CENTER
FOR SECURITY POLICY

FEBRUARY 2023

What a Failed Response to the Chinese Spy Balloon Should Tell State Leaders

BY TOMMY WALLER & CHRISTOPHER HOLTON

What a Failed Response to the Chinese Spy Balloon Should Tell State Leaders

BY TOMMY WALLER & CHRISTOPHER HOLTON

The nation watched transfixed, as a Chinese balloon, described by the U.S. Department of Defense as a "surveillance" balloon, transited the entire span of the continental United States from January 28th to February 4th, when it was finally downed by U.S. military aircraft off the South Carolina coast.

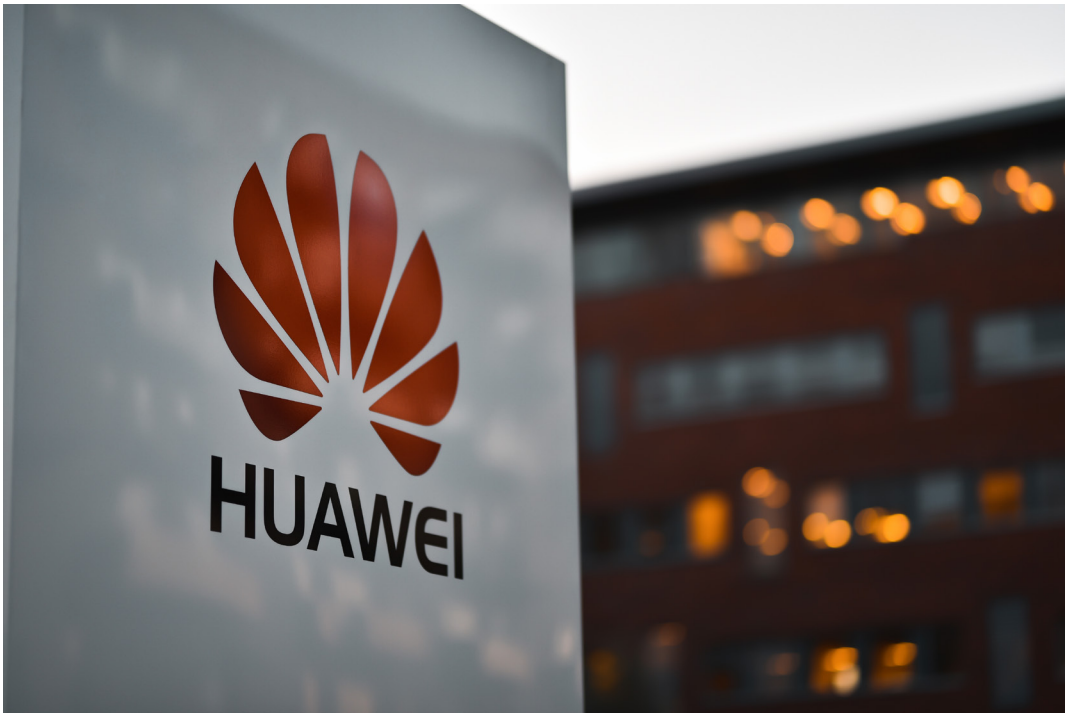
The exact purpose of the balloon remains unclear.

The Chinese government claimed the balloon was for "civilian" purposes and associated with gathering weather related information but which flew off course. Yet the balloon's path took it directly into proximity with nation's most important military installations; those associated with strategic nuclear weapons and missile silos. Even if a mere "weather" balloon, China could still benefit from gathering detailed weather and meteorological data associated with those missile sites for use in precision targeting with their own ballistic missile systems.

Perhaps the most dangerous scenario would have been if the balloon were intended as a delivery platform for a nuclear electromagnetic pulse (EMP) attack. As the balloon transited U.S. airspace, it seemed to maintain an altitude of approximately 60,000 during most of its flight, but at times increased its altitude. At approximately 100,000 feet (or 30km) and higher a nuclear detonation produces an invisible pulse that is devastating to electronics and our nation's electric grid. Experts have warned of the prospect of a "balloon EMP attack scenario" for several years and some have suggested that this was a "dry run" for such an attack.

But the purpose of the balloon is just one factor in a larger, more concerning strategic question on the minds of the American public and state leaders alike which is: Why did the federal government let the balloon simply fly by before it took action?

Montana Governor Greg Giaforte complained that he was not informed of the balloon's presence until it was "hundreds of miles" within the state's borders and had already surveilled critical military infrastructure, and noted that "If it was up to Montanans, this thing would have been taken out of the sky the moment it



Copenhagen / Denmark - 07.23.19: Signboard of Huawei corporation on factory background in night - Oleksandr - stock.adobe.com

entered our sovereign airspace." Missouri Governor Mike Parson took to Twitter to complain he'd received "zero communication" from federal officials about the balloon's entry into his state.

In the face of growing criticism over the delayed response to the penetration of U.S. airspace, leaks from U.S. government sources later alleged that Chinese balloons had also penetrated U.S. airspace under the previous administration, as though this either explained or excused the delayed response.

The reality is that the saga of the Chinese surveillance balloon is merely one more in a string of threats and provocations emanating from the People's Republic of China met with a weak or belated federal response.

As Governor Giaforte rightly noted, American citizens, of every state, look to their elected leaders to act against national security threats emanating from the People's Republic of China.

Increasingly, the lack of federal resolve against a growing array of Chinese threats underscores the need for states to build up their own capabilities to respond. In this piece we will explore eight examples where the federal government has allowed aggressive Chinese government action to harm the safety and security of U.S. citizens across the nation. We'll also look at some of the ways state leaders have stepped up to fill the "balloon-sized" holes in our national security this federal laxity on China has created.

Chinese Penetration of Critical Infrastructure

Telecommunications

While some observers noted that the recent Chinese surveillance balloon may have been equipped with signals intelligence and video surveillance equipment, in fact Chinese penetration of the telecommunications industry has already exposed Americans to far more

extensive surveillance.

The Federal Communications Commission only recently voted to prohibit the use of public funds to purchase equipment from five Chinese companies over national security concerns, and only after Congress applied needed pressure through the "Secure Equipment Act of 2021." All of those companies, (Huawei, ZTE Hytera, Hangzhou Hikvision Digital Technology, and Dahua) are backed by the Chinese government, and therefore open to major influence by the Chinese Communist Party (CCP). These companies involved in the video surveillance field not only pose a threat to US infrastructure; they also are involved in ghastly surveillance networks inside China characterized by human rights abuses.

However, it is unclear whether the federal government will do anything about rural cell networks *already* using this Chinese equipment. Despite ample media reports chronicling the risks of Huawei equipment in rural telecom networks, such as those right outside Malmstrom Air Force Base and its ICBM missile fields in Montana (the same installation targeted by China's balloon), there doesn't appear to be any movement at the federal level to require replacement for that equipment.

Telecommunications regulation is one place where states can choose to be more aggressive, however. For example, Louisiana State Senator Barry Milligan recently successfully authored legislation this year to protect his state's critical infrastructure from these nefarious Chinese tech companies.

The first piece of legislation, signed into law as Act 695 of 2022, prohibits state agencies and universities from using telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation and video surveillance equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, Dahua Technology Company, or any subsidiary or affiliate of such entities.

The second piece of legislation, signed into law as Act 766, prohibits the use by any agency of state government of telecommunications equipment or video surveillance equipment produced or provided by an entity found to be owned, controlled, or otherwise connected to the government of the People's Republic of China, the Islamic Republic of Iran, North Korea or Russia. The effect of this legislation is targeted at China since the other nations either do not have capabilities in the telecommunications or video surveillance field (such as North Korea) or are already sanctioned by US government policies (such as Iran). The Act also provides that if a vendor uses components from any such entities, the vendor must replace them at the vendor's own expense. By mandating that state agencies, such as colleges and hospitals, not include Chinese components in critical infrastructure Louisiana is setting an example for the private sector as well as helping to create an alternative market for technology vendors using safe and secure American critical components. For the purposes of the legislation "critical infrastructure" means a communication infrastructure system, cybersecurity system, electric grid, hazardous waste treatment system, or water treatment facility.

Every state needs to follow suit and pass legislation like Senator Milligan's in Louisiana. By protecting infrastructure inside each respective state, they will also be protecting our nation as a whole.

CenterPoint Energy sub station providing power to downtown Houston - Joe Hendrickson - stock.adobe.com

The Electric Grid & Transformers

Similar to the telecommunications sector, the nation's electrical grid infrastructure has growing exposure to Chinese components, leaving it vulnerable to malicious action – exposure that goes largely unmitigated by the federal government.

Transformers serve as the "backbone" of modern electric grids. They are time consuming and difficult to manufacture, transport, and install but they play a critical role in moving electricity over long distances. In the past decade, China has made itself a leader in transformer manufacturing and exports these transformers around the world –especially to the United States.

