CONFRONTING THREATS FROM THE CCP TO THE HOMELAND

HEARING

BEFORE THE

SUBCOMMITTEE ON COUNTERTERRORISM, LAW ENFORCEMENT, AND INTELLIGENCE

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

MARCH 9, 2023

Serial No. 118–2

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
51–888 PDF WASHINGTON : 2023

COMMITTEE ON HOMELAND SECURITY

MARK E. GREEN, MD, Tennessee, *Chairman*

MICHAEL T. MCCAUL, Texas
CLAY HIGGINS, Louisiana
MICHAEL GUEST, Mississippi
DAN BISHOP, North Carolina
CARLOS A. GIMENEZ, Florida
AUGUST PFLUGER, Texas
ANDREW R. GARBARINO, New York
MARJORIE TAYLOR GREENE, Georgia
TONY GONZALES, Texas
NICK LALOTA, New York
MIKE EZELL, Mississippi
ANTHONY D'ESPOSITO, New York
LAUREL M. LEE, Florida
MORGAN LUTTRELL, Texas
DALE W. STRONG, Alabama
JOSH BRECHEEN, Oklahoma
ELIJAH CRANE, Arizona

BENNIE G. THOMPSON, MISSISSIPPI, RANKING MEMBER
SHEILA JACKSON LEE, Texas
DONALD M. PAYNE, JR., New Jersey
ERIC SWALWELL, California
J. LUIS CORREA, California
TROY A. CARTER, Louisiana
SHRI THANEDAR, Michigan
SETH MAGAZINER, Rhode Island
GLENN IVEY, Maryland
DANIEL S. GOLDMAN, New York
ROBERT GARCIA, California
DELIA C. RAMIREZ, Illinois
ROBERT MENENDEZ, New Jersey
YVETTE D. CLARKE, New York
DINA TITUS, Nevada

STEPHEN SIAO, *Staff Director*
HOPE GOINS, *Minority Staff Director*
NATALIE NIXON, *Chief Clerk*
SEAN JONES, *Legislative Clerk*

SUBCOMMITTEE ON COUNTERTERRORISM, LAW ENFORCEMENT, AND INTELLIGENCE

AUGUST PFLUGER, Texas, *Chairman*

DAN BISHOP, North Carolina
TONY GONZALES, Texas
ANTHONY D'ESPOSITO, New York
ELIJAH CRANE, Arizona
MARK E. GREEN, MD, Tennessee *(ex officio)*

SETH MAGAZINER, Rhode Island, *Ranking Member*
J. LUIS CORREA, California
DANIEL S. GOLDMAN, New York
DINA TITUS, Nevada
BENNIE G. THOMPSON, Mississippi *(ex officio)*

MICHAEL KOREN, *Subcommittee Staff Director*
BRITTANY CARR, *Minority Subcommittee Staff Director*
ALICE HAYES, *Subcommittee Clerk*

CONTENTS

CONFRONTING THREATS FROM THE CCP TO THE HOMELAND

Thursday, March 9, 2023

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON COUNTERTERRORISM,
LAW ENFORCEMENT, AND INTELLIGENCE,
Washington, DC.

The subcommittee met, pursuant to notice, at 9:01 a.m., in Room 310, Cannon House Office Building, Hon. August Pfluger [Chairman of the subcommittee] presiding.

Present: Representatives Pfluger, Gonzales, D'Esposito, Crane, Magaziner, Correa, Goldman, Titus, and Jackson Lee.

Chairman PFLUGER. The Committee on Homeland Security, Subcommittee on Counterterrorism, Law Enforcement, and Intelligence will come to order.

Good morning. The purpose of this hearing is to receive testimony from expert witnesses in the security realm that will educate our efforts to mitigate threats posed by the Chinese Communist Party to the U.S. homeland.

I now recognize myself for an opening statement.

Good morning. I would like to thank all of our witnesses for testifying today, bringing your expertise to this committee, and informing Members of Congress about the threats that we are currently facing. Despite years of attempts by the United States to develop a productive, fair, and honest relationship with the People's Republic of China, America has been met with dishonesty and aggression. The PRC government, run by the Chinese Communist Party, has deceived and manipulated us at every turn, committing espionage in our homeland and working to overturn the global rules-based order. United States is now locked in a peer competition with the CCP in which the Chinese government is seeking to place itself at the top of the global world order while degrading America's power militarily, diplomatically, and economically. In recent months, events have shown us that the CCP has escalated this competition.

On January 28, a Chinese surveillance balloon entered U.S. airspace and spent the next 8 days traveling over the majority of the continental United States. While we do not know yet what kind of information the Chinese surveillance balloon was able to collect, we can be certain that the CCP's intention was to exploit sensitive sites, including military sites and critical infrastructure across our country. This Chinese surveillance balloon was a brazen display of espionage in the U.S. homeland, but it is ultimately one of the many ways that the CCP is working to exploit our vulnerabilities.

Today we must take the conversation beyond that balloon and discuss all avenues the CCP is threatening U.S. homeland security in. Through the CCP's aggressive national strategy of Military-Civil Fusion, which aims to establish the People's Liberation Army as the dominant global military force by 2049, the Chinese government is stealing information from U.S. military and civilian targets. A majority of the threats China poses to the U.S. homeland security are occurring below the threshold of traditional conflict. We need to be cognizant of these threats and generate multi-faceted solutions to deter them.

These threats are already directly affecting American citizens. MD Anderson Cancer Center, for instance, one of the Nation's top hospitals for cancer in my home State of Texas, ousted several scientists from the center in 2019 who had ties to the CCP. The scientists were flagged by the U.S. National Institutes of Health regarding a variety of threats, including data security, intellectual property loss, and they were ultimately investigated by the FBI. This incident was by no means unique, with the CCP consistently targeting American research and innovation across the country.

Additionally, the CCP is exploiting the open nature of American academia to steal vital research and development. Confucius Institutes, marketed as mechanisms to promote Chinese language and culture, have used the CCP to recruit American talent to support Military-Civil Fusion, monitor Chinese nationals who are studying at American universities, and have faced allegations of visa fraud.

In recent years the U.S. Government has worked to close most of these Confucius Institutes, however, the CCP has made efforts to change the Institutes' names or obfuscate their influence on American universities. Today, as a matter of fact, I am reintroducing with Chairman Green and Congressman Brad Wenstrup the DHS restrictions on Confucius Institutes and Chinese Entities of Concern Act, which passed out of this committee with bipartisan support last Congress. This bill works to close Confucius Institutes and any other programs with the same goal operating in the United States. It also holds American universities accountable and ensures they prioritize their students' education and right to free speech, above partnerships with Confucius Institutes that require universities to censor curriculums in favor of CCP ideology.

I appreciate the support of Chairman Green, Congressman Wenstrup, and look forward to a bipartisan discussion on this.

In addition to threats to American IP and academic freedom, the CCP is targeting U.S. cybersecurity and critical infrastructure and undermining our economic security. Moreover, illicit fentanyl, fentanyl analogs, and related precursor chemicals are predominantly sourced from the PRC and then sent to Mexico. These poisonous drugs continue to fuel the tragic fentanyl crisis in our homeland. I am eager to discuss these challenges and more during today's hearing.

Let me be clear about this hearing to anyone who is listening at home or abroad. This conflict and the discussion today doesn't have anything to do with the Chinese people who are living in China and being manipulated by the CCP. This conflict is with the CCP. It is an authoritarian regime that commits genocide against its own people, they censor free speech, not just in China, but across

the globe, and they aim to end democracy as we know it. This hearing is the first of many, but it is a first step on this subcommittee and the greater Committee on Homeland Security, which we intend to confront the threats stemming from CCP influence that target our homeland. We will meet CCP aggression with strength, its deception with unflinching truth, and its attempts at exploitation with justice.

We look forward to a bipartisan cooperation in this Congress as we all seek effective solutions to combat pervasive threats posed by the CCP to our homeland security.

I now recognize the Ranking Member, my friend from Rhode Island, Mr. Magaziner, for his opening statement.

[The statement of Chairman Pfluger follows:]

STATEMENT OF CHAIRMAN AUGUST PFLUGER

MARCH 9, 2023

Good morning, and welcome to the Subcommittee on Counterterrorism, Law Enforcement, and Intelligence's first hearing of the 118th Congress. I would like to thank all our witnesses for testifying today and welcome the Ranking Member and other Members of the subcommittee.

Despite years of attempts by the United States to develop a productive, fair, and honest relationship with the People's Republic of China, America has been met with dishonesty and aggression.

The PRC government, run by the Chinese Communist Party (CCP), has deceived and manipulated us at every turn, committing espionage in our homeland and working to overturn the global rules-based order. The United States is now locked in a peer competition with the CCP in which the Chinese government is seeking to place itself at the top of the global world order while degrading America's power militarily, diplomatically, and economically. In recent months, the CCP has escalated this competition.

On January 28th, a Chinese surveillance balloon entered U.S. airspace and spent the next 8 days traveling over the majority of the continental United States.

While we do not know what kind of information the Chinese surveillance balloon was able to collect, we can be certain that the CCP's intention was to exploit sensitive U.S. military sites and critical infrastructure across the country. This Chinese surveillance balloon was a brazen display of espionage in the U.S. homeland, but it is ultimately one of many ways the CCP is working to exploit our vulnerabilities. Today, we must take the conversation beyond the balloon and discuss all the avenues the CCP is threatening U.S. homeland security.

Through the CCP's aggressive national strategy of Military-Civil Fusion, which aims to establish the People's Liberation Army (PLA) as the dominant global military force by 2049, the Chinese government is stealing information from U.S. military and civilian targets. A majority of the threats China poses to U.S. homeland security are occurring below the threshold of traditional conflict. We need to be cognizant of these threats and generate multifaceted solutions to deter them.

These threats are already directly affecting American citizens.

MD Anderson Cancer Center, one of the Nation's top hospitals for cancer care in my home State of Texas, ousted several scientists from the center in 2019 who had ties to China. The scientists were flagged by the U.S. National Institutes of Health regarding a variety of threats, including data security and intellectual property loss, and they were ultimately investigated by the Federal Bureau of Investigation (FBI). This incident was by no means unique, with the CCP consistently targeting American research and innovation across the country.

Additionally, the CCP is exploiting the open nature of American academia to steal vital research and development. Confucius Institutes, marketed as mechanisms to promote Chinese language and culture, have been used by the CCP to recruit American talent to support Military-Civil Fusion, monitor Chinese nationals studying at American universities, and have faced allegations of visa fraud. In recent years, the U.S. Government has worked to close most of these Confucius Institutes; however, the CCP has made efforts to change the Institutes' names or obfuscate their influence on American universities.

Today, I am reintroducing with Chairman Green and Congressman Wenstrup the "DHS Restrictions on Confucius Institutes and Chinese Entities of Concern Act,"

which passed out of this committee with bipartisan support last Congress. This bill works to close Confucius Institutes, and any other programs with the same goal, operating in the United States. It also holds American universities accountable and ensures they prioritize their students' educations and right to free speech above partnerships with Confucius Institutes that require universities to censor curriculums in favor of CCP ideology.

I appreciate the support from Chairman Green and Congressman Wenstrup and look forward to working with the two of them to advance this bill.

In addition to threats to American IP and academic freedom, the CCP is targeting U.S. cybersecurity and critical infrastructure and undermining our economic security. Moreover, illicit fentanyl, fentanyl analogues, and related precursor chemicals are predominately sourced from the PRC and Mexico. These poisonous drugs continue to fuel the tragic fentanyl crisis in our homeland. I am eager to discuss these challenges and much more during today's hearing.

Let me be clear to anyone who is listening at home or abroad: This conflict is not with individual citizens of the PRC—this conflict is with the CCP, an authoritarian regime that commits genocide against its own people, censors free speech across the globe, and aims to end democracy as we know it.

This hearing is the first step of many this subcommittee and the greater Committee on Homeland Security intend to take to confront the threats stemming from the CCP that target our homeland security.

We will meet CCP aggression with strength, its deception with unflinching truth, and its attempts at exploitation with justice. We look forward to bipartisan cooperation this Congress as we all seek effective solutions to combat the pervasive threats posed by the CCP to U.S. homeland security.

Mr. MAGAZINER. Good morning. I want to thank Chairman Pfluger for calling this important hearing and thank our witnesses for coming today. I especially want to thank Dr. Tyler Jost from Brown University in Rhode Island for joining us, along with our other expert witnesses.

It is an honor to serve as Ranking Member of this subcommittee, and I look forward to working with you, Mr. Chairman, and all Members of the subcommittee on a bipartisan basis to protect Americans from those who seek to threaten the security of the homeland.

Make no mistake, China is the competitor with the greatest combination of intent and capacity to threaten U.S. global leadership. President Xi himself stated last year that by 2049 he wants to ensure that China and the CCP lead the world in terms of composite national strength and international influence. This is concerning for all of us who believe deeply that democracy and human rights must be advanced and protected here in our own country and across the world. Just last year, FBI Director Christopher Wray sat before this committee in this very room and warned that the greatest long-term threat to our Nation's information and intellectual property and our economic vitality is the counterintelligence and economic espionage threat from China. Commerce Secretary Gina Raimondo has warned that the Chinese Communist Party is accelerating their efforts to fuse economic and technology policies with their military ambitions in ways that are forcing us, compelling us to defend United States businesses and workers.

We have already seen the Chinese Communist Party threaten the safety and privacy of American citizens through economic espionage and theft of U.S. intellectual property, the theft of personal data of American citizens through cyber attacks, the recent use of a spy balloon and other methods of surveillance to illegally gather intelligence on American territory, and the build-up of military capabilities that seek to eclipse the United States and our democratic allies. We must recognize that threat posed by the CCP and take

immediate action to best position the United States to confront China's attempts to undermine our national security.

Today's hearing is an important opportunity for Members of this subcommittee to demonstrate that we are united in a bipartisan effort to defend the privacy and safety of the American people, to protect U.S. industries and supply chains, and enhance national security, all while remembering that one of the most important ways to counter the Chinese Communist Party's ambitions is to build an economy here at home that works for working people, so we can show the world that our American system of democracy and freedom is more effective in lifting people up than the CCP model of autocracy and repression.

Democrats are committed to doing this work with our Republican colleagues in a spirit of collaboration. Last year, thanks to the leadership of President Biden, Congress passed the Bipartisan CHIPS Act to invest $280,000,000,000 into domestic semiconductor production that will enhance our national security, strengthen U.S. industry, create jobs, reduce inflation, and improve our competitiveness with China. The CIA has recently launched a dedicated China Mission Center and the State Department has launched a new Office of China Coordination in order to strengthen the U.S. diplomatic, military, and intelligence capabilities in meeting CCP threats. It is my hope that today's hearing will further illuminate the CCP's strategies to undermine our democracy, our economy, and way of life, and how Congress can work together to meet these challenges.

As we do this work together, we must remember that the people of China and people of Chinese origin experience oppression and human rights violations at the hands of the authoritarian Chinese Communist Party, and anti-Asian harassment and discrimination is too prevalent globally and here at home. So I also want to be abundantly clear that we do not condone any anti-Chinese or anti-Asian bigotry, and we must condemn any acts of anti-Asian discrimination in the strongest possible terms. Our struggle is not with the Chinese people, but rather with the Chinese Communist Party that is increasingly hostile to democracy and human rights. The CCP wants nothing more than to see Americans become divided and prejudiced, but they will be disappointed. Instead, we will out-compete the CCP by ensuring that America remains a beacon of freedom to the world and by continuing to provide safe harbor to those fleeing oppression and violence. That is how we will strengthen our Nation and our economy.

I look forward to hearing from today's witnesses, and I yield back.

[The statement of Ranking Member Magaziner follows:]

STATEMENT OF RANKING MEMBER SETH MAGAZINER

MARCH 9, 2023

Make no mistake, China is the competitor with the greatest combination of intent and capacity to threaten U.S. global leadership. President Xi himself stated last year, that by 2049 he wants to ensure China and the CCP "lead the world in terms of composite national strength and international influence." This is concerning for all of us who believe deeply that democracy and human rights must be advanced and protected here in our own country and across the world.

Just last year, FBI Director Christopher Wray sat before this committee, in this very room, and warned that "[t]he greatest long-term threat to our Nation's infor-

mation and intellectual property, and to our economic vitality, is the counterintelligence and economic espionage threat from China."

Director Wray is not alone in his assessment. Commerce Secretary Gina Raimondo has warned that the Chinese Communist Party is "accelerating their efforts to fuse economic and technology policies with their military ambitions . . . in ways that are forcing us, compelling us, to defend United States businesses and workers."

We have already seen the Chinese Communist Party threaten the safety and privacy of American citizens through:

- economic espionage and theft of U.S. intellectual property
- the theft of personal data of American citizens through cyber attacks
- the recent use of a spy balloon and other methods of surveillance to illegally gather intelligence on American territory, and
- the build-up of military capabilities that seek to eclipse the United States and our democratic allies.

We must recognize the threat posed by the CCP and take immediate action to best-position the United States to confront China's attempts to undermine our National security.

Today's hearing is an opportunity for Members of this subcommittee to demonstrate that we are united in a bipartisan effort to defend the privacy and safety of the American people, to protect U.S. industries and supply chains, and enhance National security—all the while remembering that one of the most important ways to counter the Chinese Communist Party's ambitions is to build an economy here at home that works for working people so we can show the world that our American system of democracy and freedom is more effective in lifting people up than the CCP model of autocracy and repression.

Democrats are committed to doing this work with our Republican colleagues in a spirit of collaboration.

Last year, thanks to the leadership of President Biden, Congress passed the bipartisan CHIPS Act, to invest $280 billion into domestic semiconductor production that will enhance our national security, strengthen U.S. industry, create jobs, reduce inflation, and improve our competitiveness with China.

Under President Biden, the CIA has launched a dedicated China Mission Center and the State Department has launched a new Office of China Coordination, in order to strengthen the U.S. diplomatic, military, and intelligence capabilities in meeting CCP threats.

It is my hope that today's hearing will further illuminate the CCP's strategies to undermine our democracy, our economy, and way of life—and how Congress can work together to meet these challenges.

As we do this work together we must remember that the people of China and people of Chinese origin experience oppression and human rights violations at the hands of the authoritarian Chinese Communist Party, and anti-Asian harassment and discrimination is too prevalent globally and here at home.

I want to be abundantly clear that we do not condone any anti-Chinese or anti-Asian bigotry, and we must condemn any acts of anti-Asian discrimination in the strongest possible terms. Our struggle is not with the Chinese people, but rather with the Chinese Communist Party that is increasingly hostile to democracy and human rights.

The Chinese Communist Party wants nothing more than to see Americans become divided and prejudiced. But they will be disappointed. Instead, we will out-compete the CCP by ensuring that America remains a beacon of freedom to the world and by continuing to provide safe harbor to those fleeing oppression and violence. That is how we will strengthen our Nation and our economy. Let us not forget that.

Division and rancor is the goal of the CCP. We must stand together and work in a bipartisan fashion to show that we stand united and prepared in the face of their efforts to weaken our Nation.

Chairman PFLUGER. Thank you, Ranking Member.

Other Members of the committee are reminded that opening statements may be submitted for the record.

[The statement of Honorable Goldman follows:]

STATEMENT OF HONORABLE DAN GOLDMAN

Thank you to our witnesses for being here. I represent New York's 10th Congressional District, home to Chinatown communities in Manhattan and Brooklyn—some of the most historic and vibrant Asian communities in this country.

The Chinese Communist Party and China's government pose legitimate threats to the United States that must be taken seriously. We cannot allow the CCP to invade our sovereignty with spy balloons, influence our elections, or threaten democracies around the world.

At the same time, we must not forget that Asian Americans and immigrants who live in our communities are suffering because of the CCP. They suffer because the authoritarian regime in China has surveilled their communities here in the United States. They suffer because they have families in China whose lives may be at risk simply because they have families in America. And they suffer from hate crimes here in the United States that are fueled, in part, by disgusting political rhetoric.

Today's hearing is an opportunity for Members to show that we are united in a bipartisan effort to strengthen the United States in our global strategic competition with the Chinese government and the Chinese Communist Party—not with Chinese people or Asian Americans.

At a time when Anti-Asian hate crimes in the United States are up by 339 percent year over year from 2020 to 2021, and anti-Asian hate crimes jumped from 30 to 133 in New York City alone,[1] it is imperative that Members of Congress and political leaders do not allow our legitimate critiques of the CCP and China's government to veer into anti-Asian stereotyping and prejudice that fuels hateful violence.

Like when Republicans repeatedly called COVID–19 the "China virus" or "kung flu", or when a Republican Member of Congress recently questioned the loyalty of the first Chinese American Congresswoman to score cheap political points.

I was elected to Congress to serve my constituents and to stand up for their safety and security. The best way to counter the Chinese Communist Party's ambitions is to safeguard our values, our elections, our sovereignty, and our diversity. As Ranking Member Magaziner said, the CCP would like nothing more than to see the United States festering with anti-Asian prejudice.

Chairman PFLUGER. I am pleased to have a distinguished panel of witnesses before us today on this very important topic, and I ask that our witnesses please rise and raise their right hand.

[Witnesses sworn.]

Chairman PFLUGER. Let the record reflect that the witnesses have answered in the affirmative. Thank you.

I would like to now formally introduce our witnesses.

The Honorable William Evanina dedicated his life for 32 years to government service. In May 2020, the Senate confirmed him as the very first director of National Counterintelligence and Security Center. In this position Mr. Evanina was the head of counterintelligence for the entirety of the U.S. Government. His background in counterintelligence lends itself well today to our specific discussion, which will focus heavily on the ways of CCP espionage efforts and how they impact our homeland, including the theft of U.S. IP, the exploitation of academic research, and much more.

Lieutenant General Joseph T. Guastella joins us from the Mitchell Institute, also a friend of mine in a former life as a fighter pilot, and he is a senior fellow at the Mitchell Institute for Aerospace Studies. Lieutenant General Guastella is a command pilot who most recently served as deputy chief of staff of operations at U.S. Air Force headquarters. It was his job to oversee air power capabilities, including the homeland defense mission of North American aerospace defense, or NORAD and NORTHCOM.

With the foundation of his impressive background, Lieutenant General Guastella will be able to speak to America's evolving homeland security needs as it faces a challenge never seen before by the CCP. Given the recent shocking events, which I think were a wake-up call of the surveillance balloon, we are grateful for your service, General, and for being here today.

---

[1] *https://www.nbcnews.com/news/asian-america/anti-asian-hate-crimes-increased-339-percent-nationwide-last-year-repo-rcna14282*.

The Honorable Kari Bingen joins us from the Center for Strategic and International Studies, or CSIS, where she is the director of Aerospace Security Project. Prior to this, she served as deputy under secretary of defense for intelligence and security. Her strong background in homeland security and defense policies will be an exceptional addition as we discuss the growing and changing threat landscape, including threats to American critical infrastructure as it pertains to the U.S. peer competition with China.

I now would like to once again recognize the Ranking Member, gentleman from Rhode Island, Mr. Magaziner, for a brief introduction of the next witness.

Mr. MAGAZINER. Thank you, Chairman.

I am pleased to welcome our fourth witness, Dr. Tyler Jost. Dr. Jost is an assistant professor of political science and international and public affairs at Brown University in the great State of Rhode Island. He is also the Watson Institute assistant professor of China studies and devotes his time and effort to improving our understanding of national security decision making in the People's Republic of China. Professor Jost also previously served as a military intelligence officer with assignments in Afghanistan, U.S. Cyber Command, and the Office of the Secretary of Defense.

Thank you to all of our witnesses for being here today, and I yield back.

Chairman PFLUGER. Thank you very much. Again, thank you to all the witnesses for taking time here.

I now recognize the Honorable William Evanina for an opening statement. We do have a timer and we will keep them 5 minutes.

You are recognized.

STATEMENT OF WILLIAM R. EVANINA, FOUNDER AND CEO, THE EVANINA GROUP

Mr. EVANINA. Chairman Pfluger, Ranking Member Magaziner, Members of the subcommittee, it is an honor to be here with you today to discuss this really important topic.

I spent 32 years of my career working for the U.S. Government in the FBI, the CIA, as the Chairman referenced, as the first Senate-confirmed director of the National Counterintelligence and Security Center. But I am here before you today as the CEO of the Evanina Group, where I provide consulting services to boards of directors, CEOs, and executives on this exact threat we discussed today.

Today's topic, China and the threat to the homeland, is an existential threat. It is the most complex, pernicious, aggressive strategic threat our Nation has ever faced. I proffer to this subcommittee that the U.S. private sector and academia have become the geopolitical battlespace for China. Xi Jinping has one goal to be the geopolitical, military, and economic leader of the world, period. Along with the Ministry of State Security, the People's Liberation Army, the United Front Work Department, they drive a comprehensive whole-of-country approach to their efforts to invest, leverage, infiltrate, influence, and steal from every corner of the United States. This is a generational battle for Xi, and it drives through every decision. We must approach this threat from the Communist Party of China with the same sense of urgency, spend-

ing, and strategy we have done for the past two decades to combat terrorism.

I would offer to the subcommittee that we are in a terrorism event. A slow, methodical, strategic, persistent, and enduring event, which requires in response, a degree of urgency of action. Let me be more specific. The Communist Party of China's capabilities and intent are second-to-none as an adversary. The cyber breaches, insider threats, surveillance, and penetrations into our critical infrastructure, of which 85 percent is owned by the private sector, have all been widely reported. There is much more in the classified realm, but we have become numb to it as a Nation. Additionally, it is estimated that 80 percent of American adults have had all of their private data stolen by the Communist Party of China. The other 20 percent, just most of it.

Layering in the Communist Party of China's crippling stranglehold on many aspects of our supply chain, and what results is a daunting vulnerability and susceptibility of unacceptable proportions. When we layer in the current threat landscape, sophisticated surveillance balloons, maritime port surveillance, strategic land purchases by military bases, terrestrial and space-based 5G threats, U.S.-based Chinese police stations, Huawei and TikTok, the collage begins to paint a very bleak mosaic. From a cybersecurity perspective, China possesses persistent and unending resources to penetrate our systems and exfiltrate our data, or sit dormant and wait, or plant malware on critical infrastructure for future hostilities. At the same time, the insider threat epidemic originating from the Communist Party of China has been nothing short of devastating to the U.S. corporate world. Additionally, the Communist Party of China strategically conducts malign influence campaigns at the State and local level with precision. This effort must be exposed and mitigated.

So why does it all matter? Economic security is national security. Our economic global supremacy, stability, and long-term vitality is at risk and squarely in the cross hairs of Xi Jinping and the Communist regime.

In 2020 the estimated economic loss from theft of intellectual property and trade secrets just from the Communist Party of China, just from what we know in prosecutions, is between $300 billion and $500 billion per year. That equates to about $4,000 to $6,000 per year for American family of four after taxes. The cost is real.

So how do we mitigate these threats? We must create a robust public-private partnership with real intelligence sharing, while at the same time staying true to our core values, morals, and rule of law, which made America the greatest country the world has ever seen. This will take a whole-Nation approach. It will take time. Such approach must start with contextual awareness campaigns reaching a broad audience from every level of government to chambers of commerce to university campuses and from the board rooms to the business schools. Because the why matters. U.S. boards of directors and investment leaders must begin to look beyond the next fiscal quarter earnings and begin to think strategically about how their investment decisions and awareness of the long-term

threat can impact not only their business model, but the economic and national interest to the United States.

In conclusion, I investigated terror attacks after September 11 and led counterintelligence programs for the FBI. I would suggest the threat posed by China is much more dangerous to the longevity and sustainability of our Nation than any terrorist threat actor.

Thank you. I look forward to your questions.

[The prepared statement of Mr. Evanina follows:]

PREPARED STATEMENT OF WILLIAM R. EVANINA

MARCH 9, 2023

Chairman Pfluger, Ranking Member Magaziner, and Members of the subcommittee—it's an honor to appear before you today. I have spent 32 years of my adulthood working the U.S. Government. Twenty-four of which with the FBI, CIA, and NCSC.

I was tremendously honored to be the first Senate-confirmed director of the National Counterintelligence and Security Center (NCSC) in May 2020.

I am here before you today as the CEO of The Evanina Group, LLC. In this role, I work closely with CEOs, boards of directors, and academic institutions to provide a strategic approach to mitigating risk in a complicated global environment.

THE CHINA THREAT

Our Nation faces a diverse, complex, and unprecedented sophisticated threats by nation-state actors, cyber criminals, and terrorist organizations.

However, the existential threat our Nation is from the Communist Party of China (CCP). This threat is the most complex, pernicious, strategic, and aggressive our Nation has ever faced. It is an existential threat.

We must first clearly understand this threat. We must also continue to mitigate this threat with a whole-of-society approach. We must also approach this comprehensive and holistic threat with the same sense of urgency, spending, and strategy . . . As we have done for the past two decades in preventing terrorism.

I would offer to this subcommittee that we ARE in a terrorism event. A slow, methodical, strategic, persistent, and enduring event which requires a degree of urgency of action. It is clear that under Xi Jinping, the CCP's economic war with the United States is manifested itself into a terrorism framework.

Let me be more specific. The CCP's capabilities and intent are second-to-none as an adversary. The cyber breaches, insider threats, surveillance and penetrations into our critical infrastructure have all been widely reported and we have become numb to these episodes, as a Nation. Add in the CCP's crippling stranglehold so many aspects of our supply chain and what results is an imbalance and vulnerability of unacceptable proportions. When we move to new areas of the CCP to include surveillance balloons, ZPMC cranes at out maritime ports, Huawei, and TikTok, the collage begins to paint a bleak mosaic.

I would ask the subcommittee is it not terrorism when a hospital, high school, police department, college, county services, or water treatment facility are shut down by a cyber breach or ransomware event? How about a natural gas pipeline that is shut off via a malware or virus? How about our electrical grid or natural gas being shut off in the winter in the Northeast part of the United States resulting in millions of households, and buildings, without heat? How about our telecommunications infrastructure going down 1 day because Verizon and AT&T are hit with a cyber attack on the same day? Or, our financial services sector having to go off-line, for even a few hours, would cause significant international chaos and disruption. Are these not terror events? "Terror" must be redefined beyond our framework which includes loved ones dying from a kinetic event.

It is easy to parlay all the "would be" and "could be" scenarios as fear-based paranoia. However, intelligence and law enforcement professionals, cyber professionals and international organizations have all seen the intent, capabilities deployed by the CCP. The inability or unwillingness to look behind the curtain and visualize this existential threat is no longer an option for anyone. There is no more curtain to look behind.

WHERE IS THE THREAT?

The U.S. private sector, academia, research and development entities, and our core fabric of ideation has become the geopolitical battlespace for China.

Xi Jinping has one goal. To be the geopolitical, military, and economic leader in the world. Xi, along with the China's Ministry of State Security, People's Liberation Army, and the United Front Work Department, drive a comprehensive and whole of country approach to their efforts to invest, leverage, infiltrate, influence and steal from every corner of U.S. success.

Economic security is national security. Our economic global supremacy, stability, and long-term vitality is not only at risk, but squarely in the cross hairs of Xi Jinping and the communist regime. This is a generational battle for Xi and the CCP, it drives their every decision, particularly geopolitically. How to counter and push past the United States is goal No. 1 for Xi and the CCP.

HOW DOES THE THREAT MANIFEST?

Intelligence services, science & technology investments, academic collaboration, research partnerships, joint ventures, front companies, mergers and acquisitions, and outright theft via insiders and cyber intrusions, begin the comprehensive and strategic framework for how China implements their strategy.

China continues to utilize "non-traditional" collectors to conduct a plurality of their nefarious efforts here in the United States due to their successful ability to hide in plain sight. The non-traditional collectors, serving as engineers, businesspersons, academics, and students are shrouded in legitimate work and research, and oftentimes become unwitting tools for the CCP and its intelligence apparatus.

China's ability to holistically obtain our Intellectual Property and Trade Secrets via illegal, legal, and sophisticated hybrid methods is like nothing we have ever witnessed. Joint ventures, creative investments into our Federal, State, and local pension programs, collaborative academic engagements, Sister City Programs, Confucius Institutes on Campus, Talent Recruitment Programs, investments in emerging technologies, and utilization of front companies continue to be the framework for strategically acquiring the thoughts and ideas of our researchers, as well as development of those ideas pre- and post-patent application. The threat from China pertaining to academia is both wide, and deep. The past 6 years of indictments and prosecutions have highlighted the insidiousness of China's approach to obtaining early and advanced research as well as understanding the complexity of gifts and funding at U.S. colleges and universities, particularly when tied to Federal grants.

INDUSTRIES LEADING AS TARGETS

China's priorities for obtaining U.S.-based technology and know-how, pursuant to their publicly-available "Made in China 25 Plan" are Aerospace, Deep Sea Technology, Biotechnology, Information Technology, Manufacturing, Clean Energy, Electric Battery Technology, and DNA/Genomics.

Any CEO or board of directors leading in any of these critical industries must become aware of the threat posed to them and work with their security team and outside experts to identify risk-based mitigation strategies.

LONG-TERM CONSEQUENCES OF IP THEFT

The proverbial salt in the wound of the China's nefarious activity is when the CCP steals our thoughts, ideas, patents, and technology, and manufactures that same technology in China, and then sells it back to American companies and around the world. One needs to look no further than the American Supercomputer Corporation for just a glimpse of the long-term impact to economic espionage.

Then one must factor in all the manufacturing plants which were are not built, and the tens of thousands of jobs which were not created because China, via its theft, beat the United States to the global market and is selling the same product and a significant reduction in real costs.

Currently prescient is the passage of the CHIPS and Science Act, as well as the Inflation Reduction Act. Rest assured, China has already begun their strategic, and comprehensive, efforts to acquire (both legally and illegally) any and all ideation, research, and trade secrets emanating from the extensive funding provisions and technological incentives, provided by these legislative actions.

I would offer emerging renewable energy technologies, and semiconductor production will be targeted most aggressively. Congress must lead and hold everyone accountable for assuring that 10 years from now Congress cannot be holding hearings

and asking how China stole our technology, and capabilities, and are selling them back to us . . . as consumers.

CORPORATE AWARENESS OF DETAILS

Boards of Directors and investment leaders must begin to look beyond the next fiscal quarterly earnings call and begin to think strategically with respect to how their decisions and unawareness of the long-term threat impact their businesses and industries, which is woven with our national security, economic stability, and endurance of our republic.

In 2017, the Communist Party of China issued new State laws to facilitate the perniciousness of their efforts to obtain data, from everywhere. Three specific portions of those laws should be understood, and be an enduring reminder to CEOs, general counsels, chief data officers, CIOs, and CISOs, throughout our private-sector ecosystems.

The first is Article 7 of the People's Republic of China National Intelligence Law summarily stating that all business and citizens shall cooperate with China's intelligence services and shall protect all national work secrets.

The second is Article 77 of the same National Security Law summarily stating that Chinese citizens and business shall provide anything required or requested by the Chinese government or intelligence services.

The third is Article 28 of the 2016 Cybersecurity Law summarily stating that all network operators must provide data to, and anything requested by, national, military or public security authorities.

Hence, if you are a U.S. business seeking to enter a business relationship with a company in, or from, China, your data will be obtained and provided to the MSS or PLA for their usage. This includes third-party data as well. The analogy is a U.S. company enters into a business deal or partnership with a company from another country. The U.S. company must provide all relevant and requested data from their company, as well as the partner company, to the NSA, CIA, and FBI.

CHINA DOES NOT PLAY BY ANY RULES

China plays by their own rules. China does not conform to any normalized set of regulations, guidelines, norms, laws, or value-based agreements throughout the global economic ecosystem.

To further the CCP's unleveled economic playing field, out of the 15 largest companies inside China, 13 are either owned by the CCP, or run by the CCP. The world has seen recently what the CCP is capable of when one of the largest companies in the world, Alibaba, pushes back on state-run efforts. Additionally, many of the CCP's largest corporate leaders and CEO's have gone missing.

American business leaders, and Americans in general, must understand that China is a Communist country run by an authoritarian "President" for life. Unlike in the United States and Western democracies, and like Putin's Russia, there is no bifurcation between the government, industry, and or criminal organizations.

ANALOGY

Hence, for a prospective business deal with a company in the United States, the Chinese company can partner with China's intelligence services to assist in negotiations, vulnerabilities, and utilization of any already-acquired data from said U.S. company. Again, this is akin to a U.S.-based company calling he CIA and NSA for assistance on preparing a bid to merge with a company outside the United States and use all types of classified collection to form a proposal or use during negotiations.

DATA ACCUMULATION

The willingness of China, and its intelligence services, to illegally, and legally, obtain DATA to drive artificial intelligence, research and development programs, and to facilitate their military and economic goals without doing the hard work to independently develop on their own, drives at the heart of China's unfair practices. It is estimated that 80 percent of American adults have had all of their personal data stolen by the CCP, and the other 20 percent most of their personal data.

From genomics and DNA to third-party financial data stored in cloud services providers, to fertility to internet of things technology, the effort du jour is accumulation of data, and lots of it.

SOCIAL CREDIT SCORE

China continues to surprise the world by aggressively stifling their citizens via laws, regulations, unparalleled domestic surveillance, and a debilitating Social Credit Score for every citizen. And a conversation about what is occurring the Uyghurs is for another hearing. It is important to remember that Chinese nationals, here in the United States are continuously monitored and their actions impact their credit score.

UNITED FRONT WORK DEPARTMENT

China's efforts to prohibit and violate free speech inside the United States must be identified, exposed, and mitigated. China conducts such activities on Chinese nationals and on American citizens. Similarly, the CCP utilizes a suite of capabilities to silence critics here in the United States when the activity is exposed. The utilization of the United Front Work Department to drive false narratives in social media and within mainstream print and television media is consistent and enduring. There are numerous examples of such, however I want to reference just a few recent examples. The first is the Chinese Embassy in Washington, DC pressuring Nobel scientists to censor their speeches at the 2021 Noble Prize Summit. The prize winners were bullied by the government of China to disinvite the Dalai Lama for the award ceremony. The second example is Zoom executive charged for working with the Chinese intelligence services to disrupt Zoom calls in the United States commemorating Tiananmen Square. The third example is American actor John Cena apologizing, in Mandarin, because of the pressure Chinese officials placed on him, and Hollywood, because he referenced Taiwan as a country. The pressure being placed by China on Hollywood has grown to a credibility-questioning level and impacts just about every decision they make with respect to scripts and potential villains. This is referred to as "apology diplomacy" and has been publicly visible for many years when CEOs and company executives must apologize to Xi or the China for indiscretions with respect to referring to Taiwan as an independent country.

A final example, and one that really illustrates the granularity and scope of the CCP and UFWP, is when the CCP forced a small Jesuit high school in Colorado to change language on their website to designate Taiwan as part of China. The CCP identified this when the high school applied for credentials to take part in the United Nations Commission on the Status of Women.

OPERATION FOX HUNT

One of the most disturbing, and illegal, activities by the CCP on American soils is Operation Fox Hunt. Operation Fox Hunt is an international effort by the CCP to identify, locate, and attempt to bring back Chinese dissidents who have left China and are causing President Xi and the Communist Party discontent. For almost a decade Chinese intelligence service have been building teams to conduct surveillance in the United States, oftentimes falsely entering relationships with local law enforcement to garner information on who China claims are fugitives and attempt to bring them back to China. In January 2023, the FBI conducted a search warrant of a suspected Chinese police station in New York City which was furthering this effort, and most likely more undisclosed illegal activity.

The willingness, ability, and success of the Communist Party of China to conduct such aggressive activity within the confines of America's borders is disturbing and unacceptable.

CYBER CAPABILITIES

From a cyber perspective, China has significant and unending resources to penetrate systems and obtain data, or sit dormant and wait, or to plant malware for future hostilities.

The FBI recently unveiled details for the first time on a 2011–2013 Chinese state-sponsored cyber campaign against U.S. oil and natural gas pipeline companies that was designed to hold U.S. pipeline infrastructure at risk.

Additionally, in July 2021, DOJ unsealed an indictment charging four individuals working with China's MSS for a global cyber intrusion campaign targeting intellectual property and confidential business information, including infectious disease research. Targeted industries around the world included aviation, defense, education, government, health care, biopharmaceutical, and maritime.

And last, in July 2021, NSA, FBI, CISA publicly released more than 50 cyber tactics and tools used by Chinese state-sponsored hackers against the United States as well as mitigation steps for U.S. companies.

Over the past decade we have seen CCP cyber and insider threat breaches and criminality to such a level I fear we are becoming numb when it is identified. One such event was the Equifax breach in May 2017. As a former head of U.S. Counterintelligence, I consider this to be one of the CCP's greatest intelligence collection successes. More than 145 million Americans had all their financial data, nicely aggregated, to the CCP along with Equifax's business process and trade secrets on how they acquire and share such data. That is every American adult.

Anthem lost 80 million medical records in 2015, Marriott lost 500 million guest's records in 2014, and in 2015 OPM lost 21 million records to China's cyber theft. I would be remiss if I left out China's breach of multiple cloud service providers in which China obtained access to over 150 companies' data.

INSIDER THREAT

The insider threat epidemic originating from the CCP has been nothing short of devastating to the U.S. corporate world. Anyone can go to Department of Justice's web site and search economic espionage. The result is hard to swallow and quantify. And those listed cases are just what was identified, reported by a U.S. company, and then prosecuted. I will touch on the impact of economic espionage a bit later.

In April 2021, a former scientist at Coca-Cola and Eastman Chemical was convicted of economic espionage & theft of trade secrets, on behalf of the CCP. The scientist stole trade secrets related to formulations for bisphenol-A-free (BPA-free) coatings for the inside of beverage cans. The scientist was working with a corporate partner inside China to monetize the stolen data utilizing the new company in China. The CCP had invested millions in the shadow new company in China. The stolen trade secrets cost U.S. companies approximately $120 million to develop per open-source reporting. This is one example from the dozens identified in the past 5 years.

AGGREGATED CAPABILITIES

When you combine the persistence of intent and capability for the CCP's cyber intrusion programs, with the onslaught of insiders being arrested, indicted, and convicted by the FBI and DOJ over the past decade, it creates a formidable mosaic of insurmountable levels. But it is not. With a comprehensive whole-of-government, and whole-of-society, approach of defending against China with awareness, strategy, enhanced defenses, practical mitigation programs, and a patriotic value-based return to great competition, the United States can begin change the course of history as I see it now.

SUPPLY CHAIN

So, what is current and next in the targeted view scope by the CCP? Look no further than President Biden's economic growth agenda and proposed Congressional legislation detailing our strategic movement in the next few years. Electric vehicles, battery technology, bio agriculture, precision medicine, and sustainable green energy. All of this is prime targets for penetration, and theft, by the CCP. And at the same time, Ford Motor Company decided to partner with Contemporary Amperex Technology Co. Limited (CATL). This partnership is selfish, creates disincentive for investors to develop battery plans here in the United States. Additionally, and more importantly, this partnership creates a critical supply chain dependency not only to the state-sponsored CATL, but as well the CCP as a whole.

As an analogy, China manufactures, produces, and delivers 80 percent to the antibiotics sold and utilized in the United States. We cannot afford to continue to allow China to control and/or manipulate our critical and emerging supply chains and potentially hold us hostage in the future.

LEGITIMATE BUSINESS USED AS INTELLIGENCE GATHERING

China's strategic ability to utilize legitimate business ventures and investment in the United States that can also serve as intelligence collection and monitoring vehicles is comprehensive. It also provides the signature mosaic of how the best capitalistic economy the world has ever seen can be vulnerable to adversaries who hide their capabilities on our soil and in plain sight. Three simple and current event examples I will proffer is Huawei Technologies, farmland purchases near military installations, and ZPMC Cranes at critical U.S. maritime and military shipping ports.

MALIGN INFLUENCE

I would be remiss if I did not reference the strategic and aggressive nature in which the CCP conducts malign foreign influence in the United States. Unlike Rus-

sia's persistent attempts to undermine our democracy and sow discord, the CCP strategically, and with precision, conducts nefarious influence campaigns at the State and local level.

I have referenced the influence success in Hollywood and the self-censoring which occurs to not offend China to ensure sales of their product to the Chinese markets. When it comes to Taiwan, the CCP becomes the most aggressive. Oftentimes State and local officials agree to travel to Taiwan to identify or negotiate economic investment opportunities. The CCP will undoubtedly apply holistic pressure to the local officials, from overt threats to subtle promises of economic infusion at the city or town level. There is most likely a company or business located inside an official's town which is heavily influenced or leveraged by prior investment by the CCP. China will apply pressure to that U.S. company and threaten to slow down production or manufacturing in China if the company officials do not apply their respective influence on the elected leader to not travel to Taiwan. This State or local official, or even U.S. Congressperson, may have no knowledge of China's intent beneath the surface. At the same time, and not coincidently, an op-ed or article will appear in the local newspaper downplaying economic investment opportunities in Taiwan and championing alternative efforts in China.

WHY IT ALL MATTERS

In 2020, the estimated economic loss from the theft of intellectual property and trade secrets, JUST from the CCP, and JUST from known and identified efforts, is estimated between $300 billion and $600 billion per year (Office of the U.S. Trade Representative). To make it more relevant to Americans reading this, it is approximately $4,000 to $6,000 per American family of four . . . after taxes.

Additionally, in 2010 China had 1 company in the top 10 of Forbes' Global 2000 list. In 2020 they had 5. That is a 500 percent increase in one decade. Competition is great and necessary and is what made America the global leader we are today. However, I would proffer China's growth through any and all means is much less than fair competition. To reiterate, competition is always good, and necessary in any aspect. My question is . . . are we really competing? If we do not alter how we compete on the global ecosystem with awareness of China's methodology and practices, we will not be able to sustain our global position as the world leaders in technology, manufacturing, education, science, medicine, research, development, and thoughts and ideas. We must aggressively enhance our willingness to not only understand these threats and unfair practices but be willing to create a robust public private partnership with intelligence sharing to combat the CCP while at the same time staying true to the values, morals, and rule of laws made America the greatest country in the world. Additionally, we must urgently decide that breaking the stranglehold of the CCP on our vast supply chain must end. The United States must engage in an aggressive and urgent redundancy effort and begin to have alternate servicing of goods, products, and technologies.

PROTECT WHAT IS DEVELOPED

Congress's recent passage of a bill to bolster competition and provide the much-needed resources to do so is a great start down this long road. However, we must also protect the fruits of this legislative labor from being stolen and siphoned out of the United States by the same techniques China successfully utilizes today. Otherwise, we will continue to conduct research and development which the CCP will obtain, legally, and illegally, to bolster their economic, geopolitical, and military goals of global dominance well into the future.

CLOSING

In closing, I would like to thank this subcommittee, and the House Homeland Committee writ large, for acknowledging the significant threat posed by China, not only by holding this hearing, but with all the recent legislative actions the past year on combatting this threat as well as driving enhanced competition. Continuing to combat the threat posed by the CCP will take a whole-of-Nation approach with a mutual fund analogous long-term commitment. Such an approach must start with robust and contextual awareness campaigns. The WHY matters. Regarding these awareness campaigns, we must be specific and reach a broad audience, from every level of government to university campuses, from board rooms to business schools, educating on how China's actions impair our competitive spirit by obtaining our research and development, trade secrets and intellectual property, and degrading our ability to maintain our role as economic global leaders. I have provided some recommendations for this committee, the IC, the administration, academia, research

and development, as well as CEOs and boards of directors in our holistic efforts to detect and deter these threats, as well as educate, inform, and compete.

Our Nation needs strategic leadership now more than ever, particularly when we face such an existential threat from a capable competitor who is looking beyond competition to the global dominance.

Last, I would like to state for the record the significant National security threat we face from the Communist Party of China is NOT a threat posed by Chinese people, as individuals. Chinese nationals, or any person of Chinese ethnicity here in the United States, or around the world, are not a threat and should NOT be racially targeted in any manner whatsoever. This is an issue pertaining to a communist country, with an autocratic dictator who is committed to human rights violations and stopping at nothing to achieve his goals. As a Nation, we must put the same effort into this threat as we did for the terrorism threat. The threat from China, particularly with respect to the long-term existential threat is hard to see and feel, but I would suggest it is much more dangerous to our viability as a Nation.

RECOMMENDATIONS

The holistic, and existential threat posed by the CCP is one of the few bipartisan agreements in the U.S. Congress today. We must take this opportunity to expeditiously advise, inform, and detail the threat to every fabric of our society, and why it matters. We must, as a Nation, compete at the highest level possible while at the same time understand why we are doing so, and what is at stake.

1. Enhanced and aggressive real-time and actionable threat sharing with private sector. Create an Economic Threat Intelligence entity which delivers actionable, real-time threat information to CEOs, boards of directors, State and local economic councils to enable risk-based decision making on investments and partnerships. The analogy would be the Financial Services ISAC. This intelligence delivery mechanism should include the intelligence community, FBI, and CISA and have at is core constituency State and local entities at risk and utilize existing vehicles such National Governors Association and the Chamber of Commerce to increase threat awareness of illicit activities investment risk at the State and local level.
2. Congress must ensure U.S. Government agencies are leaning aggressively forward in providing collected intelligence pertaining to plans and intentions, as well as nation-state activities, in software, coding, supply chain, and zero-day capabilities. The U.S. Government must be more effective in providing intelligence to the private sector. Enhanced declassification of collected intelligence with respect to threats to our economic well-being, industries, and companies must be delivered at speed to impacted entities prior to the threat becoming realized.
3. Bipartisan Congressionally-led "China Threat Road Shows" to advice and inform of the threat to CEOs, Governors, and Boards of Directors in critical economic, research, and manufacturing sectors.
4. Close governance and oversight of China Competition legislation with measurable outcomes and effectiveness reviews. Particularly in the research and development space.
5. Create a panel of CEOs who can conversely advise and inform Congress, the IC, and U.S. Government entities on perspectives, challenges, and obstacles in the investment arena and private sector. Currently, there is no such venue existing. I would recommend a Business Round Table type of framework. Membership should be diverse and include but not limited to the following sectors: Financial Services, Telecommunications, Energy, Bio Pharmaceutical, Manufacturing, Aerospace, Transportation, Private Equity and Venture Capital. Select key government participants and encourage actionable outcomes. This entity should be co-chaired by a CEO form this group.
6. Create a domestic version of the State Department's Global Engagement Center. The U.S. Government needs a "sales and marketing" capability which can partner with U.S. business and academia to guide new and emerging threat intelligence, answer pertinent questions, and construct awareness campaigns against the threat from the CCP and other similar issues.
7. Establish an over-the-horizon panel to discuss, in a public forum, emerging threats posed to the long-term economic well-being of America. The first topic should take a close look at the strategic investments the CCP is making into State and local pension plans, as well as the Federal Thrift Savings Plan.
8. Immediately create a Supply Chain Intelligence function which can sit both in the U.S. Government, as well as outside of government, to facilitate real-time intelligence sharing. This entity should include members of the private sector

skilled in understanding our supply chain and who can expedite reacting to emerging threats. This entity will also be able to provide the U.S. Government cogent mitigation strategies and assistance with policy formulation to protect our vulnerable supply chain from persistent penetration and manipulation by China and Russia.

9. STEM must become a U.S. educational priority once again. It must be funded, focused, measurable, and begin at the earliest stages of the K through 12 educational tracks. It must also be looked upon as a long-term project (25 years).

Chairman PFLUGER. Thank you, Mr. Evanina.

I now recognize General Guastella for his opening statement.

STATEMENT OF LIEUTENANT GENERAL JOSEPH T. GUASTELLA, JR. (RET.), SENIOR FELLOW, THE MITCHELL INSTITUTE

General GUASTELLA. Chairman Pfluger, Ranking Member Magaziner, Members of the committee, thank you for the opportunity to appear before you today.

As an individual who spent over 3 decades in service to our Nation, I am also deeply concerned about the threats the Chinese Communist Party drives toward the U.S. homeland, especially in the military swim lane. That is why events like this today are so important.

On my last assignment on active duty I was the deputy chief of staff for operations for the United States Air Force. Our job was to organize, train, and equip forces, air forces, and then present those forces to the combatant commanders around the world. That includes NORAD NORTHCOM, the command in charge of homeland defense. I also developed a very good understanding of the threats that China poses to the United States and the capabilities they use to achieve those those objectives.

I would first like to highlight or begin describing the threat that China poses to the United States and its allies. So in 1991, when the United States was celebrating the end of the cold war, and we also were celebrating victory in Operation Desert Storm, China went to school on United States. They took note, and they started a very concerted and deliberate effort to modernize their military capabilities. Here we are, 3 decades later, they have largely met that mark, and they even seek further progress. That's why this year, they saw even a significant increase in their defense spending. Their military now enjoys leading-edge capabilities that include long-range precision strike, hypersonic weapons, advanced integrated air defense weapons, stealthy aircraft, surface-to-air missiles, and electronic warfare. Several of those systems have the range to hold the U.S. homeland at risk. So the Chinese spy balloon, as was mentioned before, which garnered significant attention this past February, is a very loud wake-up call regarding CCP's global ambition.

Unfortunately the United States is stretched thin when it comes to the capabilities and the capacity required to defend our homeland in the air domain—air and space domain. NORAD was originally designed to detect and defend North America from a catastrophic attack from the Soviet Union, later Russia. An additional role was added on after 9/11 to intercept, identify, and redirect unidentified aircraft that are approaching restricted areas. So the

NORAD radars were optimized and tuned to detect aircraft that met those criteria. So balloons, until recently, generally did not fit in that category.

As threats evolve, including balloons, stealth aircraft, UASs, unmanned aerial systems, cruise missiles, so must our detection and defense enterprise. This will require that we modernize current radars and install new sensors in emerging zones of vulnerability, not just over the Nation, but well outside our sovereign territories so we can get a heads-up that they are coming.

We must invest resources in the NORAD mission. That command gets its aircraft from the U.S. Air Force, but the Air Force today is the oldest and the smallest it's ever been in history. We're still flying B52s that are 60 years old, tankers that are over 50 years old, fighters over 30 years old. Even the famed F22, the best air air fighter ever made, first flew in 1997.

The homeland defense, however, doesn't start here in the homeland. Homeland defense starts abroad with the combatant commanders. The combatant commanders that have the forces that are capable of an offensive punch against our adversary countries that deters them from attacking United States. That's where it begins. The Air Force has to be modernized in the numbers necessary to meet the demands of the National Defense Strategy, as well as to deter threats against our homeland.

More specifically, consider the Air Force's fighter inventory is too small to meet real-world demands. It's a major security concern, for while other services possess fighters, the Air Force is specifically tasked with homeland security, the Air Sovereignty Mission. The Air National Guard is the entity within the Air Force that bears a preponderance of homeland defense. Their mission is particularly hard-hit by the gap between old aircraft that are aging out of the inventory and a lack of new aircraft arriving to back-fill those spots on the ramp.

So homeland defense also requires investment in modernization and command and control, resiliency ground and space-based sensors, data fusion, air refueling capabilities. Homeland defense is our highest priority mission. We need to start treating it that way.

You know, and more story, you know, to share with, with the group here. On January 8, 2020, 11 Iranian ballistic missiles hit a U.S. base at Al Asad in Iraq. I was the coalition forces air component commander at that time. We possessed the intelligence about the attack was going to happen, we were able to detect the missiles at launch, we were able to track the trajectory, but when it came to shooting them down, to defeating the missiles, we lacked any options. Why? Because we did not have the capacity, the defensive capacity, due to the other global commitments that our Force was spread across. American service members had to ride out that attack and hope for the best. It was an appalling set of circumstances.

Let's think what could happen against our homeland with threats like that.

Adversaries like China understand these vulnerabilities. The United States is gradually waking up to this reality, but leaders have yet to seriously address the shortfall. We're still in a problem-

admiring phase, not in a solution-implementation phase. That has to change.

So we have the bravest men and women in uniform. But we owe it to them to ensure they are prepared for the mission we ask them to execute. We owe it to our American citizens to ensure they are protected from attack. America's homeland is no longer a sanctuary against threats like China. We must recognize this new reality and aggressively close critical gaps in capacity and capability in the air domain.

Thank you for allowing us to focus on this topic today, and I look forward to your questions.

[The prepared statement of General Guastella follows:]

PREPARED STATEMENT OF JOSEPH T. GUASTELLA

MARCH 9, 2023

Chairman Pfluger, Ranking Member Magaziner, Members of the committee, thank you for the opportunity to appear before you today. As an individual who spent over 3 decades in service to our Nation, I am deeply concerned about the threats the Chinese Communist Party (CCP) poses to the U.S. homeland. That is why events like today's hearing are so important.

In my last assignment on active duty, I served as the deputy chief of staff for operations at Headquarters U.S. Air Force, where I was charged with leading the development and implementation of policy directly supporting global operations, force management, weather, training, and readiness across air, space, and cyber fields. To this end, I am well-versed in the threat China poses to the United States and the capabilities they have to manifest their objectives. It was my job to oversee airpower capabilities and capacity so that our combatant commands could respond to these challenges every day—and this included the homeland defense mission of North American Aerospace Defense Command (NORAD)/Northern Command (NORTHCOM).

I would first like to begin by describing the threat China poses to the United States and its allies. In the 1991, when the United States was celebrating the end of the cold war and victory in Operation Desert Storm, China made a concerted decision to modernize their military capabilities as a key ingredient in empowering their ascent as a leading military superpower.

Three decades later, they have largely met this mark and they seek further progress—that is why this year saw a marked increase in their defense spending. Their military now enjoys leading-edge capabilities that include long-range precision strike, hypersonic medium-range ballistic missiles, sophisticated integrated air defense system (IADS) comprised of stealthy fighter aircraft like the J–20 aircraft, surface-to-air missiles (SAMS), and electronic warfare (EW) units. These capabilities radically complicate the operating environment for U.S. forces and could portend significant combat attrition, especially for forward-operating bases and the non-stealth portions of America's combat air arm which makes up a vast portion of Air Force aircraft. Several of these offensive systems have the range to hold U.S. territory at risk, affecting us right here in the homeland.

The Chinese spy balloon, which garnered significant attention this past February, should serve as a wake-up call regarding the CCP's global ambitions. China's space-based intelligence, surveillance, and reconnaissance capabilities also gather information regarding the U.S. homeland. Nor are all these long-range systems passive threats. China's quest to field a "fractional orbital bombardment system"—a long-range missile that transits space en route to its target—are not capabilities designed to secure China's immediate borders. They are part of a strategic global strike system. The United States must take note.

Unfortunately, the United States is stretched thin when it comes to the capabilities and capacity required to defend our homeland. NORAD was originally designed to detect and defend North America from a catastrophic attack from the Soviet Union, later Russia. An additional role was added after 9/11: to intercept, identify, and redirect unidentified aircraft heading toward restricted air space. So, the NORAD radars were optimized and tuned to detect aircraft that meet those criteria.

Balloons—until recently—generally do not fit into that category. As the threat evolves, including balloons, stealth aircraft, UASs and cruise missiles . . . so must our detection and defense enterprise. This will require that we modernize current

radars and install new radars to cover emerging zones of vulnerability, not just over our Nation but well outside our sovereign territory. Approaches to our homeland China would use are far different than those used by Russia. We must invest new resources in the NORAD mission. The command gets its aircraft from the Air Force, but our Air Force today is the oldest and smallest it's ever been in its history.

The balloon intrusions should be a wake-up call to rebuild our air and space defenses—we are still flying B–52s over 60 years old; tankers over 50; and fighters over 30. Homeland defense doesn't start in the homeland. It starts abroad with the combatant commands having credible offensive punch to hold targets at risk in adversary countries. The Air Force needs to be modernized in the numbers necessary to meet the demands of our national defense strategy, and to deter threats against our homeland.

More specifically, consider that the Air Force's fighter inventory is too small to meet real-world demand. This is a major security concern, for while other service branches possess fighter aircraft, the Air Force is specifically tasked with the homeland security air sovereignty mission.

In 1991, the Air Force possessed 4,459 fighters. Today, it has 2,221. This represents a 49 percent reduction in capacity—the majority of which were produced in the cold war. However, this decrease in volume is not matched with a drop in operational demand. Quite the contrary given that the Air Force has been meeting nonstop combat requirements since Desert Storm in 1991. As the numbers of fighters decreased, the workload assigned to the remaining aircraft increased. They are now physically worn out and must be retired. Fourteen years ago, a Congressional Budget Office report concluded: "By 2009, 80 percent of the [Air Force's fighter] aircraft had used more than 50 percent of their originally planned service life. Clearly, the Air Force's fighter fleet is wearing out."[1] Circumstances have not improved over the ensuring decade, in fact, they have gotten worse. That is why you saw F–15C/Ds fighter aircraft withdrawn from Kadena Air Base in the Pacific this past year—not because the Air Force wanted to do this, but because the aircraft were so old they had to be retired and there were not enough new fighters to backfill them. Think of the signal that sent to China.

The simple reality is that Air Force has lacked funding necessary to procure a sufficient volume of new fighters to ensure the outflow of aging aircraft is matched by the inflow of newer examples. They have ranked third—behind the Army and Navy—in terms of Department of Defense funding for the past 3 decades.[2] That manifested very real results. Consider that the Air Force's leading 5th generation fighter, the F–22, had its production terminated at less than 20—5 percent of the original requirement. In the 2000's, leaders outside the Air Force thought the era of peer conflict was over. They were wrong. Nor is this a one-off example, with the production ramp rate of the F–35 lagging dangerously behind original intentions. In 2020, the Air Force was supposed to have 800 F–35As in its inventory, but instead only had 272.[3]

The Air National Guard, the entity which bears the preponderance of the homeland defense mission, is particularly hard-hit by gap between older aircraft aging out and a lack of new aircraft arriving to backfill their spots on the ramp. The Air National Guard tends to fly older fighters, so they are a fleet lead indicator for the broader Air Force. What happened at Kadena will be replicated throughout bases across America absent rapid intervention to reset the Air Force's fighter force.

Homeland defense also requires investment and modernization in command and control, resiliency, ground and space-based sensors, data fusion technology, AI, and air refueling capabilities. Homeland defense is our highest-priority mission, we need to start treating it that way.

We also lack sufficient capabilities and capacity to defend against a concerted air and missile attack at our forward bases. On January 8, 2020, 11 Iranian ballistic missiles struck U.S. forces based at the Ayn al Asad military complex in Iraq. I was the Coalition Forces Air Component Commander at the time. Our leadership possessed intelligence signaling the attack would happen, we were able to detect the missiles being launched, and we could track their trajectory. However, when it came to defeating these missiles, we lacked viable options because the joint force lacked sufficient missile defense capacity given other global commitments. American service members and many allies had to ride out the attack and hope for the best. That

---

[1] Congressional Budget Office (CBO), *Alternatives for Modernizing U.S. Fighter Forces*, (Washington, DC: CBO, May 2009), p. 55.

[2] David Deptula and Mark Gunzinger, *Decades of Air Force Underfunding Threaten America's Ability to Win* (Arlington, VA: Mitchell Institute for Aerospace Studies, 2022), p. 3.

[3] John A. Tirpak, "Keeping 4th-Gen Fighters in the Game," *Air Force Magazine,* October 1, 2019.

was an appalling set of circumstances. Think if that had happened in your home town or key bases here in America.

Adversaries like China understand these vulnerabilities. The United States is gradually waking up to this reality, but leaders have yet to seriously address the shortfall. Note how difficult it is to provide effective, sustainable solutions to Ukraine—guarding against everything from air strikes, drone attacks, and missile bombardment. We are still in a "problem admiring" phase, not in a "solution implementation" window. This must change.

It is worth remembering that some of the first responders on the morning of 9/11 were airmen. Two off them quickly scrambled from Andrews Air Force Base to intercept a hijacked airliner bound for the Nation's capital. We had no time to arm those F–16s because in the post-cold war era, we thought our homeland was safe—we had stopped sitting alert. That meant those airmen were prepared to sacrifice their lives to bring down that hijacked aircraft. The passengers on Flight 93 bravely took matters into their own hands before our airmen were asked to make that sacrifice. The point in telling this story is to highlight that we have the bravest men and women in uniform. But we owe it to them to ensure they are prepared for the mission we ask them to execute. We also owe it to our citizens, to ensure they are protected from attack. America's homeland is no longer a sanctuary. We must recognize this new reality and aggressively close critical gaps in capacity and capabilities for homeland defense. Thank you for focusing on this topic today. With that, I look forward to your question.

Chairman PFLUGER. Thank you very much for your opening statement.

I now recognize Ms. Bingen.

STATEMENT OF KARI A. BINGEN, DIRECTOR, AEROSPACE SECURITY PROJECT AND SENIOR FELLOW, INTERNATIONAL SECURITY PROGRAM, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

Ms. BINGEN. Thank you, Chairman Pfluger, Ranking Member Magaziner, and distinguished Members of the subcommittee. Thank you for letting me appear before you today.

I have been fortunate to examine these issues from my time at a technology start-up, time at the Department of Defense, and then here legislatively, as a staffer on the House Armed Services Committee.

Let me start by saying conflict with China is not inevitable. Not inevitable. However, the Chinese Communist Party has ambitions to become the world's leading power and has undertaken a broad campaign using all tools of national power and influence to achieve its aims. While strategic competition and potential military conflict with China may seem abstract to many Americans, the Chinese surveillance balloon was a tangible, visible sign that the U.S. homeland is not out of reach of Beijing's threats. The piracy challenge is one of both national and economic security. It is not only the pacing military threat for the United States, but also the top threat to U.S. technology competitiveness.

I will discuss three areas where the CCP threat to the U.S. homeland is particularly acute—technology acquisition, critical infrastructure, and influence operations—and then I'll offer a few recommendations to help address these challenges.

First, technology acquisition. Beijing has made it a national goal to acquire foreign technologies, to advance its economy and modernize its military. It continues to use both legal and illegal methods to target U.S. technologies, including in areas such as high-performance computing, biopharmaceuticals, robotics, energy, and aerospace. It targets the people, information businesses, and re-

search institutions in the United States that underpin them. These methods include economic espionage, cyber data exfiltration, joint ventures, research partnerships, and talent recruitment programs, among others. My written testimony offers several specific examples of where the CCP has put these methods into practice. This matters for our defense, as our military's battlefield advantage has long rested on our superior technology. However, that is at risk as Beijing seeks to close the gap in our technology advantage. This matters for American businesses, as Mr. Evanina said, wherein $225 to $600 billion is the annual estimated cost to the U.S. economy from stolen intellectual property. CCP law and policy further bolsters these methods. For example, its 2017 National Intelligence Law requires organizations and citizens to support intelligence work and to keep it secret.

Second, the CCP is targeting critical infrastructure in the United States. I fully anticipate that Beijing would seek to disrupt it, possibly through cyber attacks, especially early in a conflict. This could be motivated by a desire to deter U.S. action, affect U.S. decision making, delay the mobilization of U.S. forces, or affect the will of the American people. The government has taken some steps to share intelligence information on PRC campaigns to target critical infrastructure, such as oil and gas pipelines, and importantly, it also included sharing tactics and techniques and procedures used by the Chinese.

Third. The U.S. homeland is within reach of the PRC's influence activities. Examples include TikTok, that U.S. intelligence officials caution can be influenced by CCP-driven manipulation of its algorithms. They also include Operation Fox Hunt, where CCP-directed individuals spy on U.S.-based pro-democracy advocates, intimidate Chinese and Chinese-American students at universities, and pressure individuals in the United States to return to China, including by threatening their family members. The PRC also exerts influence through its Belt and Road Initiative, exporting terrestrial infrastructure, information and communications technologies, and other technology areas. This global influence directly impacts U.S. businesses and U.S. security interests here at home.

One acute area of competition is in commercial telecommunications, including satellite broadband communications like SpaceX's Starlink and Amazon's Project Kuiper, which CSIS recently examined. Further expansion of Chinese telecommunications services could boost Beijing's presence in foreign terrestrial networks, providing the CCP with remote access, enabling it to surveil users, block internet access, and sensor information.

I offer a few recommendations to help address these challenges. Expanding education and awareness. This hearing is very important on that regard to remind the American public that the threat posed by the CCP is not abstract, nor solely a distant military conflict that could take place across the Pacific. The American public and businesses need to understand the security and economic risks posed by the CCP and understand that they are a target.

Expand intelligence threat sharing with the private sector, building off CISA's work to date, so companies can better understand their vulnerabilities and make risk-informed decisions regarding their protection and resiliency.

Transform counterintelligence and security missions, including leveraging technology like artificial intelligence to help identify supply chain vulnerabilities, track foreign agents, and illuminate disinformation.

Leverage technology innovation. Maintaining U.S. technology leadership means not just preventing the transfer of technology to the PRC, but also setting the conditions for our innovation sector to stay ahead of the competition.

Boosting cooperation with our allies and partners, which is a competitive advantage and source of strength that the CCP does not have. Technology cooperation can be a strong feature of these relationships.

Then finally, continuing to invest in a strong defense, including homeland defense, which is required to deter PRC aggression, build resiliency to attacks, and ensure that we have the trained people posture, intelligence, weapon systems and munitions to defend the United States and the American people.

Thank you again for your time today, and I look forward to your questions.

[The prepared statement of Ms. Bingen follows:]

PREPARED STATEMENT OF KARI A. BINGEN

MARCH 9, 2023

Chairman Pfluger, Ranking Member Magaziner, and distinguished Members of the subcommittee, thank you for the opportunity to appear before you today to discuss "Countering Threats from the CCP to the Homeland." The Center for Strategic and International Studies (CSIS) does not take policy positions, so the views represented in this testimony are my own and not those of my employer.

I have the privilege of leading the Aerospace Security Project at the Center for Strategic and International Studies, where I examine these issues largely through a national security lens, drawing from my experiences working at a U.S. technology startup, serving in the Department of Defense (DoD) guiding defense intelligence and security activities, and supporting the House Armed Services Committee.

Conflict with China is not inevitable, but the Chinese Communist Party (CCP) has been studying the United States, studying our way of war and our vulnerabilities, expanding and modernizing its military, using its economic influence to coerce others, and putting in place the pieces to "win without fighting." As stated in the administration's 2022 National Security Strategy, the People's Republic of China (PRC) has ambitions "to become the world's leading power" and to "reshape the international order . . . to its benefit."[1] For the Department of Defense, the PRC is its "pacing challenge."[2]

Beijing has undertaken a broad campaign using all tools of national power and influence—diplomatic, economic, military, technological, and informational—to achieve its aims. While strategic competition and potential military conflict with China may seem abstract to many Americans, the Chinese surveillance balloon, shot down off the East Coast on February 4, 2023, was a tangible, visible signal that the U.S. homeland is not out of reach of Beijing's threats. It is also a reminder that the CCP's broad campaign for global power status and domination in the Indo-Pacific necessitates a focus on the U.S. homeland.[3]

I offer three areas where the CCP threat to the U.S. homeland is particularly acute: Technology acquisition, critical infrastructure, and influence operations.

---

[1] "National Security Strategy," The White House, October 12, 2022, *https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.*

[2] "National Defense Strategy of The United States of America," Department of Defense, October 27, 2022,*https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.pdf.*

[3] "Annual Threat Assessment of the U.S. Intelligence Community," Office of the Director of National Intelligence, February, 7, 2022, *https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf.*

TECHNOLOGY ACQUISITION

Beijing has made it a national goal to acquire foreign technologies to advance its economy and modernize its military. It continues to comprehensively target advanced U.S. technologies, including in areas such as high-performance computing, biopharmaceuticals, robotics, energy, and aerospace. These are among ten areas that Beijing has explicitly identified as high priorities in its "Made in China 2025" strategic initiative to achieve technological superiority.[4] Aerospace is an example where Chinese President Xi Jinping has articulated his "space dream" to make China the foremost space power by 2045.

To acquire these technologies, Beijing uses both licit and illicit methods to target the people, information, businesses, and research institutions in the United States that underpin them. These methods include economic espionage, cyber data exfiltration, joint ventures, research partnerships, and talent recruitment programs, among others.[5]

The Director of National Intelligence's 2018 Worldwide Threat Assessment judged that, "most detected Chinese cyber operations against U.S. private industry are focused on cleared defense contractors or IT and communications firms."[6] Over the past several years, U.S. Department of Justice convictions or indictments highlight numerous of these methods in practice. Both Chinese nationals and U.S. citizens have been charged with economic espionage and attempted acquisition of sensitive U.S. defense technology in areas such as anti-submarine warfare, aviation, and submarine quieting technology.[7] Lucrative stipends, as part of Beijing's Thousand Talents Program, were offered to researchers to bring their technical knowledge to China.[8] Chinese real estate investors sought U.S. farmland and wind farms in proximity to U.S. military bases, and Chinese telecommunications equipment (e.g., Huawei devices) has been found near U.S. missile bases, all of which could be used to surveil or disrupt U.S. defense activities.[9]

This matters for our defense, as the PRC employs methods on American soil to funnel U.S. technology and know-how back to Beijing to advance its own military capabilities while also exploiting U.S. military vulnerabilities. The U.S. military's battlefield advantage has long rested on our superior technology. But that is at risk as Beijing seeks to close the gap in our technology advantage and become a world-class military power, on par with the United States, by 2049.

This matters for American businesses. The Office of the Director of National Intelligence estimated in 2015 that the cost of economic espionage through hacking is $400 billion per year, largely attributable to the PRC. The Commission on the Theft of American Intellectual Property in 2017 estimated that the cost to the U.S. economy from stolen intellectual property (IP) could range from $225 to $600 billion annually.[10]

---

[4] Karen M. Sutter, "'Made in China 2025' Industrial Policies: Issues for Congress," Congressional Research Service, December 22, 2022, 1, *https://crsreports.congress.gov/product/pdf/IF/IF10964/9.*

[5] "Foreign Economic Espionage in Cyberspace," National Counterintelligence and Security Center, 2018, *https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.*

[6] Daniel R. Coats, "Worldwide Threats Assessment of the US Intelligence Community," Office of the Director of National Intelligence, Feb 13, 2018, *https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA__Unclassified-SSCI.pdf.*

[7] United States Attorney's Office, District of Massachusetts, "Chinese National Arrested for Conspiring to Illegally Export U.S. Origin Goods Used in Anti-Submarine Warfare to China," Department of Justice, June 21, 2018, *https://www.justice.gov/usao-ma/pr/chinese-national-arrested-conspiring-illegally-export-us-origin-goods-used-anti-submarine;* United States Attorney's Office, Northern District of New York, "Former GE Power Engineer Sentenced for Conspiracy to Commit Economic Espionage," Department of Justice, January 3, 2023, *https://www.justice.gov/usao-ndny/pr/former-ge-power-engineer-sentenced-conspiracy-commit-economic-espionage.*

[8] Ellen Barry and Gina Kolata, "China's Lavish Funds Lured U.S. Scientists. What Did It Get in Return?," The New York Times, February 6, 2020, *https://www.nytimes.com/2020/02/06/us/chinas-lavish-funds-lured-us-scientists-what-did-it-get-in-return.html.*

[9] Eamon Javers, "Chinese Company's Purchase of North Dakota Farmland Raises National Security Concerns in Washington," CNBC, July 1, 2022, *https://www.cnbc.com/2022/07/01/chinese-purchase-of-north-dakota-farmland-raises-national-security-concerns-in-washington.html;* Lars Erik Schönander and Geoffrey Cain, "China Is Buying the Farm," The Wall Street Journal, September 8, 2022, *https://www.wsj.com/articles/the-chinese-are-buying-the-farm-north-dakota-hong-kong-land-food-shortage-supply-chain-usda-11662666515;* Lillis, Katie Bo. "CNN Exclusive: FBI Investigation Determined Chinese-Made Huawei Equipment Could Disrupt US Nuclear Arsenal Communications." CNN, July 25, 2022. *https://www.cnn.com/2022/07/23/politics/fbi-investigation-huawei-china-defense-department-communications-nuclear/index.html.*

[10] Chris Strohm, "No Sign China Has Stopped Hacking U.S. Companies, Official Says," Bloomberg, November 18, 2015, *https://www.bloomberg.com/news/articles/2015-11-18/no-sign-*

CCP law and policy further bolsters these methods. The CCP's Military-Civilian Fusion (MCF) policy blurs the distinction between civil/commercial sectors and military/defense industrial sectors. It facilitates the transfer of technology and investments from the commercial sector to the military. Its national intelligence law, passed in 2017, requires that "all organizations and citizens shall support, cooperate with, and collaborate in national intelligence work . . . and shall protect national work secrets they are aware of."[11]

Finally, the PRC's advances in technology will undoubtedly also be fueled by its increase in research and development (R&D) expenditures and its science, technology, engineering, and math (STEM) workforce, both of which have trendlines that are increasing in China and decreasing in the United States. Data from the National Science Board shows that, over the 2000 to 2019 period, the United States share of global R&D declined from 37 to 27 percent while the share by China increased from 5 to 22 percent.[12] A recent study by Georgetown's Center for Security and Emerging Technology estimated that, by 2025, China's yearly STEM PhD graduates will nearly triple the number of U.S. graduates (in the same fields).[13]

The PRC challenge is one of both national and economic security. It is not only the pacing military threat for the United States, but also the top threat to U.S. technological competitiveness.

CRITICAL INFRASTRUCTURE

The CCP is targeting critical infrastructure in the United States. I fully anticipate that—should a crisis or conflict unfold—Beijing would seek to disrupt the operations of critical infrastructure in the United States, especially early on. This could be motivated by a desire to deter U.S. action, affect U.S. decision making, delay the mobilization of U.S. forces, or affect the will of the American people.

The DoD's annual military assessment of the PRC was stark in its assessment, "China seeks to create disruptive and destructive effects . . . to shape decision making and disrupt military operations in the initial stages of a conflict by targeting and exploiting perceived weaknesses of militarily superior adversaries."[14] Both the DoD and intelligence community have further assessed that China could launch cyber attacks against critical infrastructure in the United States, such as oil and gas pipelines, and rail systems, that would disrupt service for days to weeks.[15]

The ransomware network hack of the Colonial Pipeline in May 2021, although not attributed to the PRC, provided a glimpse of what such disruptions could look like, with gas shortages, long lines at gas stations, and the panic buying that ensued. Similarly, the electrical grid failure in Texas in February 2021, also not the result of any PRC action, showcased the wide-spread impact of the loss of power for millions of Americans.[16]

The U.S. Government has taken some steps to share intelligence information on PRC campaigns to target critical infrastructure. Notably, in July 2021, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) released information on Chinese state-sponsored cyber intrusion campaigns, including tactics, techniques, and procedures (TTPs) that have been been employed

---

china-has-stopped-hacking-u-s-companies-official-says; "Update to the Report of the Commission on the Theft of American Intellectual Property," The National Bureau of Asian Research, February 2017, *https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report_Update.pdf.*

[11] Murray Scot Tanner, "Beijing's New National Intelligence Law: From Defense to Offense," Lawfare, July 20, 2017, *https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense.*

[12] Amy Burke et al., "The State of U.S. Science and Engineering 2022", National Science Board, January 18, 2022, *https://ncses.nsf.gov/pubs/nsb20221/u-s-and-global-research-and-development.*

[13] Remco Zwetsloot et al., "China is Fast Outpacing U.S. STEM PhD Growth," Center for Security and Emerging Technology, Georgetown University, August 2021, *https://cset.georgetown.edu/publication/china-is-fast-outpacing-u-s-stem-phd-growth/.*

[14] "Military and Security Developments Involving the People's Republic of China 2020: Annual Report to Congress," U.S. Department of Defense, *https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF.*

[15] "Military and Security Developments Involving the People's Republic of China 2020: Annual Report to Congress," U.S. Department of Defense, *https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF;* "Annual Threat Assessment of the U.S. Intelligence Community," Office of the Director of National Intelligence, February 2022, *https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf.*

[16] "The Timeline and Events of the February 2021 Texas Electric Grid Blackouts," The University of Texas at Austin's Energy Institute, July 2021, *https://energy.utexas.edu/research/ercot-blackout-2021.*

with the aim of "holding U.S. pipeline infrastructure at risk" through physical damage to pipelines or disruption of pipeline operations.[17]

INFLUENCE ACTIVITIES

The U.S. homeland is within reach of the PRC's influence activities. The PRC "conducts influence operations that target media organizations, business, academic, cultural institutions, and policy communities of the United States."[18] As part of its "three warfares" concept, the PRC seeks to leverage psychological warfare, public opinion warfare, and legal warfare to influence decision makers, shape public narratives, spread disinformation, and advance its interests.

Examples include TikTok, with over 100 million U.S. users that U.S. intelligence officials caution can be influenced by CCP-driven manipulation of its algorithms. They also include Operation Fox Hunt, where CCP-directed individuals spy on U.S.-based pro-democracy activists, intimidate Chinese and Chinese-American students at U.S. universities, and pressure individuals in the United States to return to China, including by threatening family members.[19] In contrast, Chinese state-run media characterize Fox Hunt as, "targeting suspected economic criminals, many of them corrupt officials."[20]

The PRC also exerts influence through its Belt and Road Initiative (BRI), including its Digital Silk Road (DSR) initiative, which involves a strategy of exporting terrestrial infrastructure, information and communications technology, and other high technology areas.[21] This global influence directly impacts U.S. businesses and U.S. security interests here at home.

One acute area of competition is in commercial satellite communications, which CSIS recently examined in a study on low Earth orbit (LEO) broadband networks.[22] These space-based constellations, such as SpaceX's Starlink and Amazon's Project Kuiper, offer a compelling solution for bridging the digital divide, specifically for rural and underserved communities, as nearly 40 percent of the world's population, and 28 percent of rural households in America remain unconnected. However, with its heavy economic presence in many BRI countries, China is positioned to negotiate concessions for its telecommunications and satellite broadband services, while discouraging the adoption of U.S. commercial services.

Further expansion of its telecommunications services could boost Beijing's presence in foreign terrestrial networks. This would provide the CCP with remote access to route data back to Beijing (as was reportedly done to the African Union Headquarters, whose network infrastructure was built and operated by Chinese entities), grant it extensive surveillance and coercive powers, enable it to block internet access or censor information, and exert greater control over international data flows.[23]

While the U.S. Government has taken steps to ban Chinese telecommunications devices by Huawei, ZTE, and others, such high levels of dependence by other countries on Chinese-built and -operated digital infrastructure may lead to greater adoption of Chinese-crafted techno-authoritarian norms, standards, and data-governance practices.

RECOMMENDATIONS

Below are a few recommendations that I believe can help address these challenges.

---

[17] "Cybersecurity Advisory: Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013," Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, July 21, 2021, *https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-201a.*

[18] "Military and Security Developments Involving the People's Republic of China: Annual Report to Congress," U.S. Department of Defense, September 4, 2020, *https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.pdf.*

[19] Office of Public Affairs, "Eight Individuals Charged With Conspiring to Act as Illegal Agents of the People's Republic of China," Department of Justice, October 28, 2020, *https://www.justice.gov/opa/pr/eight-individuals-charged-conspiring-act-illegal-agents-people-s-republic-china.*

[20] Cao Yin, "Success of Fox Hunt campaign continues," China Daily, November 5, 2015, *http://www.chinadaily.com.cn/china/2015-11/05/contentx22375920.htm.*

[21] Makena Young and Akhil Thadani, "Low Orbit, High Stakes: All in on the LEO Broadband Competition," Center for Strategic and International Studies, December 14, 2022, *https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/221214__Young__Low-Orbit__High-Stakes.pdf?VersionId=vH1lp3dD7VcHGRcvuF9OdzV2WJc__KG42.*

[22] Ibid.

[23] Abdi Latif Dahir, "China 'Gifted' the African Union a Headquarters Building and Then Allegedly Bugged It for State Secrets," *Quartz,* January 30, 2018, *https://qz.com/africa/1192493/china-spied-on-african-union-headquarters-for-five-years.*

- *Expand education and awareness*.—This hearing is an important way to educate the American public that the threat posed by the CCP is not an abstract notion nor solely a distant military conflict that could take place across the Pacific. The American public and businesses need to understand the security and economic risks presented by the CCP and understand that they are a target of CCP influence and operations. Clearly, the U.S. homeland is not out of reach of Beijing's threats, with PRC malign activities and operations occurring here every day, below the level of armed conflict. The FBI now opens two new counterintelligence investigations nearly every day.[24] Should deterrence fail, the CCP is likely to ensure that the conflict is not contained in the Indo-Pacific but that it is felt in the United States, particularly through disruptions of critical infrastructure and influence campaigns.[25]
- *Deepen threat sharing with the private sector*.—Building off CISA's work to-date, further expand threat intelligence sharing with the private sector. Encourage the downgrading of intelligence and provide security read-ons for business leaders across critical infrastructure sectors, e.g., energy, water, and financial services. Examples like the 2021 CISA advisory on oil and gas pipeline cyber threats, where specific TTPs attributable to Chinese state actors were shared, enable companies to better understand their vulnerabilities, the sophistication of adversary threats, and to make risk-informed decisions regarding protection and resiliency measures.
- *Transform counterintelligence (CI) and security missions*.—CI and security missions have traditionally involved manual, labor-intensive processes, from espionage casework to background investigations for security clearances to defense industry site visits for inspections. The scale of the CCP threat, the various methods it uses for acquiring technology, and the sheer volume of data that could be tapped into, necessitate adapting the tradecraft for these challenges. This includes incorporating new technologies, approaches to, and additional resources for the mission. For example, how can big data and artificial intelligence/machine learning (AI/ML) help identify supply chain vulnerabilities, monitor abnormal cyber activities, track foreign agents, and illuminate disinformation? How can CI analysts work with technology start-ups, on relevant business time lines, to prevent investment deals that involve adversarial capital?
- *Leverage technology innovation*.—Maintaining U.S. technological leadership means not just preventing the transfer of technology to the PRC, but also setting the conditions for our innovation sector to prosper and to stay ahead of the competition. We are in a period of rapid technological change, with the commercial sector leading in many areas of technological innovation. The Government should seek greater adoption and integration of commercial technologies to support mission needs, taking advantage of their speed, agility, and the private capital being invested in them.
- *Boost cooperation with allies and partners*.—Our alliances and partnerships are a competitive advantage and source of strength that the CCP does not have. In order to lessen this advantage, China is actively trying to divide and weaken U.S. alliances and partnerships.[26] Our technology is soft power for the United States, and technology cooperation can be a strong feature of these relationships while also bolstering our private-sector innovation base. But increasing cooperation will require revisiting U.S. technology control policies. We need to strike the right balance between protecting our sensitive technology, recognizing Beijing's extensive efforts to steal it, and enabling American companies to be the partner of choice for our allies and partners.
- *Continue investing in a strong defense*.—Continued investment in a strong defense is required to deter PRC aggression, build resiliency to attack, and ensure we have the trained people, posture, intelligence, weapon systems, and munitions to defend the United States and the American people.

Thank you again for your time today and I look forward to your questions.

---

[24] Remarks by FBI Director Christopher Wray at the Ronald Reagan Presidential Library and Museum, January 31, 2022, Simi Valley, CA, *https://www.fbi.gov/news/stories/director-wray-addresses-threats-posed-to-the-us-by-china-020122.*

[25] "Military and Security Developments Involving the People's Republic of China: Annual Report to Congress," U.S. Department of Defense, September 4, 2020, *https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.pdf.*

[26] Seth G. Jones, "Empty Bins in a Wartime Environment: The Challenge to the U.S. Defense Industrial Base," Center for Strategic and International Studies, January 23, 2023, *https://www.csis.org/analysis/empty-bins-wartime-environment-challenge-us-defense-industrial-base.*

Chairman PFLUGER. Thank you, Ms. Bingen.

The Chair now recognizes Dr. Jost for his opening statement.

STATEMENT OF TYLER JOST, PH.D., ASSISTANT PROFESSOR OF POLITICAL SCIENCE AND INTERNATIONAL AND PUBLIC AFFAIRS, BROWN UNIVERSITY

Mr. JOST. Chairman Pfluger, Ranking Member Magaziner, and distinguished Members of the subcommittee, thank you for the opportunity to testify today. It is really an honor to be with you.

My testimony is given as a scholar of Chinese foreign policy, and I emphasize this for two reasons. First, my role in academia is one of a researcher, not an administrator, and my testimony is not on behalf of or directly or indirectly associated with my employer. Second, as a former intelligence officer in the U.S. military, I am well aware that some of the most detailed reporting on topics as sensitive as homeland security remained classified. And as such, the testimony I am best positioned to offer pertains to the scholarly conclusions that can be drawn based upon publicly-available research.

My remarks today will focus on two areas. No. 1, the broader strategic context through which China's overseas intelligence collection and information campaigns should be viewed, and No. 2, what the publicly-available research to date can tell us about the scope and effectiveness of those campaigns.

The competition between the United States and China represents one of the defining international challenges of this century. But in my view, at the center of this critical problem rests two issues that most divide Washington and Beijing, the future of Taiwan and perceptions that the other side poses an existential threat to the stability of the domestic regime. Thus, while it is important to seriously evaluate the threats to the homeland posed by China, you should not distract attention from the issues that are likely to define the future of the global competition at their root.

China's overseas activities that emerge from this contemporary strategic context can be loosely divided into two categories. The first focuses on China's intelligence collection, which is well-documented. The recent incident in which a Chinese high-altitude balloon traversed American airspace illustrates in vivid fashion that China is willing to assume risks in order to gather data against American targets. In parallel to intelligence collection, China engages in operations to disseminate information to foreign audiences. To date, the bulk of these activities are aimed at shaping global public opinion. In simplest terms, China presents foreign citizens with information with a hope that it will shape the target's attitudes and perhaps their behavior. These efforts to shape foreign public opinion through party propaganda are real, and their scope is broad. But there are a few comparatively few studies that apply validated research methods for estimating the causal effect that exposure to such messages have on foreign audiences. In addition, trends in the global public opinion should provide some comfort. If one judges the effectiveness of China's public diplomacy campaign based solely on China's approval rating in foreign countries, the effort has, at least to date, been a failure.

Finally, what evidence we do have suggests there are several reasons why these operations might actually prove to be less effective than some of us might fear. By emphasizing gaps in public knowledge, I am not suggesting that we can dismiss potential threats that China poses to the U.S. homeland. The fact that China has demonstrated its intent to engage in both intelligence collection and efforts to shape foreign public opinion, coupled with the competitive nature of the bilateral relationship broadly, is sufficient cause for serious attention. Rather, my hope is that emphasizing what we do and do not yet know can illuminate policy recommendations which are detailed in my written testimony.

Allow me to briefly summarize them here.

First, the U.S. Government should devote resources toward publicly-available research that fills in gaps in our knowledge regarding China's activities abroad.

Second, the U.S. Government should use diplomatic channels to reestablish opportunities for American researchers to better understand the Chinese political system and do so in ways that they feel protected from potential exploitation and detainment by the Chinese authorities.

Third, the U.S. Government needs to better disclose its understanding of the threats that China poses to homeland security. Specifically, it needs to provide citizens with more data about the different risks that American citizens assume when they use foreign technologies.

Thank you very much for your time, and I look forward to answering your questions.

[The prepared statement of Mr. Jost follows:]

PREPARED STATEMENT OF TYLER JOST

MARCH 9, 2023

Chairman Pfluger, Ranking Member Magaziner, and distinguished Members of the committee, thank you for the opportunity to testify before the Subcommittee on Counterterrorism, Law Enforcement, and Intelligence. My remarks today will focus on two areas: (1) The broader strategic context through which China's overseas intelligence collection and information campaigns should be viewed; and (2) what the currently available evidence can tell us about the scope and effectiveness of these campaigns.

My testimony today is given as a scholar of Chinese foreign policy and U.S.-China relations. I emphasize this for two reasons. First, my role in academia is one of a researcher, rather than an administrator. My testimony is not on behalf of or directly or indirectly associated with my employer. Second, as former intelligence officer in the U.S. military, I am well aware that some of the most detailed reporting on a topic as sensitive as homeland security remains classified. As such, the testimony I am best positioned to offer pertains to the scholarly conclusions that can be drawn based on publicly-available research.

To summarize, my assessment regarding China's threat to the U.S. homeland is three-fold. First, it is clear that China is interested in using its capabilities to gather information and promote narratives that are consistent with its interests. Second, publicly-available research provides inconclusive evidence regarding the effectiveness of China's operations, particularly those aimed at shaping global public opinion. Third, the U.S. Government should consider devoting more resources toward research that can more precisely and conclusively assess the level of threat posed by China's activities in the United States. The absence of authoritative and publicly-available evidence does not necessarily confirm the ineffectiveness of China's actions, but leaves observers without a clear picture of how to rank the severity of these threats in comparison to other aspects of American foreign policy toward China, such as the emerging bilateral security competition and the possibility of future military conflict.

THE CONTEXT OF U.S.-CHINA STRATEGIC COMPETITION

The competition between the United States and China represents one of the defining international challenges of this century. In my view, the central problem of the U.S.-China relationship continues to be how to manage the two issues that most divide Washington and Beijing.

The first is that the United States and China have potentially irreconcilable differences over Taiwan. These differences have been effectively managed for decades, but both sides are increasingly apprehensive about the ability to maintain the status quo. There is healthy debate among scholars as to what is driving recent apprehensions. Some emphasize changes to the balance of power.[1] Others emphasize the difficulties of credible assurance, which might cause Beijing to feel it has no choice but to take military action.[2]

These dynamics are primed to put the United States in a difficult position. If the United States hopes to deter future military action against Taiwan, it will need to do one of the following: (1) Match Chinese capabilities in the region to keep the costs of conflict prohibitively high; (2) reassure Beijing that the United States and Taiwan will not change the status quo, assuming that such concerns are central to Beijing's decision making; or (3) some combination of the two. If the United States does not manage this aspect of the bilateral relationship effectively, deterrence may fail. The consequences of such a conflict would be devastating, not only in terms of the human and economic costs imparted on both sides, but also in terms of the reputational toll to the credibility of American strategic judgment if it fails to win. The stakes of successfully navigating this issue could not be higher.

The second issue is that the United States and China eye each other's domestic institutions with suspicion. Chinese decision makers think about national security as the security of the regime.[3] From the perspective of Beijing's leaders, one of the most formative events in the country's history was the collapse of communist regimes in Eastern Europe, followed by the Soviet Union, which demonstrated the possibility of a similar fate for the Chinese Communist Party.[4] Beijing views some, although not all, of the global rules and norms that emerged after the cold war as threats to the regime's stability, particularly those regarding the effectiveness and appropriateness of democratic institutions.[5]

Thus, while it is important to seriously evaluate the threats that China poses to the homeland, these inquiries should not distract attention from the issues that are likely to be central in the global competition—and will greatly shape whether the two sides end up in what could be the most costly and dangerous conflict between two major powers since 1945.

CCP ACTIVITIES ABROAD

It is helpful to view China's activities toward the U.S. homeland in this context. Like many countries, China seeks to gain advantages over states with whom it has differences in order to improve its bargaining power. The more intelligence that China is able to collect regarding foreign military capabilities, for instance, the more they might be able to emulate those capabilities within their own military portfolio, with an eye toward bargaining hard for the two priority issues discussed above.

China's overseas activities that emerge from this strategic context can be loosely divided into two categories. The first focuses on intelligence collection. The second focuses on information distribution. It is important to distinguish these two areas, because each is quite different in terms of the nature, scope, and potential to impart costs on the United States.

---

[1] Heginbotham, Eric, et al. *The US-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996–2017.* Santa Monica: Rand Corporation, 2015; Kastner, Scott L. "Is the Taiwan Strait Still a Flash Point? Rethinking the prospects for armed conflict between China and Taiwan." *International Security* 40.3 (2015): 54–92.

[2] Blanchette, Jude and Ryan Hass. "The Taiwan Long Game: Why the Best Solution Is No Solution." *Foreign Affairs.* 102.1 (2023): 102–114; Weiss, Jessica Chen. "The U.S. Should Deter—Not Provoke—Beijing over Taiwan." *The Washington Post.* February 20, 2023.

[3] Weiss, Jessica Chen. "A World Safe for Autocracy?" *Foreign Affairs* 98.4 (2019): 92–108; Greitens, Sheena Chestnut. "Internal Security & Grand Strategy: China's Approach to National Security Under Xi Jinping." *Statement before the US-China Economic and Security Review Commission, Hearing on US-China Relations at the Chinese Communist Party's Centennial (2021).*

[4] Sarotte, Mary Elise. "China's Fear of Contagion: Tiananmen Square and the Power of the European Example." *International Security* 37.2 (2012): 156–182; Gewirtz, Julian. *Never Turn Back: China and the Forbidden History of the 1980's.* Cambridge: Harvard University Press, 2022.

[5] Johnston, Alastair Iain. "China in a World of Orders: Rethinking Compliance and Challenge in Beijing's International Relations." *International Security* 44.2 (2019): 9–60.

Intelligence Collection

In terms of intelligence collection, it is well-documented that China is gathering data in order to improve its military capacity, provide insight into U.S. decision-making processes, and potentially gain a tactical advantage over the United States in the event of a future conflict. The recent incident in which a Chinese high-altitude balloon traversed American airspace illustrates in vivid fashion that China is willing to assume risks in order to gather data against U.S. targets.

The fact that this event occurred shortly before Secretary of State Anthony Blinken's planned diplomatic visit to China is noteworthy. If recent reporting from the U.S. Department of Defense stating that Xi Jinping was unaware of the timing of this particular mission is true, it suggests that Beijing may have delegated decision making regarding tactical execution of these operations to bureaucratic stakeholders who had limited understanding of how the disclosure of such an intelligence mission could shape China's other strategic priorities.[6] Such a posture could imply that Beijing has a high level of risk tolerance in its intelligence collection.

There are equally concerning aspects the security of personal data. Investigations into Chinese intelligence have long noted Beijing's interest in collecting data on foreign citizens, demonstrated by the 2015 Office of Personnel Management data breach and the 2017 cyber espionage operation against Equifax.[7] These events, coupled with the technical realities of digital technologies, illustrate that Government communications and the privacy of American citizens may both potentially be compromised through the use of foreign hardware and software.

It seems more than plausible that China's defense espionage campaign has contributed to its ability to develop more advanced military technologies, which could shape its ability to fight and win a war in the Asia-Pacific region.[8] There is less publicly-available reporting to document whether these intelligence operations, which have been successful at the collection phase, have also been effective in advancing Beijing's broader diplomatic, economic, and security goals beyond defense production.

Simply collecting data, particularly in large quantities, is insufficient to help decision makers achieve their goals.[9] I am unaware of any publicly-available study that has been able to document such a connection in the recent past. Recognizing this gap in our understanding is important, not only because it should drive the United States' own intelligence collection priorities, but also because we should recognize the challenges Beijing will face in effectively managing such large amounts of data.

Shaping Global Public Opinion

In parallel to intelligence collection, China engages in operations to disseminate information to foreign audiences. To date, the bulk of these activities are aimed at shaping global public opinion.[10] In simplest terms, China presents foreign citizens with information with the hope that it will shape the target's attitudes and, possibly, behavior. Perhaps the most concerning facet of these activities occurred last fall, when Meta and Google each reported that China-based groups had disseminated political content prior to the 2022 midterm elections.[11]

The idea of information control and propaganda is deeply embedded in the Chinese Communist Party's institutions—and it is easy to see how this would naturally spill over into efforts to shape public opinion abroad.[12] They also tie into the second core issue motivating the bilateral competition: China's concern about regime survival and the threat that a lack of international status might have on the Party's continued ability to rule. Furthermore, it is plausible that China genuinely believes

---

[6] Eric Schmitt and Zach Montague. "Balloon Crisis Highlighted a Split in China's Leadership, Pentagon Official Says," *The New York Times,* February 17, 2023.

[7] David E. Sanger and Julie Hirschfeld Davis. "Hacking Linked to China Exposes Millions of U.S. Workers," *The New York Times,* June 4, 2015; Katie Benner. "U.S. Charges Chinese Military Officers in 2017 Equifax Hacking," *The New York Times,* May 7, 2020.

[8] Department of Defense. *Report on Military and Security Developments Involving the People's Republic of China,* 2022, 147, 153.

[9] Wohlstetter, Roberta. *Pearl Harbor: Warning and Decision.* Stanford: Stanford University Press, 1962.

[10] Diamond, Larry, and Orville Schell, eds. *Chinese Influence and American Interests: Promoting Constructive Vigilance.* Stanford: Hoover Institution Press, 2018; Brazys, Samuel, and Alexander Dukalskis. "China's Message Machine." *Journal of Democracy* 31.4 (2020): 59–73.

[11] Kurlantzick, Joshua. "China's Growing Attempts to Influence U.S. Politics." *Council on Foreign Relations,* October 31, 2022.

[12] King, Gary, Jennifer Pan, and Margaret E. Roberts. "How Censorship in China Allows Government Criticism But Silences Collective Expression." *American Political Science Review* 107.2 (2013): 326–343; Roberts, Margaret E. *Censored: Distraction and Diversion Inside China's Great Firewall.* Princeton: Princeton University Press, 2018.

that the rest of the world misunderstands it—and that these misunderstandings can be rectified through methods similar to those it employs at home.

These efforts to shape foreign public opinion through party propaganda are real and their scope broad. It is estimated that China spends approximately $8 billion on public diplomacy efforts alone.[13] To date, however, there is limited publicly-available research documenting whether China's operations to shape foreign attitudes have been effective. For example, China Global Television Network (CGTN), a broadcasting company affiliated with the Chinese state, is actively disseminating China's public messaging world-wide.[14] But there are few studies that apply validated research methods for estimating the causal effect of exposure to such messages on public opinion.

The available evidence suggests several reasons why these operations might actually prove to be less effective than we might fear. Broadly, efforts to shape foreign public opinion do not always work out the way that states hope. Some research suggests, for example, that salient components of China's public diplomacy initiatives do not improve foreign attitudes toward China.[15] Scholars at Yale University have found that Twitter messaging by Chinese diplomats were only able to positively shape perceptions of China when the message was framed in positive terms. When Chinese diplomats instead resorted to nationalist messages, often termed "Wolf Warrior" diplomacy, Twitter messages instead had a negative effect on foreign public opinion.[16]

Some of the best available evidence on the domestic effects of China's propaganda also suggests that such messages do not necessarily operate as one might think. Several experimental studies have found that propaganda inside China can backfire, causing Chinese citizens to adopt less favorable views toward the government.[17] It is worth noting, however, that these studies have also found that Chinese propaganda is effective in signaling the strength of the state. That is, propaganda does not always change political attitudes, but it does remind citizens of the CCP's ability to coerce. Other studies suggest that Chinese domestic propaganda can be effective when it is able to emotionally resonate with its citizens, such as through nationalistic narratives recounting past wars in a positive light.[18] However, it is not yet clear that these same methods can be effectively applied in foreign countries.

One possible reason that Chinese propaganda could fail to sway global public opinion as intended is that foreign audiences may ascribe malign intentions to foreign governments, especially China. Research suggests that the ability to sway political attitudes depends in part on whether a target audience believes that what social scientists term the "cue-giver" (in this case China) has the audience's best interests at heart.[19] To illustrate this point in more familiar terms, consider how an American voter may be more likely to update their political attitudes when they receive a message from a co-partisan than when they receive one from a member of another party. There is an intuitive logic behind this: people make general judgments about who they deem trustworthy (e.g., one who shares the same basic political values) and then prioritize messages from these sources as they wade through the vast amounts of information to which they are exposed in daily life.[20]

Applying this intuition to China's public messaging campaigns would suggest that American citizens may be predisposed to severely discount or even completely discard messages received from Chinese propaganda outlets, provided that their baseline trust of such sources is low and they are able to accurately identify the creator of the content. Some studies of public diplomacy in other country contexts, usually focusing on the ability of American officials to shape global public opinion, are con-

---

[13] Martin, Peter. *China's Civilian Army: The Making of Wolf Warrior Diplomacy.* New York: Oxford University Press, 2021, 213.

[14] Diamond and Schell 2018, 103.

[15] Green-Riley, Naima. *How States Win Friends and Influence People Overseas: The Micro-Foundations of U.S. and Chinese Public Diplomacy* (PhD Thesis). Harvard Department of Government.

[16] Mattingly, Daniel C., and James Sundquist. "When Does Public Diplomacy Work? Evidence from China's 'Wolf Warrior' Diplomats." *Political Science Research and Methods* (2022).

[17] Huang, Haifeng. "Propaganda as Signaling." *Comparative Politics* 47.4 (2015); Huang, Haifeng. "The Pathology of Hard Propaganda." *The Journal of Politics* 80.3 (2018): 1034–1038.

[18] Mattingly, Daniel C., and Elaine Yao. "How Soft Propaganda Persuades." *Comparative Political Studies* 55.9 (2022): 1569–1594.

[19] Lupia, Arthur, Mathew D. McCubbins, and Lupia Arthur. *The Democratic Dilemma: Can Citizens Learn What They Need to Know?* New York: Cambridge University Press, 1998.

[20] Druckman, James N. "On the Limits of Framing Effects: Who Can Frame?" *The Journal of Politics* 63.4 (2001): 1041–1066.

gruent with this conclusion.[21] Other experimental studies find a similar effect with regard to American perceptions of foreign public diplomacy as well.[22]

In addition, trends in global public opinion should provide some comfort. If one judges the effectiveness of China's public diplomacy campaign based solely on China's approval rating in foreign countries, the effort has been a catastrophic failure. This is true not only in the United States, but in Japan, Australia, South Korea, and much of Europe as well. Across these countries, China is less well-trusted today that it was 10 years ago. China may be attempting to win hearts and minds globally, but they have not succeeded in many contexts.[23]

If China's public diplomacy campaign has backfired (i.e., the effect of the program has been in the opposite direction than Beijing intended), it would be unsurprising not only for the reasons cited above, but also because China has often miscalculated in its foreign policy decision making. For example, one scholar at the University of Southern California has shown that China's attempts to use economic statecraft to advance its relationships with other countries are often ineffective, particularly when the target state is a democracy.[24] Several of China's international security crises, ranging from the 1969 Sino-Soviet Border Conflict to the 1979 Sino-Vietnamese War, failed to achieve many of the strategic objectives toward which Beijing's use of force was aimed.[25] In short, Beijing's ability to get what it wants in world politics is far from unchecked.

Three points of caution are merited with regard to these data. First, the aggregate relationship between a more active public diplomacy campaign and less favorable public opinion toward China is confounded by other events, particularly the COVID–19 pandemic. This implies that China could be able to shape public opinion abroad more effectively as the pandemic ends. Second, while the decline in public opinion toward China is well-documented in developed countries, these polls often do not include countries from the Global South, which may be a priority for Chinese decision makers. Third, none of the research discussed above addresses the possibility that China could use fake on-line profiles to hide the source of China's messaging from foreign audiences.

POLICY RECOMMENDATIONS

By emphasizing gaps in public knowledge, I am not suggesting that we can dismiss the potential threats that China poses to the U.S. homeland. The fact that China has demonstrated its intent to engage in both intelligence collection and efforts to shape foreign public opinion, coupled with the competitive nature of the bilateral relationship, is sufficient cause for serious attention. Rather, my hope is that emphasizing what we do and do not yet know can illuminate recommendations for policy.

1. Fund Social Science Research on the Topic.—The U.S. Government should devote resources toward publicly-accessible research that fills gaps in our knowledge regarding China's activities abroad. The social sciences are in the early stages of understanding whether and how new types of social media, sometimes employed by foreign actors, can shape public opinion. It is worth emphasizing again that existing research is insufficient to determine how costly these new technologies will be to the U.S. homeland. Yet, U.S. policy makers should be open to the possibility that better research on the topic would, for example, lead to the conclusion that China's capacity to shape American public opinion is low—and the broader conclusion that U.S. efforts might be better directed toward other parts of the competitive relationship.

2. Protect U.S. Researchers in China.—The U.S. Government should work to ensure that American scholars who choose to conduct field research in China are protected.[26] Our ability to answer many of the most pressing questions regarding the future of the competition between the United States and China is increasingly limited by restrictions on American scholars by the Chinese govern-

---

[21] Goldsmith, Benjamin E., and Yusaku Horiuchi. "Spinning the Globe? US Public Diplomacy and Foreign Public Opinion." *The Journal of Politics* 71.3 (2009): 863–875.

[22] Rhee, Kasey, Charles Crabtree, and Yusaku Horiuchi. "Perceived Motives of Public Diplomacy Influence Foreign Public Opinion." *Political Behavior* (2023).

[23] Silver, Laura, Christine Huang and Laura Clancy. "How Global Public Opinion of China Has Shifted in the Xi Era." *Pew Research Center,* September 28, 2022.

[24] Wong, Audrye. "How Not to Win Allies and Influence Geopolitics: China's Self-Defeating Economic Statecraft," *Foreign Affairs.* 100.3 (2021), 44–53.

[25] Jost, Tyler. "Authoritarian Advisers: Institutional Origins of Miscalculation in China's International Security Crises," *International Security,* forthcoming.

[26] For an overview, see Greitens, Sheena Chestnut, and Rory Truex. "Repressive Experiences Among China Scholars: New Evidence from Survey Data." *The China Quarterly* 242 (2020): 349–375.

ment. The U.S. Government should use diplomatic channels to reestablish opportunities for American researchers to study the Chinese political system while feeling protected from potential exploitation and detainment by Chinese authorities.

3. Build Evidence-Based Public Awareness.—The U.S. Government needs to explain the threats that China poses the privacy of their data to the American public. Specifically, it needs to provide more detailed explanations of the different risks that American citizens assume when they use foreign and domestic technologies. This may seem obvious to individuals who have served in government, but the social appeal of these technologies will raise the burden of proof for U.S. policy makers to convince American citizens.

Chairman PFLUGER. Thank you, Dr. Jost.

Members will now be recognized in order of seniority, alternating between Republican and Democrat for 5 minutes of questioning. It is my hope today that we will be able to go through maybe two rounds of questioning.

The Chair now recognizes myself for 5 minutes of questioning.

I think what we heard there is just an incredible breadth of knowledge and experience about what the Chinese Communist Party has been doing, you know, for several decades; what they are currently doing; and the threats that, as that wake-up call moment happened several weeks ago with the Chinese surveillance balloon, that it is incumbent upon us to really start uncovering these threats and focusing on them. Quite honestly, from what we have heard from this panel—thank you for all of your opening statements—we could have several hearings on the individual subjects. But appreciate the time here.

I will start with Mr. Evanina.

When you look at the ownership of property in the United States and we go back, PRC-based ownership of U.S. farmland in the last 20 years has jumped from about $81 million in 2010 to $1.9 billion at the end of 2021. Moreover, I think it is widely reported that a lot of the PRC or PRC-linked ownership is adjacent to very sensitive facilities, government facilities, military facilities in the United States. Can you provide insight as to why that is, what the goal is, and what they are doing with those lands?

Mr. EVANINA. Thanks for the question, Mr. Chairman.

I'm going to try really hard to stay in the unclassified realm here, but it's a comprehensive strategic plan that goes back about a decade to the CCP's plans and intentions and incorporates multifaceted intelligence apparatus, both the MSS and the PLA. It starts what I would call and phrase outside the fence line of DoD facilities. That began with the Huawei cell tower capabilities, tracking and being able to monitor not only trip movements, but weapon silos and other areas, the strategic purchases of businesses outside of not only military bases but military residential areas, the influence of the Chinese to be able to do software and malware manipulation, penetration on electrical grids and power stations outside of the military bases.

I think the next aspect is exactly what you referenced, right? What is the next thing that the Communist Party of China and Russia, for that matter, are looking to exploit outside the fence line of U.S. military bases? That includes land purchases. I think when you look at all the land that not only the Chinese Communist Party and their proxies have purchased, you are going to find a strategic military base and/or subterrestrial things in the ground

as well as energy issues to the military base. Also we look at the balloon we just saw, very similar trajectory to those areas. So it's a comprehensive strategic plan that you see from the Communist Party of China.

Chairman PFLUGER. Do you think there was coordination between—staying in the unclassified—I mean the lands that the balloon flew over, purchases that we have seen, I mean could there be coordination either now or in the future?

Mr. EVANINA. Absolutely. There's nothing done by the Communist Party of China that does not have strategic entity or coordination. I think we'll see in the future, if it's declassified, what some of the things the balloon was surveilling and or potentially doing more surveillance too.

Chairman PFLUGER. Thank you.

General Guastella, thanks for the testimony. You know, the threats that you mentioned that you are very worried about and concerned about, I mean what keeps you up at night on the air power threats and what needs to happen resource-wise, specifically here or at NORTHCOM in order to identify, deter, detect, and defeat?

General GUASTELLA. Thank you, Chairman.

What keeps me up at night is the age and the capabilities of our existing air and space forces.

You know, for 20 years we have been engaged in the very land-centric campaigns in the Middle East. We have been doing counter-insurgency, counter-violent extremists, counterterrorism, all important for our Nation. But during that 20 years, we did not invest in air and space forces to the extent we needed to. So we are left with that old fleet that I described before. You know, a 30-year-old fighter can do fine providing close air support in Iraq or Afghanistan against a low-end threat, but it is not going to survive very well against—and it is not going to survive in China fight and moreso it doesn't deter China. So we have to realize the investment that is needed in the air and space domain has been neglected and we have to get after it for the exact reasons that's been described by our expert panelists on China.

That's what keeps me up at night.

Chairman PFLUGER. When you look at the threats that are being posed, hypersonics, the ranges that are increasing, the ability to reach out and touch us, how important is NORAD, the joint air power enterprise to the defense of our homeland?

General GUASTELLA. You know, NORAD, the National Defense Strategy, two of them now in a row, have said that homeland defense is the No. 1 priority. Problem is we haven't resourced it to that extent that our words say. The commanders of the NORAD have asked for modernization of radars for years now and have not gotten it. That would have helped us detect those balloons sooner. Then the aging fighters. You know, almost every major metropolitan city in America is defended by our National Guard fighters that are getting older and older. They don't have the capabilities, the radars that they need not only for the balloons, but the radars they need for the real threat, which would be a cruise missile attack against our homeland.

So that is what concerns me.

Chairman PFLUGER. Thank you.

My time has expired. I yield back.

I now recognize the Ranking Member.

Mr. MAGAZINER. Thank you, Chairman.

It is clear that the Chinese Communist Party is taking a whole-of-government approach to advancing its ambitions at the expense of U.S. and democratic interests, and therefore we must take a whole-of-government approach to meeting that threat. So that covers homeland security, defense, commerce, State Department, et cetera.

So I want to focus on the homeland realm. Dr. Jost, can you expand on the methods that the CCP is using to influence public opinion both here at home in the United States and globally, and what more we could be doing to measure their efforts and to mitigate their success?

Mr. JOST. Sure. Thank you very much for the question.

The bulk to date of China's influence operations, both in the United States and abroad, are focused on what you might say are winning friends and influencing people. Right. This is coming directly from Xi Jinping, who has directed the Party's apparatus that has deep roots in propaganda to leverage those capabilities in order to tell China's story well to the world. It is interesting to think about the ways in which China's institutions domestically are sort-of naturally positioned to make that transition from a domestic-based propaganda machine to an international one. If one thinks from the perspective of the Chinese Communist Party, from their perspective domestic propaganda has worked thus far in keeping the CCP in power. Those capabilities and organizations exist, and it is easy to see how they would assume that those same types of propaganda would work in foreign audiences.

To date, however, as I emphasized in my written testimony, we don't necessarily have the best evidence to judge whether or not these propaganda efforts outside of Chinese borders have been effective. As I mentioned in the opening statement, we do know that global public opinion toward China, particularly in the United States and the countries with whom we share closest interests, has declined substantially in the past few years, which would actually suggest that from a certain perspective, the propaganda doesn't necessarily work as well as the CCP would hope.

That being said, there is a multitude of things that are confounding that relationship of course. Like the fact that there has been a global pandemic, the fact that it could be working in certain areas and not others. Certain framings that the Chinese Communist Party and its diplomats use are more effective than others. That is one of the reasons why I think there needs to be more research on this matter and something the U.S. Government can certainly help with.

Mr. MAGAZINER. Thank you.

Mr. Evanina, in your written testimony on the threat of corporate espionage and the theft of intellectual property, you recommended the creation of an economic threat intelligence agency to assist U.S. companies in protecting themselves against corporate espionage. Can you expand on how that should be structured to be most effective if we were to do it?

Mr. EVANINA. Thank you, Ranking Member.

I recommended an entity similar to the FS–ISAC that is specifically geared toward the economic awareness and understanding of IP and trade secret theft and emerging of not only the thought process but the ideation, but also the law that governs our patent processes and our IP theft around the world and to mirror what the Communist Party are doing around the world and then educate our American businesses, the general counsels, the people that do law for them, outside counsel, to understand what it looks like when you are about to be stolen and robbed of IP theft and to be able to provide that real-time actual intelligence from the intelligence community, DHS, and Commerce and Treasury to businesses who are not only at risk, but in the process. Because once it happens, it's too late, the data's already gone. The Government needs to be more forward-leaning and left of boom.

Mr. MAGAZINER. Thank you.

I found that very interesting. So perhaps as a follow-up, after this hearing, you can send us some recommendations in more detail about where it should be housed, how it should be staffed, which agencies should be involved? Because I think that is a very interesting recommendation.

Mr. EVANINA. Yes, sir.

Mr. MAGAZINER. I yield back.

Chairman PFLUGER. The gentleman yields.

The Chair now recognizes the gentleman from New York, Mr. D'Esposito.

Mr. D'ESPOSITO Thank you, Mr. Chairman. Thank you all.

So dozens of demonstrators protested outside of a building in New York City's Chinatown last month. The building, which is owned by the Chang Le Association, operates what they call a service station, and that they are accused of operating a CCP police station that allegedly conducts surveillance and intimidates CCP descendants and activists. Like the recent incident with the Chinese surveillance balloon, this station could be the latest CCP action that violates U.S. sovereignty and poses a threat to national security. It has been reported that there is over 100 of these offices around the world.

Mr. Evanina, please describe your concerns surrounding this potential CCP police station in terms of counterintelligence threats and the safety of Americans.

Mr. EVANINA. Thank you, Congressman.

I think when you look at that specific issue in New York City and the subsequent search by Department of Justice and FBI, which is a high threshold to obtain, it's a manifestation of the strategic plan of the Communist Party of China to not only influence, manipulate their own diaspora here in the United States, but provide an intimidation factor. I would say that this issue in New York and the search of that domestic police station is in part and partnership with their Operation Fox Hunt that my colleague Ms. Bingen talked about, which is an international program, but very, very aggressive in the United States, to surveil and try to rendition Chinese diaspora here who are anti-Xi regime. They have been very successful at it. The fact that this happens on our American soil to me, is unacceptable.

Mr. D'ESPOSITO I agree.

So it is been reported that there is over 100 throughout the world. Do we know how many are actually on U.S. soil?

Mr. EVANINA. I do not, but I'm pretty confident our law enforcement, both at the State, local, and Federal level, are pretty aware of that.

Mr. D'ESPOSITO Thank you, Mr. Chairman. I yield back.

Chairman PFLUGER. The gentleman yields.

I now recognize my good friend, the gentleman from California, Mr. Correa.

Mr. CORREA. Mr. Chairman from Texas, thank you very much.

I have been sitting in this committee for a number of years. Cyber, big issue continues to be a big issue. A number of testimonies ago, we heard that Russians have essentially penetrated most of our infrastructure, just like we penetrated most of their infrastructure. So we have a stand-off, so to speak. Action by either side is too expensive, so to speak, in terms of the damage. Now we have a situation internationally, a geopolitical realignment, where Russia and China are beginning to work much more collaboratively.

My question, common thought, first of all, Mr. Evanina, how do you see this, given that China's foreign minister recently said, essentially warned us of conflict and confrontation in the United States? How do you see this evolution in terms of multiplier effect of a threat on the United States, Russia and China working together? How real is that? What is the potential for the future of continued collaboration to really challenge the United States in ways we have not envisioned in the past?

Thank you.

Mr. EVANINA. Mr. Congressman, I concur with your statement, and I think it is a very concerning issue when two nation-states who don't like each other are emerging against one common enemy, the United States.

Geopolitically, diplomatically——

Mr. CORREA. You are saying that enemy of an enemy is my friend? Is that the situation?

Mr. EVANINA. I wasn't going to say that, but it—better you said it. Yes, correct. I think when you look at I will stick in my lane here from—you mentioned the Russians' penetration to our systems, both IT and OT, SCADA, ICS systems here in the United States, probably predates the Communist Party of China, but I'm pretty confident the Communist Party of China has either duplicated those penetrations or ridden along those. I think the sharing of the intelligence services between Vladimir Putin and Russia and the Communist Party is probably the most problematic for me as what they see, because that's the most invisible part of that threat.

Mr. CORREA. I think that right now we still have an edge when it comes to cyber. Two or 3 years, maybe.

So I often think of defense, a good offense is the best defense you can have. So, if I may, what would you recommend moving forward would it be the best way to counter these unprecedented challenges that a country has?

Mr. EVANINA. Congressman, I think you make a good point, and it's probably important that we reiterate the fact that as much as

what you're hearing here is depressing, demoralizing, and it is a legitimate threat to our Nation, we must pause and remember that we have the most amazing military and intelligence and law enforcement capabilities the world has ever seen. The women and men of DoD and the intelligence community are phenomenal. Our capabilities are second-to-none in cyber, military apparatus, and intelligence. So Americans should go to sleep at night, be thankful of the fact that offensively, we've never seen anything better than we can do. Unfortunately, it's not public.

Mr. CORREA. Today. Today.

Mr. EVANINA. Yes, sir.

Mr. CORREA. Please continue. Didn't mean interrupt you.

Anybody else have comments, thoughts on my questions? Ma'am?

Ms. BINGEN. Congressman, if I might build off of that on cyber. When I look at the homeland, so much of our commerce and activity rights on commercial infrastructure, and building off of Mr. Evanina's point earlier, it's very important that the government figure out how to share threat intelligence information with the private sector with those oil, gas pipeline, energy, financial services sectors——

Mr. CORREA. In real time.

Ms. BINGEN. In real time. That's the key. If you're a business, you hear this top-level talk. But what is particularly valuable is figuring out a way to provide security read-ins to some of these business leaders, bring them into the tent, but also share specific tactic, techniques, procedures with them. It's one thing to hear about this general Chinese threat, it's another thing to hear, here are the tactics that they're using to go after you. Then you realize, holy crap, that's what is been happening in my network. Now, let me work with you to take some preventative measures.

Mr. CORREA. Thirty seconds—anybody else?

The Chair, I yield. Thank you very much.

Oh, please.

Mr. EVANINA. Just amplifying, Ms. Bingen, I would I would point to your question, sir, to the incredible success our Intelligence and Defense Department has had with Ukraine and preventing Russian cyber capabilities, not only in Ukraine and Europe and here in the United States as a category for us being ahead of others in the cyber space.

Mr. CORREA. Thank you for ending on a good, positive note.

Mr. CHAIR. I yield.

Chairman PFLUGER. The gentleman yields.

The Chair now recognizes the gentleman from Arizona, former Navy Seal, Mr. Crane.

Mr. CRANE. Thank you, Mr. Chairman. I appreciate it. Thank you guys for attending today. We appreciate it.

You know, it is not often up here that, you know, me and my colleagues on the other side of the aisle can agree upon something. So it is great to be in agreement on the threat that China is.

Obviously, the American people are watching and they are very concerned when they see spy balloons flying over the United States, farmland being bought up near—you know, farms, fentanyl all coming across our Southern Border—we know, you know, where the origin of a lot of that comes from—theft of intellectual property,

covering up the origins of COVID, Chinese police stations in some of our cities.

My first question is for you, Mr. Evanina. Did I pronounce that correctly? Sir, do you know what elite capture is?

Mr. EVANINA. Yes, sir.

Mr. CRANE. Can you for the panel, and for maybe some of those watching, can you describe what elite capture is, please?

Mr. EVANINA. Congressman, I can.

I would probably refer to some of the more better-informed experts here on that panel for that particular definition.

Mr. CRANE. OK. Is there anybody want to take a stab at it? Sir? Am I correct that you are an expert in counterintelligence, right?

Mr. EVANINA. Yes, sir.

Mr. CRANE. So can you just give me a really broad—doesn't have to be super specific. What is elite capture?

Mr. EVANINA. Yes, I think when you look at the capabilities and intent of our adversaries and our ability to be proactive and make an affirmative effort to capture telecommunications to humans, to technology in or at the battlefield or in the gray space, provides us the best venue or avenue for potential to win.

Mr. CRANE. OK. can you give me some examples of how that is often done, how that is carried out?

Mr. EVANINA. Sure. Well, first of all, I would say a lot of it's done with authorities that are granted to both NSA and the FBI overseas. Section 702, our abilities to capture telecommunications conversations to foreign adversaries, both the foreign-born, but are also overseas. That gives us leads and intentions on nefarious activities, both terrorism and counterintelligence espionage of those actors overseas that are, as Ms. Bingen said, riding on commercial capabilities that are around the world. That capability allows the United States to be able to pre-identify and do threaten warning to actors here in the United States, both from a systems data and people perspective.

Mr. CRANE. Would you say that it is accurate that foreign states and actors often try and compromise and corrupt leaders and officials within our own government? Would you say that that is a form of elite capture?

Mr. EVANINA. I would. It's done quite regularly for decades.

Mr. CRANE. Would you say that it is often true that family members are often used in these types of efforts to corrupt foreign leaders, officials?

Mr. EVANINA. Congressman, for the past decade, I have spent my time in three different organizations advising and informing Americans, Members of Congress about the threat to them as a person. It always starts with family members' utilization of mobile telephones.

Mr. CRANE. Thank you.

Sir, are you also aware of some of the reported business dealings of Hunter Biden with individuals linked to the Chinese Communist Party?

Mr. EVANINA. Only what I have seen in public reporting, sir.

Mr. CRANE. What did you think of the reporting that you read, sir?

Mr. EVANINA. I'm not sure I could actually opine of what I have read in public reporting, but I could say that the TTPs, of which foreign entities are utilized against Americans and family members, is tried and true and very predictable and reportable.

Mr. CRANE. Let me ask you a follow-on to that, sir. Did you find the reports—whether you believe them or not—did you find those reports concerning? Just with all of your knowledge in this space and how you have seen this type of thing play out in the past?

Mr. EVANINA. Yes, sir. I think when you look at what's been reported publicly about the potential tactics and techniques that were displayed publicly about the potential for penetration to a family member of the United States President is something that most intelligent services try to do regularly.

Mr. CRANE. Thank you. I yield back.

Chairman PFLUGER. The gentleman yields.

We will now proceed to second round of questions, and if we have other Members that had previous commitments that show up, then we will yield that initial question to them.

The Chair now recognizes myself for an additional round of 5 minutes of questions.

Ms. Bingen, thank you for your expertise and your testimony today. I would like to focus on that critical infrastructure piece and on what you said that the CCP is targeting critical infrastructure and that you fully anticipate that should a crisis—hopefully one does not happen—but should one happen and unfold, that Beijing would seek to disrupt the operations of critical infrastructure.

Then I was very intrigued by your discussion on sharing information with local State partners, law enforcement and otherwise. From the Colonial incident to now, have we as a Federal Government, and specifically within the Department of Homeland Security, can you give us your opinion of how we are sharing information? If that is effective and if our critical infrastructure, private partners—because most of that is owned by private industry,—are they ready for what is next should that Colonial incident happen again?

Ms. BINGEN. Chairman, thank you for that question. I think the Colonial incident, though not attributable to China, as the Government has come out and said, highlights the catastrophic impacts that can occur as a result of a potential attack against cybercritical infrastructure.

Your point is exactly right. From everything that I have seen previously, I would anticipate that as a crisis or conflict builds, that the CCP would seek to target critical infrastructure early on. There's a first mover advantage here, I would say, in terms of the kind of tools that they would seek to use to delay or to deter us or to potentially delay us.

On the point of information hearing, I think the success that I would point to is the summer of 2021. I thought CISA did a very good job bringing in oil and gas operators and providing very specific detail on the CCP cyber intrusion campaign, what specifically they were targeting, but equally important, how they were doing it, so the tactics, techniques, and procedures. But that is one sector. There are several different critical infrastructure sectors, and I think there's some very good intelligence information that the com-

munity has that they could provide, whether it be to financial services, the electrical grids, et cetera.

Chairman PFLUGER. Thank you very much.

I will turn to General Guastella. What is the impact of 8 days transit of a balloon, a surveillance balloon, you know, when we look at the fact that it transited and then, you know, got to the Atlantic Ocean before it was eventually shot down? What kind of message is that sending? What is the impact strategically?

General GUASTELLA. It's a significant wake-up call, like we discussed before, that an air vehicle could traverse American airspace for that long and be afforded the opportunity to collect that much information. You know, a balloon is up there around 12 miles up, satellites are 350 miles. So it's down in close or it hangs out for a long time. The potential for collection is significant. So, ideally, the thing would have been taken down prior to hitting U.S. airspace. But like I said, they exploited the scene. I don't think that'll happen again. We have to talk to Government officials about it. But we don't know until we fully exploit what was flown over, what they could have gotten, or what they got. But to me, it is a very grave violation of our sovereignty.

Chairman PFLUGER. Does something like that embolden the CCP and reduce our deterrence? Then what do we have to do to claw that back if it does?

General GUASTELLA. Absolutely anytime an authoritarian regime does something of that nature and we don't do anything about it, they will say, what can I get away with next? So we have to close this gap. We also have to demonstrate credible capability that we can affect them in some way of our choosing. I think that's important for us not only have the capability, but the will to do so. That's how you deal with the regime of that nature.

Chairman PFLUGER. Mr. Evanina, let's turn to the precursors that China produces that are then used in the production of fentanyl and the connection between the cartels that are, you know, taking these products that they are making fentanyl and then eventually getting it into the United States. Can you kind-of talk to your opinion as a former intelligence expert on that flow, what the CCP and the cartels are doing to work together, collude, and produce a very deadly substance?

Mr. EVANINA. Mr. Chairman, this is a very important topic, not only for this conversation, for our Nation. I think the recent reporting is that over 100,000 people have died in the last year, 12–15 months from fentanyl overdose. That's multiple times what happened on 9/11, right? So for our Nation to not look at fentanyl as a national epidemic that stems from a nation-state threat actor is probably unacceptable and we have to be more vigilant in what we do. We can map the production of the precursors from China to Mexico, to the drug gangs, to the American soil. It's clear and I know our intelligence and military apparatus are working hard to disrupt that, but it takes more than that to disrupt. There has to be a preemptive effort to put China on notice that this process of killing Americans must stop, and we have to look at it as a terrorism event.

Chairman PFLUGER. Thank you very much.

My time has expired.

The Chair yields back and now recognizes the Ranking Member, Mr. Magaziner.

Mr. MAGAZINER. Thank you very much.

Dr. Jost, in your testimony, you wrote that while the evidence shows that Chinese propaganda efforts in the United States and in other aligned countries do not show evidence of much success yet, we do not have as much data in the global south, in the emerging markets. We know that China is making big investments in many of these emerging countries for strategic reasons. I think that is very important for our work here in Congress because there is always a perennial debate on the level of foreign aid that we provide to those same nations.

So can you just expand a little bit on why this topic is important and what the tie is to the homeland security of the United States?

Mr. EVANINA. Thank you, sir.

So when one thinks about how propaganda works, we have to think about why a target audience would ever believe it. If I were to come in here and read a bit of Chinese Communist propaganda—obviously I would not, but if I were, folks in this room would discount that bit of information pretty significantly. The reason is that they know it is propaganda. So the effectiveness of such an information or influence campaign rests upon the ability of targets to be able to understand that what political scientists would—the cue giver, the actor who is giving the information, doesn't have their best interests at heart. So that's component No. 1.

Component No. 2 is some baseline level of distrust of that target state.

So what we don't know, I think, is in countries outside of the United States and countries that the United States shares very close relationships with, is that baseline level of mistrust that is present in most of the U.S. public, present in those other countries, which would then cause the targets in those countries to discount the cue or discount the bit of propaganda.

Mr. MAGAZINER. Yes. Thank you. I think especially when we look at things like access to rare earth minerals that are critical to our economy and other factors, those relationships with the global south are important. China certainly understands that and we must understand it as well.

Question for Dr. Jost or anyone, you know, Chairman Pfluger and I both in our opening statements were clear that our adversary here is not the Chinese people, it is an authoritarian and anti-democratic regime that is becoming increasingly aggressive. On the topic of anti-Asian hate globally, would you agree—and Dr. Jost, but anyone else can weigh in as well, that it is important that we combat anti-Asian hate in all of its forms for a range of reasons, but including the fact that we do not want to give the Chinese Communist Party ammunition to fuel their propaganda both in China and here at home?

Mr. JOST. Thank you, Ranking Member.

Yes, absolutely. Anti-Asian racism has absolutely no place in American society. I think we can all agree on that. I think we can also all agree that the reasons why that is unacceptable in the United States are orthogonal to whether or not the Chinese Communist Party is able to exploit it, just as you said.

That being said, it is true that Chinese diplomats and the Chinese state do call attention to these trends. So, for example, there is an annual report that the Chinese state issues on human rights in the United States, which often times calls out these types of events, both broadly in terms of race and specifically on anti-Asian racial issues.

Mr. EVANINA. I would double down and amplify Doctor—statement here. As I had in my written statement, this is clearly not about the Chinese citizens, both in China or in the United States. This is an issue of Xi and the Communist Party regime and their intelligence services and their strategy. Clear. But, however, that makes it very difficult, and not only to the Doctor's point. I think we have to be very, very clear to say this all the time, this is not about Chinese citizens. But most importantly, the United Front Work Department will use that against us at every single point. So it's a double-edged sword. The more that we don't say it, the more the Communist regime and the United Front Work Department will use it against us when we don't say it. Omission is denial that it's real.

Mr. MAGAZINER. I will just close by saying I think this is yet another reason why it is important that this committee and this Congress focus on combating the rise of racially-motivated extremism here in the homeland as well.

I thank you all very much again for your testimony.

Chairman PFLUGER. The gentlemen yields.

I now recognize Mr. D'Esposito.

Mr. D'ESPOSITO Thank you, Chairman.

In your capacity as the director of the National Counterintelligence and Security Center, you estimated that the theft of intellectual property by the PRC cost America as much as $500 billion—with a B—a year. Can you just describe the impact this theft has on the everyday American, like people back in my district and on Long Island?

Mr. EVANINA. Congressman, I think to make this succinct, as I mentioned in my oral remarks, the real impact is about $4,000 to $6,000 per American family after taxes. It's a real cost to an American homeowner family member.

Mr. D'ESPOSITO I am sorry, can you just say that number again? I apologize.

Mr. EVANINA. Between $4,000 and $6,000 per year per American family of four after taxes is what that $500 billion of intellectual property theft equals. Those are known cases. That's not a guesstimate.

Secondarily, I'll proffer the subcommittee, those aren't the real costs. The real costs for all that IP theft, ideation theft, manufacturing theft, results in the Communist Party of China building that same capability overseas, getting it to patent and global markets before we do, and then selling it back to the American people, the American public and corporations. Then multiple CEOs have said to me, Bill, it's not just the dollar value of our product that's been stolen, it's the manufacturing plants that aren't built in the United States and it is the tens of thousands of jobs that are not created here in the United States because we lost that patent ideation

technology to the Communist Party of China, who went to global market first.

Mr. D'ESPOSITO What are some ways that the U.S. Government is working to identify counterintelligence issues that threatened American IP?

Mr. EVANINA. Well, I think there was a robust agenda probably starting in 2015 and 2016. Here I'd have to commend the efforts of Senator Burr, Senator Rubio, and Senator Warner and Sissy to have what I would call the Chinese roadshows. We went out around the country and briefed thousands of CEOs of industries about this threat and from different sectors financial services, energy, private equity, venture capital, telecommunications, to make sure that they understood what they were doing has a direct impact on national interests and national security. I think that Members of Congress, both in the House and Senate, should have a robust capability to go back to their home districts and document these threats to the chambers of commerce, to where you live, and to economic development corporations and to small businesses so they could identify nefarious capability early and often to prevent it before it happens.

Mr. D'ESPOSITO Thank you, sir. Thank you for your service.

Chairman, I yield back.

Chairman PFLUGER. The gentleman yields.

I now recognize the gentleman from California, Mr. Correa.

Mr. CORREA. Thank you, Mr. Chairman.

I wanted to focus a little bit on our backyard south of the border. Had a chance to go to El Salvador a few years ago and learned that China was looking to acquire, purchase 80 percent of their coast and really build a deep water port in that area. Today I am really bothered that world's largest oil reserves in Venezuela are essentially in a government of Venezuela that it has very close ties to Russia and to China. This is our backyard. It is my understanding we still have a good brand south of the border. Most countries, Colombia included, and others, still like the brand of America—the American dreams, so to speak.

Again thinking about best defense being a good offense, what do we do to make sure that we keep our backyard, our backyard, secure, and not have these kinds of advances by other countries?

Mr. EVANINA. I'll start, Congressman. I think there's some great answers on the panel as well.

I think when you look at South America specifically, we could look—as my colleagues mentioned, subsequent to 9/11, we concentrated on counterterrorism and we missed the boat of the influence of both Russia and China on South America. That influence comes with a price because they provide critical infrastructure for free, they provide mobile phones to citizens of South American countries for free. Specifically, the Chinese invest a lot of money in South America to have them beholden to their interests as well as Russia did historically. I think we probably—and this is getting more in the policy lane—have to be more aggressive and offensive with our brand and our capabilities and our investment in South America to help us in the long run.

Mr. CORREA. We make the best medicines in the world, best COVID vaccine, we are essentially breadbasket of the world. How

can you use those assets to really project our presence in the backyard?

Thoughts, Lieutenant General.

General GUASTELLA. Sir, it's a fantastic question and it's absolutely a concern.

Chinese investment in countries around the world, especially when we're absent, allows inroads for them to develop relationships, not just buy what is immediately there, but also leads to future investments and other things. It comes as a detriment to the United States. You know, like I said, homeland defense doesn't start in the homeland, it starts overseas, not only with a credible capability that we need to have, but also with our allies and partners. So if we become isolationist, if we cede that terrain to the Chinese, we're going to pay a price militarily.

When Chinese military comes into countries, it allows them to start to train with the Chinese, develop a relationship with the Chinese, and it results in an inability for us to leverage them the way we should. So it is a very significant thing for us and we need to look at that.

One last point, and that's in arms sales. A lot of times we don't sell things to countries because we have issues with the country, which is understandable, but sometimes they're going to buy it anyway. When that happens, it's the choice between them buying Chinese or buying American, sometimes we need to think, hey, maybe it's worth it. Should buy American.

Mr. CORREA. General, I am going to challenge you here. Did you use the word absence? Our absence? Did you say that?

General GUASTELLA. I may have. Absence or less——

Mr. CORREA. Are you saying we are not doing our job of here? Going overseas, visiting people, being diplomats, as Members of Congress? Do we need to do more of that?

General GUASTELLA. Sir, I think you're doing a great job.

Mr. CORREA. No, that is not the answer I am looking for, sir. You just said something and I want to make sure all of our Members of Congress understand exactly—that is a great point. I want you to back it because we do need to show our faces around the world. We need to do that. General, I want to thank you for that comment.

General GUASTELLA. You're absolutely right. We do need to show our faces around the world. Our military does a lot of international engagement, Mil to Mil. We need that same engagement at other levels of government. Our state does that. But getting out and seeing and understanding from those allied and partner perspectives—you know, the one big advantage the United States has militarily is that we have a lot of friends out there that China doesn't enjoy that same thing. We're going to lose those friends if we don't get out there and engage, because those friends allow us to base from their countries, they'll support us, they'll back us up in international forums. It happens if we engage them.

Mr. CORREA. Thank you, sir.

Chairman, I yield.

Chairman PFLUGER. The gentleman yields.

I will now recognize my good friend and national security expert, somebody who has spent 20-plus years in the U.S. Navy, Mr. Gonzalez from Texas.

Mr. GONZALEZ. Thank you, Chairman.

I want to associate my comments with my good friend Lou Correa. Him and I took a trip to Central America. We went to Guatemala, we went to Honduras and went to El Salvador. One of the, I guess, surprising things that I wasn't aware of is no Members of Congress had visited that area in 3 years. So to the point, yes, there is a military aspect of it, but there is also a diplomatic. We would like to see the State Department do more.

But up here in Congress in a bipartisan manner, we need to be doing more in our own backyard. I know many of us on this committee are committed to doing just that.

My first question is for you, General. I just got back from a trip from Taiwan, it is the second trip to Taiwan in the past 14 months. I spent 20 years in the military, as my good friend August Pfluger pointed out, our Chairman pointed out, I know what war looks like. We are at war. I mean, this is a war, maybe a cold war, but this is a war with China, with the People's Republic of China, every single day are invading Taiwan via their cyber space. Not only that, but the question I have for you is in particular, your expertise is in air. I spent 5 years as an air crewman flying against China. I know exactly when they come out and they intercept our aircraft. They are doing that every single day. There is a danger in that, right? Because everything is fine until there is an accident, a spark, if you will, that turns a cold war into a hot war.

Can you speak just to some of the dangers in which playing this game of chicken brings up in particular to Taiwan?

General GUASTELLA. Absolutely. China has demonstrated significant aggression in the air by penetrating Taiwanese airspace, and it is a violation of Taiwan's sovereignty. Also, when they're in the air, their professionalism is nonexistent. They will "dust us off", if you will. In one case, we had a collision, mid-air collision from one of their aircraft in a Navy P–3. That is the nature of how they do business.

So what we can't do is watch them and let them get away with behavior like that and not do something back and not be there with Taiwan, not be present, not be out there, and make them respect us the way they are driving fear into the Taiwan ease with their aggression.

Mr. GONZALEZ. Thank you for that.

My next question for you, