party” on such sensitive topics as Tiananmen Square, Uyghurs, Taiwan, Hong Kong and Xi Jinping.

Most worryingly for U.S. researchers, Chinese intelligence services recruit some PRC students in the United States to serve as witting or unwitting intelligence collectors, harvesting secrets from university research labs to bring back to China. In one prominent example, Chinese students in a lab at Duke University took photographs and measurements of sophisticated technology that could cloak objects from microwave signals—a device with obvious military applications. They then returned to China and built an exact replica.

Many universities already have research security programs, and university leaders are increasingly attuned to the threat posed by PRC infiltration and intellectual-property theft. My university maintains a robust research-security program that reflects its trusted relationships with the U.S. Department of Defense and other federal agencies.

Yet faculty members at some universities remain skeptical. For example, after receiving a counterintelligence briefing from federal officials, one MIT professor insisted that “law enforcement should come onto campus only when there is clear evidence of a crime.” That is not how counterintelligence works: by the time there is clear evidence of a crime, it’s too late. From the professors’ perspective, however, the response is unsurprising. They do not see the world in terms of geopolitical rivalries, but rather as an international community of scientific collaborators committed to open research. Explaining how research-security efforts fit into the broader context of geopolitical competition and the PRC’s military threat to the United States may win counterintelligence officials a warmer reception on campus.

HELP HARDEN THE TARGET

Universities present vulnerabilities, but they can also help their states become more resilient against the CCP cyber threat.

In many states, research universities offer the greatest concentration of technical talent and human resources available to state leaders. State universities are funded by the people of the state, and their missions are ultimately prescribed by state legislatures. They have a moral, if not statutory, responsibility to help protect their states, within the appropriate limits of their academic missions.

That help can be especially valuable in cybersecurity. State agencies should be able to defend themselves, but most critical infrastructure is in private hands. Nor can the federal government realistically take direct responsibility for the multiplicity of soft targets around the country. Utility districts, hospitals, school districts, ports and other transportation nodes and first responders present easy targets for ransomware and other cyberattacks. And such targets can create chaos for communities if taken offline. PRC hackers know this and would certainly not consider these targets off-limits in the event of war with the United States. Unfortunately, many such targets fall below the "security poverty line": they lack the budgets or profit margins to invest in boosting their cybersecurity.

That is where state universities can help. Universities have cyber expertise and a ready workforce: students. At UT-Austin, the Applied Cybersecurity Community Clinic trains students in basic cybersecurity techniques and then deploys them, with supervision from experienced cyber experts, to help secure vulnerable organizations. Students get course credit, organizations get better security, while the state of Texas shrinks its attack surface and builds a qualified cybersecurity workforce.

FOLLOW THE MONEY

A federal law, Section 117 of the Higher Education Act of 1965, already requires universities that receive federal funds to disclose foreign contracts and gifts. The Department of Education publishes that data on its website each year. Section 117 does not, however, prohibit universities from receiving funds from Chinese sources. The House Committee on Foreign Affairs recently reported that universities have taken in more than $426 million from Chinese sources since 2011. Bloomberg put the number at $1 billion. Some of these funds may be innocuous; others are not. For example, Huawei secretly funded a research competition for U.S. universities, despite the company's close ties to the CCP and widely documented national security concerns.

States can impose more stringent requirements on their public universities. For instance, states could require that universities notify the state-level supervisory body (Board of Regents, Board of Visitors, etc.) in advance of every gift from, or contract with, an entity from an adversary nation as defined by federal law. (Federal statues and regulations contain many such lists. All include China, Russia, Iran and North Korea; some add Cuba and Venezuela's Maduro regime.) This would give state regulators an opportunity to ensure that each gift serves appropriate academic purposes and does not create inappropriate financial dependency.

States could also consider adopting at the state level certain reforms recommended by the House Select Committee on the Chinese Communist Party. For instance, state governments could require their public universities to apply the "know your donor" principle to identify the ultimate party-in-interest behind funds received from sources in adversary nations.

STATE UNIVERSITIES AS A SOURCE OF NATIONAL STRENGTH AND WILL

Many disturbing incidents of anti-Americanism on campus have obscured the fact that universities can also be a profound source of

national strength in our competition with the PRC. Many universities already support defense and intelligence-related research through federal grants and contracts. Some also host Department of Defense-funded university-affiliated research centers, or UARCs, which serve as long-term repositories of technical expertise to support the Department of Defense, or DOD, or intelligence community.

Universities can thus provide a counterweight to Boycott, Divestment, Sanctions-style pressure to shun the U.S. military and defense industry. For example, tech employees have pressured some companies, most notably Google, to end important collaborations with the DOD. And earlier this year, the prominent South by Southwest technology and culture festival in Austin cut ties with the U.S. Army and a major defense contractor. By contrast, just across town, UT-Austin is building a $1.4 billion facility to assemble cutting-edge semiconductors for the DOD.

State universities can also help strengthen our national will to endure and prevail. That means deepening students' understanding of American history and our constitutional traditions – not through indoctrination, but through rich, Socratic engagement with our founding texts and the intellectual traditions that gave rise to them. New institutions such as the School of Civil Leadership at UT-Austin and the Hamilton Center at the University of Florida are showing how to do this with the highest standards of intellectual rigor. No matter how strong our arms, we will lose the competition with the CCP if the American people lose the ability to articulate what we seek to defend.

Adam Klein leads the Robert Strauss Center for International Security and Law at the University of Texas at Austin, where he also serves as a Senior Lecturer in the School of Law. Previously, Klein served as Chairman of the United States Privacy and Civil Liberties Oversight Board, the independent, bipartisan federal agency responsible for overseeing counterterrorism programs at the NSA, FBI, CIA, Department of Homeland Security and other federal agencies.

CCP INFLUENCE OPERATIONS AND ELITE CAPTURE

THE CHINESE COMMUNIST PARTY IS CONSTANTLY SEARCHING FOR "FRIENDS" WHO CAN BYPASS OFFICIAL CHANNELS AND PUSH CHINA'S AGENDA FROM BELOW AS PART OF ITS LONG-RUNNING EFFORTS TO "MAKE THE FOREIGN SERVE CHINA." ONE OF THE CHALLENGES IN IDENTIFYING AN INFLUENCE OPERATION IS THAT THESE ARE NOT COOKIE-CUTTER ACTIVITIES; RATHER, THEY ARE TAILORED TO THE TARGET AND THE PARTY-STATE'S PURPOSES. BUT THEY DO HAVE SOME COMMON RED FLAGS THAT WE CAN LOOK OUT FOR.

By Kelley E. Currie

VIII.

Why has it been so difficult for many American policymakers and other leaders to recognize that the People's Republic of China, or PRC, has been waging a cold war against the United States, and why do so many still refuse to acknowledge this reality? A key reason is the incredible success of Chinese Communist Party, or CCP, influence operations that have facilitated elite capture across America's political, economic, academic and social-cultural spheres. To build up resistance to and resilience against these malign CCP influence operations, our leaders must understand who is being targeted, why these efforts are effective at elite capture and what tools our open societies can use to defend against these asymmetrical attacks.

What does a CCP influence operation look like? These activities exist in the grey-zone between espionage and normal diplomatic tradecraft, which is a major reason they have proven so successful, and are especially difficult to detect and combat. While these activities may superficially look like benign "people-to-people" or cultural exchanges, they have covert, coercive and corrupting aspects—the "three Cs"—that differentiate them from public diplomacy carried out by the governments of the United States and other democracies. These efforts operate under the direction and backing of the CCP but are conducted through a range of organizations and individuals with obscured but deep connections to the Chinese party-state. Some of these organizations are affiliated with Chinese security and intelligence agencies, but the most active and most obscure node of operations is the Central United Front Work Department, or UFWD—a ministry-level instrument of party-state power that has no corollary in a democratic society. United Front work has deep roots in Communist ideology and the founding days of the CCP. Today, the UFWD is headed by Chinese President and CCP General Secretary Xi Jinping, who has described United Front work as one

of the party-state's "magic weapons" (法宝) that are essential to the CCP's hold on power.

Why is the UFWD and United Front work so important to elite capture overseas? In the CCP's totalizing worldview, there is no meaningful difference between domestic and overseas United Front work because the key distinction is between the Party and everyone else. In other words, the party-state uses United Front work to manage groups and individuals who are outside its direct control, whether at home or abroad, but which it deems important to its ability to monopolize domestic political power. In this vein, the party-state has identified twelve groups as priority targets. While these intentionally vague 'priority' categories potentially include anyone in the world who is not a CCP member, within these categories the key targets are those with influence over others or who work in fields such as academia, media and communications, politics and government administration, or critical industries and technologies. As such, subnational authorities are a critical element of Beijing's constant search for "friends" who can bypass official channels and push China's agenda from below as part of its long-running efforts to "make the foreign serve China."

One of the challenges in identifying an influence operation is that these are not cookie-cutter activities; rather, they are tailored to the target and the party-state's purposes. But they do have some common red flags, beyond the three Cs, that we can look out for. One of the biggest tells is the type of organizations that are involved on the Chinese side. Since 2013, Xi has worked to dismantle any attempts at building independent Chinese civil society. Today, it is a safe bet that any Chinese organization presenting itself as "non-governmental"—especially if its name features a variation on "friendship" or "peace"—is really an instrument of the party-state's United Front work. For instance, the China Association for International Friendly Contact, or CAIFC, the United Front platform of the People's Liberation Army's Political Warfare Department, has co-hosted party-to-party exchanges with American political parties and the CCP. With thousands of United Front organizations

at the national, provincial and local level, as well as in state-owned industries and across all government ministries, the party-state has an almost infinite array of options for running these operations and matching them up with a wide range of targets.

It is especially important for national and subnational policymakers in democratic societies to understand how Beijing targets Chinese diaspora communities—as well as Hong Kongers, Taiwanese, Tibetans and Uyghurs—and to protect these communities from CCP predations. For instance, the UFWD's Xinjiang Bureau is deeply involved in global efforts to whitewash the CCP's genocidal actions targeting primarily ethnic Uyghur Muslims. They use China-based United Front organizations to build partnerships with Muslim leaders and organizations worldwide, hosting them for propaganda "study tours" to China and cosponsoring "religious" conferences where they can reinforce Beijing's narrative that it is engaged in legitimate counterterrorism and poverty alleviation efforts. Within ethnic Chinese diasporas, influence operations target community leaders, Chinese-language media outlets and Chinese-owned business associations. These efforts can range from soft information-gathering to full-blown transnational repression, and often involve the promise of economic benefits or the threat of harm. Local and state agencies that should be the front line of defense for these communities are often oblivious to these activities due to linguistic and cultural barriers, or are fearful of investigating them because they lack expertise or have concerns about racial profiling.

In fact, now that U.S. and national-level authorities in other democracies are more attuned to the dangers of CCP foreign influence efforts, Beijing seems to be redoubling its efforts at the sub-national level. After a brief respite during the COVID-19 pandemic, there has been a dramatic resurgence of United Front work targeting local and state officials, elected representatives, media outlets and other influence nodes. One of the main vehicles for these activities is the Chinese Peoples' Association for Friendship with Foreign Countries, or CPAFFC, an organization under the

Ministry of Foreign Affairs that specifically targets subnational governments. In October 2020, the U.S. Department of State canceled a memorandum of understanding that made the CPAFFC the Chinese lead in organizing the U.S.-China Governors Forum. The Department's cancellation announcement cited CPAFFC's attempts to "directly and malignly influence state and local leaders to promote the PRC's global agenda." Nonetheless, CPAFFC's activities in the U.S. continue to this day through venues such as the China-U.S. Sister Cities Conferences, the U.S.-China Bay to Bay Dialogue hosted at the University of California at Berkeley, and relationships cultivated with the "Flying Tigers" veteran air force pilots.

Given the hydra-headed nature of China's well-resourced influence operations and the limited resources available to subnational authorities, this threat can seem overwhelming. It is important that state and local policymakers recognize how the strengths of our democratic society can be leveraged to resist these efforts. The values of transparency and reciprocity are two of the most powerful tools we have. General regulations requiring disclosure of all funding sources and linkages to foreign entities, in line with the federal Foreign Agent Registration Act and similar rules, provide transparency about organizations that are hosting mayors and lawmakers on foreign travel or supporting academics testifying in a legislative hearing. Establishing trusting and supportive relationships between law enforcement and communities that are likely to be targeted by influence operations is also key. There is also more widely available and easily accessible open-source research and information than ever about CCP agents of influence such as CPAFFC. American civil society organizations can help subnational authorities and actors identify credible sources of information, connect them with expertise and help them defend their communities against this threat. Working together with civil society, experts and other policymakers, subnational leaders can help to transform our federal system from a source of potential vulnerability to a source of strength by creating thousands of points of vigilance and resilience.

Ambassador (ret.) Kelley E. Currie is an American human rights lawyer and former government official who served as the U.S. Representative to the United Nations Economic and Social Council and as the Acting Deputy Representative of the U.S. to the U.N. She is currently a founding partner of Kilo Alpha Strategies and a senior non-resident fellow with the Atlantic Council.

IT'S TIME TO STOP STATE FUNDING OF CHINA'S MILITARY BUILD-UP AND HUMAN RIGHTS ABUSES

TOTAL AMERICAN HOLDINGS OF CHINESE EQUITIES PRESENTLY EXCEED WELL OVER $1 TRILLION; DEBT HOLDINGS IN DOLLARS AMOUNT TO NEARLY A TRILLION DOLLARS MORE. PRECISE CALCULATIONS AND VERIFIABLE VALUATIONS HAVE BEEN MADE DIFFICULT TO ASCERTAIN, FOR CHINA USES COMPLICATED LEGAL STRUCTURES, INDEX FUNDS AND TAX HAVENS TO MASK ITS ACTIVITIES INVOLVING U.S. EXCHANGES.

By Roger W. Robinson

IX.

For more than two decades, trillions of dollars of U.S. capital—drawn from scores of millions of unwitting American investors—have been funneled into Chinese state-controlled companies, including those tied to the People's Liberation Army, or PLA. This has taken place via Beijing's unfettered exploitation of the U.S. capital markets and private equity funds with virtually no screening, diligence or security-minded scrutiny by the U.S. government or the financial services industry.

This immense infusion of American wealth and cash into the coffers of the Chinese Communist Party, or CCP, has allowed—and funded—China's rise to become a near-peer military competitor to the U.S. It has also underwritten the evisceration of human rights in China, all while avoiding the same regulatory compliance requirements adhered to by companies of every other country in the world, including U.S. firms (i.e., courtesy of the May 2013 Memorandum of Understanding concluded between America's Public Companies Accounting Oversight Board and the Chinese Securities Regulatory Commission).

What is even more troubling is the continued use of taxpayer funds to finance the military modernization of the PLA and egregious Chinese corporate human rights violators. State public employee retirement systems have funneled taxpayer funds into China, despite having witnessed the asymmetric material risks involved in investing in adversary nations—as vividly shown by Russia's invasion of Ukraine. A recent report from Future Union found that state pension funds have made some $68 billion in new investments in China just since 2021.

In its 2021 Report to Congress, the U.S.-China Economic and Security Review Commission described the massive exposure of U.S. individual and institutional investors to Chinese equity and debt securities as worrisome. Total American holdings of Chinese equities presently exceed well over $1 trillion; debt holdings in dollars amount to nearly a trillion dollars more. Precise calculations and verifiable valuations have been made difficult to ascertain, for China uses complicated legal structures, index funds and tax havens to mask its activities involving U.S. exchanges.

NON-TRANSPARENCY ON CHINESE RISK EXPOSURE

As a result, the true level of American financial exposure to CCP-controlled companies and sovereign bonds is not fully known. This, and many other abuses of our equity and debt markets, are due, in large part, to U.S. government regulatory failures on the part of the Executive Branch agencies with primary responsibility for our financial markets (i.e., the Department of the Treasury, the Securities and Exchange Commission and the White House National Economic Council), which are most often headed by conflicted Wall Street executives.

These federal agencies also lack the rigorous national security mindset and expertise to assess and defend our security interests—including the protection of human rights and U.S. retail investors—from the predatory, strategic, non-transparent and non-market practices of Chinese and other authoritarian-controlled enterprises.

Those Congressional Committees with financial services oversight responsibilities have also become excessively, if not completely, beholden to Wall Street, due, in no small part, to generous campaign contributions. This has resulted in the successful thwarting of urgently needed legislation to make illegal a number of these fiduciarily reckless avenues of U.S. investing in China (several of which are listed below).

THE TSP PRECEDENT

For example, American investors remain uninformed that their pension and other stock portfolios often include a significant number of U.S.-sanctioned Chinese companies. Tragically, it is not unusual to find sanctioned Chinese PLA-linked companies and corporate human rights violators among the holdings of state retirement systems.

Worse still, states have received a clear message from the federal precedent set with regard to excluding in 2023 all mainland- and Hong Kong-based Chinese companies from the International Fund of the roughly $700 billion Federal Thrift Saving Plan, or TSP. This was a hard-fought policy battle for nearly five years against Wall Street firms (principally BlackRock), Treasury and the Federal Retirement Thrift Investment Board that administers the TSP (primarily composed of former Wall Street executives).

The reasons given for this divestment and exclusion decision had everything to do with the unacceptable levels of fiduciary, national security and human rights risks associated with such China exposure. One would think that the states would immediately follow suit for "investor protection" reasons alone. but that simply has not happened (except in a few cases). It did, however, severely compromise the opposition arguments of state pension system administrators and those in the state siding with Wall Street and, wittingly or unwittingly, the CCP.

THE REMEDY

Not surprisingly, the CCP is utterly indifferent to the serious losses that already have been sustained by American pensioners, particularly over the past three years. Prominent Wall Street asset management and other firms are, sadly, aligned with the CCP with respect to the calloused, malfeasant and greed-driven practice of

dismissing national security and human rights considerations and the associated asymmetric risks to average American investors.

Accordingly, bipartisan legislation and executive action is urgently required to declare illegal the holdings of a wide range of tainted, and even dangerous, Chinese corporate securities by U.S. investors worldwide. Moreover, state public pension administrators should be legislatively compelled to divest from: U.S.-sanctioned Chinese companies; Chinese "A-Share" companies, unregulated enterprises listed exclusively on Chinese domestic exchanges (as many as 4,000 of which are traded in the U.S. capital markets, primarily in the form of Exchange-Traded Funds, or ETFs, and other index funds); Chinese sovereign bonds, providing discretionary cash directly to the coffers of the CCP; Variable Interest Entities most often domiciled in the Cayman Islands that essentially substitute contracts with shell companies for actual shares of Chinese companies listed on the New York Stock Exchange and NASDAQ (without respecting minority shareholder rights or providing legal recourse); and Chinese companies that are equipping, and otherwise propping up, adversary regimes in Russia, Iran and North Korea.

The simplest way for states to eliminate their exposure to risky, non-transparent Chinese securities is to divest entirely from the companies of China and other adversary nations as expeditiously as possible (e.g. move to Ex-China Emerging Markets funds, ex-China ex-Hong Kong global index funds, etc. – virtually all of which, at this writing, are providing U.S. investors with higher returns and lower risk).

In addition, American asset managers should provide more robust and liquid investment options for state funds that seek international investment vehicles without risk exposure to adversary nations. Texas Gov. Greg Abbott, South Dakota Gov. Kristi Noem, Mississippi Gov. Tate Reeves and Iowa Gov. Kim Reynolds have publicly called for asset management companies to develop these alternatives.

Moreover, every state legislature should legally require the immediate public disclosure of their state's Chinese corporate securities and sovereign bond holdings (i.e., stocks and bonds), if the governor and other senior state officials continue to stonewall this essential action. This public list should include Chinese companies embedded in ETFs and other index funds. Today, in many cases, a list of state holdings in Chinese corporate and other securities are deliberately covered up from public view, as anyone seeking this information, even those working within state governments, will soon learn the hard way.

MOVING FORWARD

Our nation urgently requires an operational plan that minimizes U.S. investor losses, while transitioning out of PRC-related investments at flank speed. Just as the Reagan Administration configured a detailed plan to irreparably curtail and damage the Soviet Union's hard currency cash flow and access to external sources of Western financing, the denial of hundreds of billions of U.S. investor dollars from various sources annually into the coffers of the Chinese government can curtail the CCP's malevolent actions globally.

It is important to remember that the U.S. utterly dominates the global financial domain. We have the bulk of the world's investable capital, capital markets roughly the size of the rest of the world's combined and the world's reserve currency. In sharp contrast, China lacks even a convertible currency and is in the throes of both a debt crisis at the local government level and a debilitating property crisis. Foreign investor money is—at long last—fleeing China for a number of solid fiduciary reasons.

State divestment plans will also encourage more aggressive action from federal lawmakers and America's allies to adopt similar legal prohibitions and other prudent, sensible measures to protect our common security interests, fundamental values, retail investors

and public pensioners. States must likewise review their business incentive programs to ensure they are not funding PRC companies within their states.

Tax credits and other economic incentive programs should not be used to attract foreign adversaries. Chinese multi-national corporations inevitably come with malign strings attached. Seen or unseen, their ties to the CCP (with CCP cells actually embedded in their senior management structures) are impossible and imprudent to ignore.

For some 25 years now, trillions of dollars of American private capital and taxpayer funds have been used to prop up and modernize the Chinese military and underwrite the country's geopolitical and economic aggression, as well as egregious human rights abuses.

State leadership is urgently needed to inspire Congress, and to silence those members and executive branch officials who have, in effect, served as subsidiaries of Wall Street to preserve this disastrous and scandalous status quo. Greed must no longer be permitted to continue to prevail.

Roger W. Robinson is the former Senior Director of International Economic Affairs at the Reagan National Security Council and former Chairman of the Congressional U.S.-China Economic and Security Review Commission.

STATE LEADERS MUST DRIVE AMERICA'S WHOLE-OF-GOVERNMENT RESPONSE TO THE CHINESE COMMUNIST PARTY THREAT

CCP GRAND STRATEGY FOCUSES ON PENETRATING THE UNITED STATES FROM THE STATE AND LOCAL LEVELS TO DISRUPT AMERICAN SECURITY FROM THE BOTTOM UP AS MUCH AS FROM THE OUTSIDE IN. THEIR APPROACH IS CAPTURED IN PART BY THE PHRASE "USE THE LOCAL TO SURROUND THE CENTRAL," A LOGIC THAT ENTAILS INFLUENCING STATE AND LOCAL POLITICAL LEADERSHIP TO "SURROUND" AND INFLUENCE FEDERAL POLICYMAKING.

By Michael Lucci

X.

In the Chinese Communist Party, or CCP, the United States faces an adversary unlike any from our past. The CCP is challenging American power in the military, economic, technological, cultural and diplomatic realms, and it has even laid designs upon the American homeland. Only a whole-of-government response that leverages state powers will be sufficient to counter the comprehensive threat of Communist China.

States are now on the front lines against America's global adversaries, and state leaders must build new layers of armor to protect against our foremost adversary, the CCP. Americans historically associate national security with the federal government, and for centuries Americans have safely assumed that our oceans provide shields against foreign aggression. But these premises no longer hold, and China's government views our openness and decentralized federalist system as a vulnerability to exploit.

CCP grand strategy focuses on penetrating the United States from the state and local levels to disrupt American security from the bottom up as much as from the outside in. Their approach is captured in part by the phrase "Use the local to surround the central," a logic that entails influencing state and local political leadership to "surround" and influence federal policymaking. States are also valuable end-targets in themselves. At the state level, the CCP can develop technological dependencies, infiltrate critical infrastructure, corrupt the education system, siphon off

American capital, conduct political influence campaigns, attack free speech and generally erode America's internal strength.

The American heartland is already plagued by China's hybrid warfare. Fentanyl overdoses are the #1 cause of death for military-aged Americans, killing 100,000 people per year and causing $1.5 trillion in annual economic losses. According to Attorney General William Barr, China isn't merely the source of the fentanyl that is killing Americans, China's government and Communist Party officials are "prime movers" who are sponsoring and encouraging the export of fentanyl to the United States. Chinese criminal organizations launder the fentanyl profits to finance this cycle of mass murder. "Simply put, without China's production and export of fentanyl and fentanyl precursors, there would be no fentanyl crisis in the United States and the mass slaughter would effectively stop," Barr said. Fentanyl is Chinese government policy in action within America.

CCP cyberespionage groups such as Volt Typhoon are infiltrating critical infrastructure for the purpose of taking down American water, power and transportation systems in the event of a conflict. And CCP soft power influence campaigns are accelerating across domains within America, conducted through various United Front organizations, social media applications, businesses, education organizations and other Communist Party cut-outs.

Aggression that would have been unthinkable only 20 years ago is now common. Under dystopian programs such as "Operation Fox Hunt," China's government hunts down Chinese dissidents and American citizens within America, attacks their basic constitutional rights and even places bounties on the heads of Americans in the United States. China's influence campaigns even include the cultivation of spies in state and local governments. For proof, look no further than New York, where a former aide to Gov. Kathy Hochul has been arrested on charges of working to advance CCP interests. If CCP transnational repression is not crushed upon reaching our shores,

this foreign adversary will gradually wither away our constitutional protections.

The CCP's remarkable gains in the U.S. have come at the expense of America's economic and political strength. Americans should consider what our country will look like if Chinese aggression and hybrid warfare continues unabated for another 20 years.

These losses can and must be reversed. American economic and political strength can be revitalized from the inside out, and the restoration of our constitutional traditions and enhancement of our federalist system can be leveraged to deter and defeat CCP aggression. While China's grand strategy targets America at the state and local level, American strategy must leverage state powers to fight back. Bold state leadership is critical to execute a successful American political counterattack against the CCP.

First, state leaders must clearly understand that the regime that is intentionally mass poisoning their citizenry with fentanyl is the same regime controlling state pension investment dollars in China, the technology states procure from Chinese firms, the business ventures that want access to state land, property and critical infrastructure, the sponsorship of research and academic collaborations with state universities, and the CCP-linked nonprofits that operate openly to sway state and federal policy.

Next, states must move swiftly to secure the homeland and prepare for the fallout of a potential Chinese invasion of Taiwan. The coronavirus pandemic taught state and local leaders that a crisis originated from China can catalyze mass chaos in America. If China makes good on its repeated warnings to invade Taiwan, federal leaders have warned that state leaders can expect massive cyberattacks upon critical infrastructure in order to sow chaos and cripple America's response. If an attack on Taiwan happens, supply chains dependent upon China will fracture and states will suffer huge financial losses on any assets held in China. States should conduct

a tabletop exercise of an invasion scenario, anticipate the damage it would cause, and protect against supply chain, critical infrastructure and financial damage before it is too late.

States must stop underwriting China's military and technological development. Public pension investment dollars and economic incentives should never benefit companies that are ultimately beholden to the CCP. And despite ample warning of espionage risks, states continue to procure technologies from companies that are sanctioned by the United States federal government for their military connections and human rights abuses. States must completely phase out Chinese technologies from their public procurements, including drones, cameras, computers, laser sensor technologies, DNA sequencing devices, telecommunications equipment and automobiles.

Finally, states must lead in dismantling the vast influence campaigns conducted through CCP United Front entities. New laws are needed to crack down on foreign agents from adversary nations, and criminal codes must be updated to empower law enforcement to understand and punish transnational repression and other crimes that are specific to hostile foreign regimes such as the CCP. America's universities should bolster their liberal traditions of open inquiry, but simultaneously unwind their connections to academic and business institutions beholden to the CCP. Liberal ideals will not survive on U.S. campuses if they accommodate infiltration by an authoritarian government.

The era of waiting for China's communist regime to liberalize, respect America's traditions and behave within our borders is over. A new era of defending all we hold dear has begun.

State leaders must contribute to whole-of-government deterrence by boldly countering the CCP across all domestic threat areas, defending against China's hybrid warfare and reorienting state policies in recognition of the Communist Party's comprehensive strategy to

undermine the United States. America's liberal order will ultimately win out at home and abroad, but only if we leverage internal state strengths to stop communist aggression within our borders.

Michael Lucci is the founder and CEO of State Armor.


CITIZENS
FOR FREE
ENTERPRISE
ACTION
STATE
ARMOR