At least two transformers from China have already been discovered to contain hardware backdoors that could enable Chinese agents to remote-access and manipulate them. In the summer of 2018 the U.S. government seized a Chinese transformer in the Port of Houston and transported it to Sandia National Laboratories for a comprehensive examination.

"They found hardware that was put into that that had the ability for somebody in China to switch it off," said Latham Saddler, the former Director of Intelligence Programs at the National Security Council in the last administration. The Trump Administration tried to address the issue with Executive Order 13920 "Securing the United States Bulk-Power System" and by declaring a "national emergency related to the physical and cybersecurity of the US bulk power grid."

Government bureaucrats slow-rolled progress until January 20, 2021, however, when President Biden inexplicably suspended EO13920. There are now believed to be somewhere on the order of 400 such Chinese transformers in the grid.

In the absence of federal action, States have taken action to address the penetration.

Texas, which has its own electric grid, was the first state to take the lead addressing this threat. The "Lone Star Infrastructure Protection Act," co-authored by Texas state Senator Donna Campbell and state Representative Tan Parker, was signed into law on June 18, 2021 by Governor Abbott.

South Carolina followed suit last month with the "State Infrastructure Protection Act" modeled closely off of Texas. Every other state should take similar, but even more aggressive steps by ensuring that these Chinese transformers are identified and replaced as soon as possible.

States should also explore incentives to attract manufacturers to begin producing more transformers domestically. U.S. Navy veteran and former National Security Council staffer Joshua Steinman offered an innovative idea via twitter, to drum up a market for potential "made in America" transformers. Steinman proposed states use legislation to signal a public policy preference for critical infrastructure produced entirely from U.S.-sourced components. Such legislation might help convince investors of the potential market value for such U.S.-made transformers.

Agricultural Land & Military Installations

While emphasis on critical infrastructure often focuses on cyber-espionage and advanced technical components, Food and Agriculture is one of America's 16 critical infrastructure sectors. Included in that sector is ownership of valuable U.S. farmland. In recent years China has advanced a deliberate policy of strategic acquisitions of agricultural technology, companies, and even arable land.

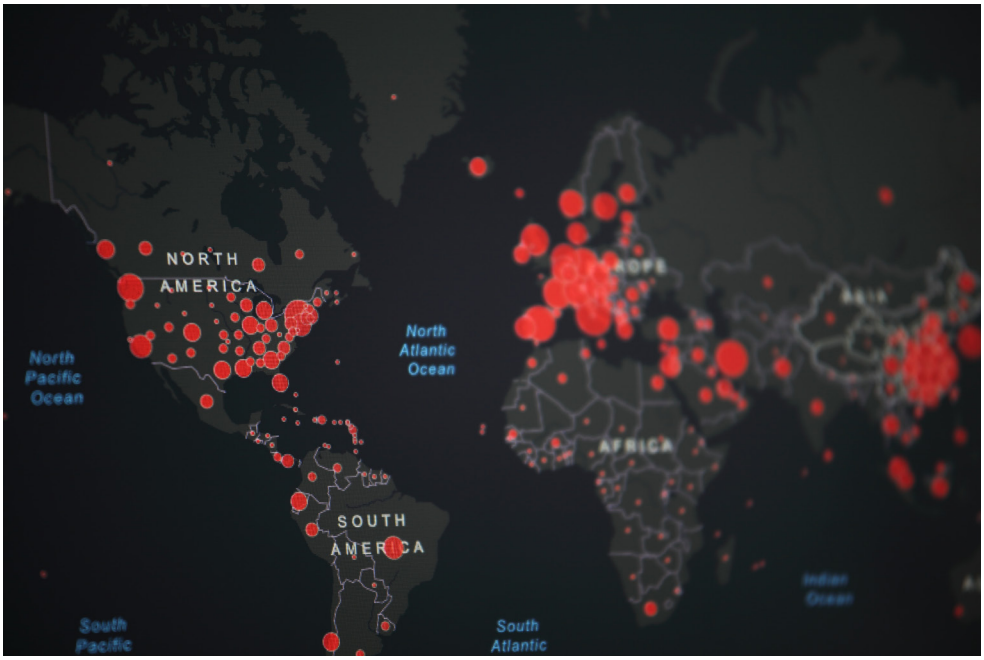
Part of CCP land acquisition in the US involves not only valuable farmland, but massive tracts in strategically sensitive areas. A case in point is the Party-controlled Fufeng Group's 2021 purchase of a 370-acre parcel in Grand Forks, North Dakota. This land is just 12 miles from Grand Forks Air Force Base, a critical military installation that conducts a range of sensitive military training exercises for the U.S. Department of Defense.

It is just 67 miles from Cavalier Space Force Station, which operates and maintains the Perimeter Acquisition Radar Attack Characterization System (PARCS), a phased-array radar system that tracks over half of all earth-orbiting objects; provides critical missile warning and space surveillance data to North American Aerospace Defense Command (NORAD), United States Space Command (USSPACECOM), and regional combatant commanders; and provides attack characterization data to the Secretary of Defense and the President for real time war plan execution decisions.

The Committee on Foreign Investment in the United States (CFIUS) determined that the Fufeng purchase did not fall under its jurisdiction however.

After months of public outcry, the U.S. Air Force finally made a rare public statement calling the deal "a significant threat to national security." As a result the local mayor and city council denied Fufeng the necessary permits to continue the project.

When tracking CCP land acquisitions, a pattern emerges which suggests a non-agricultural agenda. For example, the Guanghui Energy Company, whose owner is tied to the CCP, used a shell company to purchase 140,000 acres of land 70 miles from Laughlin Air Force Base in Texas. The project, reportedly intended as a wind farm, would have tied into Texas' electric grid. Despite its proximity to the base, it was state lawmakers, not the Department of Defense, who took action to block the move.



COVID-19 case hotspots around the world - 2020

Despite that arable land is one of America's most crucial resources (and they aren't making any more of it, as the old saying goes) no federal law restricts foreign acquisition of US farmland.

Some existing state laws do restrict foreign agricultural land purchases in a variety of ways, and more states are waking up to the importance of doing so. States including Florida, Missouri, Mississippi, South Carolina, Texas, Utah and Wyoming have all filed bills meant to address this threat.

South Dakota Governor Kristi Noem and South Dakota lawmakers responded with an innovative approach – a new bill establishing at state-level CFIUS to "investigate agricultural land purchases by foreign countries." Noem warned, "We cannot allow the Chinese Communist Party to continue to buy up our nation's food supply."

Public Health and Safety

COVID-19

Of recent events which have focused the American public's attention on the Chinese regime's perfidy, the COVID-19 pandemic was almost certainly the most impactful.

"For at least five weeks beginning no later than December 2019, Chinese officials first covered up and then lied about the human-to-human transmissibility of SARS-CoV-2, telling the world COVID-19 was essentially not contagious, when they knew it in fact was highly so" as a Center for Security Policy report noted.

Yet three years later, the 18 agencies making up the U.S. Intelligence Community remain unwilling to even confirm the origin of the outbreak, let alone discuss the motivations or objectives in China's behavior surrounding the virus' release.

Federal bureaucrats including Dr. Anthony Fauci deliberately sought to silence scientists warning that COVID-19 may have leaked from the Wuhan Institute of Virology. Fauci later misled Congress about U.S. government funding of gain-of-function research at the same lab.

Additionally Federal COVID guidelines adopted a "China Model," emphasizing economy-crippling shutdowns, liberty-violating mandates, and the promotion of intrusive surveillance technology.

Yet some state leaders, most notably in Florida and South Dakota, avoided draconian measures and their economies were among the first to bounce back as a result. As CNN reported:

> South Dakota, Florida, Rhode Island, Nebraska and Idaho are all thriving, operating at or above where their economies were in early March 2020 before the pandemic forced businesses to shutter and workers and students to stay home.
>
> The index is composed of a basket of economic indicators that includes unemployment rates, claims for jobless benefits, consumer spending and consumer behavior.
>
> South Dakota's economy is at 106% of its pre-pandemic strength, according to the index, while Florida's economy is at 101%. The other three states are operating at 100% of pre-Covid level.

In one of his first acts as President Biden reversed a Trump administration decision to withdrawal from the World Health Organization in response to that organization's domination by Chinese influence, and promotion of Chinese propaganda related to COVID-19. The federal government's embrace of the WHO and its proclivity to follow the "China Model" should prompt state governors and legislatures to be especially vigilant when assessing future public health policies.

Fentanyl

As bad as COVID was, it is not the only public health crisis facing the United States due to deliberate policies of the Chinese government or perpetuated by federal government inaction. The *leading* cause of deaths in the US among adults between the ages of 18 and 47 is fentanyl poisoning. Fentanyl, a powerful synthetic opiate which is either mixed into other illicit drugs, or increasingly, consumed by addicts directly.

Hundreds of thousands of Americans have died from this scourge. According to the CDC, "From 2013 to 2019, the age-adjusted rate of deaths involving synthetic opioids other than methadone increased 1,040%..."

The fentanyl threat is exacerbated by the willful actions of the Chinese Communist Party, which has resisted all requests by the U.S. government that it crack down on illicit fentanyl production and the involvement of Chinese companies with the Mexican narcotics trade. Most of that fentanyl flows from Chinese ports and airports and travels to the US via the Mexican drug cartels that control our border. As Center Senior Fellow and Asia expert Grant Newsham writes,

> The fact the Chinese regime doesn't ban fentanyl in its entirety—much less go after producers the way it goes after Uighurs, Christians and Falun Gong, or Hong Kongers—suggests the CCP

DEA Warns of Brightly-Colored Fentanyl Used to Target Young Americans - DEA.gov

---

> is glad America is awash in fentanyl.
>
> And when Trump told Xi to knock off the fentanyl flow back in 2018, Xi reportedly replied: "We don't have a drug problem in China." That means Xi can control the drugs and he's channeling the chemical warfare agents—in true "unrestricted warfare fashion"—towards his #1 rival and greatest enemy.

In addition to the public health crisis posed by fentanyl's illicit use, the drug can also be weaponized relatively easily by rogue actors, including terrorists. The Center's Chris Holton noted:

> If accidental contact with fentanyl can readily cause serious illness and even death, we can be sure that Al Qaeda, the Islamic State and other terrorists have taken notice. In any case there is little doubt that in the hands of nefarious actors, such as terrorists, fentanyl can be used as a weapon of mass destruction.
>
> The US Department of Defense researched the possibility of using fentanyl as a crowd control agent but determined it was far too dangerous to use as a non-lethal agent. That didn't stop the Russians however, who not only weaponized fentanyl, but used it in a hostage situation in a Moscow theater resulting in the death of more than 100 hostages. CDC guidance makes clear that if properly weaponized fentanyl does not have to be ingested or injected to kill.

Fortunately, some states are pushing back – including a bipartisan effort among 18 attorneys general to urge the federal government to classify the illicit form

Chidori_B - stock.adobe.com

of this drug what it actually is - a "weapon of mass destruction." Legislation in several states also seeks to increase criminal penalties for trafficking fentanyl.

Counterintelligence and Subversion:

TikTok

Recently accused of being a form of "digital fentanyl", the Chinese social media app "TikTok" utilizes sophisticated data collection and analysis together with powerful machine learning to manipulate, indoctrinate, and otherwise subvert coming generations of Americans. According to the Wall Street Journal, Tiktok's algorithm curated accounts identified as belonging to minors into "rabbit holes" emphasizing sex, drug abuse, violence, and eating disorders. Meanwhile the Chinese domestic market version of TikTok's promotes patriotism, academic excellence, and personal achievement. This reality led Attorneys General Jeff Landry and Austin Knudsen to refer to TikTok as a "Chinese Trojan Horse."

Additionally, the app's permissions ensure that vast amounts of user data flows directly to TikTok's owner ByteDance, which in turn is obligated by Chinese law to share data with the ministry for state security upon request.

Yet, when it comes to guarding against this problematic app, the federal government is not only absent, but moving in the wrong direction. Upon coming into office, the Biden Administration reversed a previous Trump Administration executive order intended to force the sale of the Chinese-controlled app. Meanwhile U.S. military officers have attempted to skirt security concerns and regulations banning the app in order to target potential military recruits.

At least 16 governors have banned TikTok from state-owned devices: North Dakota, Idaho, Iowa, Texas, South Dakota, South Carolina, Maryland, Utah, Oklahoma, Alabama, New Hampshire, Georgia, Tennessee, Montana, Wyoming and Virginia. Nebraska has had a ban in place since 2020,

Confucius Institute building on the Troy University campus.

Kreeder13 - Image licensed under the Creative Commons Attribution-Share Alike 4.0 International license.

---

which covers all state devices. Louisiana and West Virginia each announced partial bans and Florida legislators are seeking to ban the app from K-12 classrooms.

Confucius Institutes

Cultural exchanges between nations have long been considered a positive and useful form of public diplomacy. But there is significant risk of such contacts being abused. That's the case with Chinese government supported Confucius Institutes. After years of abuses a bi-partisan consensus emerged that these institutes were a "Trojan Horse" for the CCP, representing little more than dens of subversion, communist propaganda and outright espionage.

In 2019, following years of warnings by professionals in the intelligence community and academia, Congress took steps in the National Defense Authorization Act for Fiscal Year 2019 to limit federal funding to colleges with Confucius Institutes. Then, in 2022, the U.S. Department of Defense subsequently funded a study by the National Academy of Sciences seeking to propose waiver criteria in order to enable DoD to continue providing funding to universities with Confucius Institutes. The willful effort by DoD to skirt Congress' intent in this way is disappointment but not necessarily surprising.

In 2019 Florida became the first to completely shutter all the Confucius Institutes at universities in the state. In the Lone Star State, Texas A&M and Prairie View A&M both shut down their Confucius Institutes, but these centers continue to operate at the University of Texas at Dallas and Texas Southern University. More states and universities should recognize this threat and follow suit.

Whole of Society Espionage

More than two years ago, FBI director Christopher Wray stated that the bureau was "to a point where the FBI is opening a new China-related counterintelligence case about every 10 hours." China has been described as waging a "whole of society" approach to espionage which involves weaponizing economic, academic and cultural aspects in order to achieve a massive penetration of the United States at all levels of government, federal, state, and local. Former secretary of State Mike Pompeo told attendees at the National Governors Convention in 2020 that China meticulously documents state leaders for their attitudes on China, labeling them "friendly", "ambiguous" or "hardline." The former Director of National Intelligence John Ratcliffe noted that China uses its economic influence within states to target Congressional leaders as well:

> "The intelligence chief warned of a scenario where Chinese-owned manufacturing facilities employing thousands of Americans could influence union chiefs to turn against lawmakers supporting disadvantageous policies — or risk losing their jobs.
>
> "The union leader contacts his congresswoman and indicates that his members won't support her re-election without a change in position. He tells himself he's protecting his members, but in that moment, he's doing China's bidding, and the congresswoman is being influenced by China, whether she realizes it or not," Ratcliffe wrote.
>
> "Our intelligence shows that Beijing regularly directs this type of influence operation in the U.S."

Yet in 2021, the Biden Administration shut down an interagency program targeting Chinese espionage over concerns the approach would be viewed as "racist."

States looking at ways to counter malign China's whole-of-society approach to espionage might take a page from Florida. In 2021, the sunshine state passed a law to toughen penalties against corporate espionage which benefit foreign entities. Another Florida law requires transparency of foreign funding of state universities and additional vetting of foreign applicants to research positions.

While generally viewed as a federal government responsibility, there is a historical precedent for states to develop intelligence and counterintelligence (CI) capabilities, according to Center expert Dr. J. Michael Waller:

> Some state and city police intelligence units have operated abroad and maintained liaisons with foreign intelligence, police, and security services for their own law enforcement purposes, usually due to ethnic, diaspora, or international criminal effects in their jurisdictions.
>
> Given their "counter" role for law enforcement and public safety, and their existing duties to conduct at least four of the five main duties outlined in the National Counterintelligence Strategy, many state and city police perform CI without even realizing it.
>
> The issue now is how to build

> awareness of a threat and a solution, and to do it in ways that ensure each participating state's particular interests while contributing to national security.

Ultimately, with China levying its "whole of society espionage" against the United States, it's going to take our entire society becoming aware of the China threat to effectively counter it. Given the fact that the federal government has shut down its own interagency China-focused anti-espionage program, it's time that state and local law enforcement networks work together to fill the gap.

Conclusion

As the Chinese spy balloon saga demonstrated in neatly allegorical terms, the federal government's approach to Chinese provocation can be characterized as "too little, too late." From penetration of the nation's electric grid to digital subversion occurring at the speed of algorithm, easily recognizable threats are allowed to slide, excused away unless a vast public outcry forces the federal bureaucracy to take some kind of action, which even then is undertaken with great reluctance.

Yet these excuses just won't fly with the American people.

Citizens are demanding more from their elected leaders to address the China threat. Given the lack of leadership and resolve at the federal level, governors and state legislators are increasingly being asked to step up and demonstrate an unprecedented level of initiative to address nationwide threats. While addressing the China threat on a state-by-state basis may seem unwieldly, the prospect of doing nothing is increasingly intolerable.

Therefore, the actions taken by state leaders to address the threats outlined in this report should be an inspiration to those recognizing the need for a "bottom-up" approach to address one of America's significant security challenges – Communist China.

Cover Image Photo By: ***Navy Petty Officer 1st Class Tyler Thompson***

This report was produced by the Center for Security Policy, a nonprofit, nonpartisan 501(c)(3) institution focusing on national security policy issues.

It was made possible by generous contributions from the Center for Security Policy's supporters. All views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).