Kansas House Committee on Financial Institutions and Pensions

Testimony of Brian Cavanaugh,
Former Senior Director, the National Security Council and
Senior Vice President, American Global Strategies, LLC

Proponent of HB 2739 – Countries of Concern Divestment and Procurement Protection Act

March 4, 2024

Good morning. Thank you, Chairman Hoheisel, Ranking Member Xu, and the Members of the Committee for allowing me to appear before you all today to support HB 2739, the Countries of Concern Divestment and Procurement Protection Act.

For the record, my name is Brian Cavanaugh, and I am a Senior Vice President for American Global Strategies, a consulting firm founded by former National Security Advisor Robert O'Brien and National Security Council Chief of Staff Alex Gray. Prior to joining American Global Strategies, I spent 12 years in the federal government, nine years with the Department of Homeland Security and three years at the White House on the National Security Council as Special Assistant to the President for National Security Affairs and Senior Director for Resilience.

Given the perilous state of global affairs, I would like to focus on providing the Committee with a sense of the global threat picture as it exists today and how more than ever, state governments are finding themselves on the front lines of strategic global competition.

Global Strategic Challenges

In their 2023 Annual Threat Assessment, the Office of the Director of National Intelligence stated that the United States and our allies are confronting a complex and pivotal international security environment dominated by two critical strategic challenges that intersect with each other and existing trends to intensify their national security implications. The fall of 2023 introduced a third critical strategic challenge, one that has only hyper escalated the international security environment in a lead up to the 2024 U.S. Presidential election.

First, powerful actors vie for global dominance and influence, notably the U.S., China, and Russia with ongoing strategic competition shaping the narrative, especially in light of Russia's ongoing actions in Ukraine and the rapid destabilization of the Middle East after Hamas' actions

on and since October 7th, 2023. Meanwhile, global challenges like health security, supply chain security, and economic issues post-COVID-19, along with evolving technologies, create unpredictable impacts on the global landscape.

Amidst the challenges in Europe and the Middle East, what should be most alarming is the quiet and not so subtle behavior and messaging coming out of China. China has the capability to directly attempt to alter the rules-based global order in every realm and across multiple regions, as a near-peer competitor that is increasingly pushing to change global norms and potentially threatening its neighbors.

Previous conflicts of the modern era did not directly challenge or target domestic civilian infrastructure, it was not a widely adopted planning assumption to disrupt and sow discord among the civilian population to gain a tactical advantage or, even more worrisome, erode a nation from within. However, U.S. intelligence agencies and military planners now accept that the tactics of our adversaries have shifted in favor of asymmetric tactics and planning assumptions. This change in adversarial behavior can be attributed to several factors including:

- A digital era in which 1) cyber-means enabled attacks against infrastructure and 2) social engineering and other malign influence operations targeting the civilian populace can disrupt a nation's society and its ability to project force.
- Globally interconnected economies which when manipulated can stoke fear or animosity within the United States populace, including towards the government or one another, and foment an unwillingness to engage in international affairs.

The shift in tactics and the evolving nature of threats in emerging technology, have placed state governments, local governments, and essentially our citizens in the crosshairs. Herein lies a fundamental challenge, it blurs the lines in terms of roles and responsibilities between the federal government and state governments. The Constitution makes it clear, powers not granted to the Federal government are reserved for States and the people, which are divided between State and local governments. Confronting and countering much of our nation's threats do fall on the shoulders of the federal government; however, as threats evolve and target domestic assets, state governments are uniquely positioned to act. It is critical that these actions ensure a greater level of resilience and security for a state's communities and economy.

China

Before I would like to make very clear that my comments in this testimony are not about the Chinese people or Chinese Americans, many of whom contribute much to this country and are often the victims of Chinese Communist Party aggression themselves. Rather, my comments about the threat posed by China refer to the government of China, led by the CCP.

Just last week, FBI Director Christopher Wray stated, “The CCP’s dangerous actions—China’s multi-pronged assault on our national and economic security—make it the defining threat of our generation.” Since I am all too often confronted with public leaders who still misinterpret China as a neutral nation simply engaged in economic competition, I must reiterate: China is not an ally. In fact, the U.S. government has labeled them an enemy, codified in Federal regulation – 15 Code of Federal Regulations Section 7.4.

The tension between the U.S. and China is manifesting itself in myriad of ways, across a wide spectrum of issues. We continue to witness what FBI Director Christopher Wray cited as the largest transfer of wealth via intellectual property theft by the CCP. This is done thru several methods such as cyber-espionage, human intelligence collection, programs such as China’s Thousand Talents Plan, which aims to expatriate scientists and foreign researchers to relocate to China, and lawfare.

China presents a significant threat to U.S. critical infrastructure through a combination of cyber capabilities, economic leverage, and geopolitical influence. The Chinese government has been accused of engaging in cyber espionage and cyberattacks targeting key sectors such as energy, telecommunications, and finance. These attacks, often sophisticated and persistent, like the recently disclosed Volt Typhoon, aim to steal sensitive information, compromise systems, and potentially disrupt essential services.

Moreover, China's economic ties with the United States provide a platform for potential leverage, allowing Beijing to exert pressure on U.S. businesses and infrastructure projects. The strategic competition between the two nations amplifies the risk of adversarial actions that could impact critical infrastructure. Advancements in technology borne out of American innovation are spurring a digital transformation in communications and bringing about the internet of things, yet the utilization of state-owned enterprises and heavy subsidization of products manufactured in China are undercutting Western products and introduce vulnerabilities into U.S. infrastructure.

There are several examples of the U.S. receiving inferior products or receiving products that were capable of sharing surveillance data with the People’s Liberation Army (PLA). Specifically, one could look at bulk power transformers, communications equipment (Huawei), semiconductors (SMIC), and drones. To understand how including these Chinese products in critical infrastructure creates vulnerability, you do not have to look beyond China’s own cyber regulation and law. Their cybersecurity laws require network operators to store select data within China, allows Chinese authorities to conduct spot-checks on a company's network operations, and requires any software used in China provide source code to the CCP. Essentially, the CCP has established a conduit for not just open-source data collection, but the collection of all data passing through Chinese software and hardware.

China is our most capable cyber adversary, employing various cyber means to target U.S. infrastructure, utilizing advanced tactics and techniques. One common method is through cyber espionage, where Chinese state-sponsored hackers infiltrate networks to steal sensitive information related to critical infrastructure systems. These attacks often involve the use of sophisticated malware, phishing campaigns, and zero-day exploits to gain unauthorized access. The goal may be to gather intelligence on the design, operation, and vulnerabilities of U.S. infrastructure, enabling potential future disruptions or exploitation.

China has emerged as a pivotal player in the fentanyl epidemic facing the United States. The illicit production and distribution of fentanyl, a potent synthetic opioid responsible for a significant portion of opioid-related deaths in the U.S. In 2023 the overdose death rate topped 112,000 in a 12-month period for the first time, according to the Centers for Disease Control and Prevention. This is up from 65,000 deaths in 2020. Fentanyl has been linked to the vast majority of these overdose deaths and the source of fentanyl have been linked to clandestine laboratories in China. The connection between China, an open border, and the fentanyl epidemic underscores the intricate challenges facing our nation and in need of real solutions.

Finally, the CCP has spent a tremendous amount of energy, time, and money to establish levers within U.S. society to manage perception and control critical voices. From establishing a secret physical presence in the U.S. through its repressive security apparatus to monitor and intimidate dissidents and those critical of its government to leveraging (wittingly or unwittingly) athletes, members of Hollywood, and other public officials to shape and manage the perception of the PRC.

Russia

Russia poses significant threats to U.S. critical infrastructure, employing a range of cyber capabilities to target key sectors such as energy, finance, and transportation. The Kremlin has demonstrated a willingness to engage in sophisticated cyber-attacks, utilizing advanced hacking techniques to infiltrate computer networks and potentially disrupt essential services. One such example can be linked to the Colonial Pipeline disruption two years ago. Instances of ransomware attacks, attributed to Russian cybercriminals if not directly linked to state-sponsored entities, have highlighted vulnerabilities in the U.S. critical infrastructure, leading to concerns about the nation's ability to protect against and respond to these cyber threats effectively. The constant evolution of Russia's cyber capabilities underscores the need for robust cybersecurity measures to safeguard the integrity and functionality of critical infrastructure assets.

Additionally, Russia's interference extends beyond cyber threats to include efforts aimed at influencing U.S. state governments. Through disinformation campaigns, propaganda, and

attempts to sow discord, Russia seeks to exploit existing political and social divisions within the United States. These tactics aim to undermine public trust in democratic institutions and create internal strife, potentially affecting state-level governance. By fostering polarization and exacerbating existing tensions, Russia aims to weaken the fabric of U.S. society and reduce the country's overall resilience against external manipulation. Recognizing and addressing these multifaceted threats is crucial to bolstering the security and stability of both U.S. critical infrastructure and state governments.

Iran

Iran also poses potential threats to U.S. critical infrastructure through a combination of cyber capabilities and geopolitical tensions that may spur terrorist acts here in the U.S. Iranian state-sponsored hacking groups, such as APT33 and APT34, have been linked to cyber activities targeting critical sectors like energy, telecommunications, and financial services. These cyber threats often involve tactics such as spear-phishing, malware deployment, and data exfiltration, with the aim of compromising key infrastructure systems. Iran's motives may include gathering intelligence, causing disruptions, or establishing a foothold for potential future attacks. The ongoing geopolitical tensions between the two nations further amplify the risk, emphasizing the need for robust cybersecurity measures to protect against potential Iranian cyber threats to U.S. critical infrastructure.

In addition to cyber threats, Iran's influence extends to attempts to manipulate and interfere with U.S. state governments. This may involve disinformation campaigns, spreading propaganda, or attempting to exploit existing political and social divisions within specific states. Iran's geopolitical agenda and perceived grievances against the U.S. could lead to efforts to undermine state-level governance and create internal discord. The horrific attack by Hamas, an Iranian proxy, on Israel and the ensuing global unrest that has sparked disruptive and violent protests have the potential to ultimately lead to targeted attacks on infrastructure or even more violence. Vigilance in monitoring and addressing these multifaceted threats, both in the digital realm and in the socio-political sphere, is crucial to safeguarding U.S. critical infrastructure and maintaining the stability of state governments.

State Level Action

Circling back to how these complex challenges can be addressed and who is empowered to do so, I believe states are positioned to be agile in addressing the issues and have the ability to wield powerful tools to do so. Initial steps to address these threats at a state level include:

- Prohibit state and local pension funds, university endowments, and other investments from being invested in assets domiciled in or controlled by countries determined to be adversaries of the United States.
- Prohibit procurements by state agencies from countries of concern.

Again, thank you for convening this important hearing. Undoubtedly, the topics you are addressing today will merit thought provoking questions, including how do we as a nation stay informed of the threats and what does mitigation look like? With that in mind, I look forward to a healthy conversation and stand ready to assist you and your staff as you debate policy solutions to the issues impacting Kansas and our nation like those found in HB 2739.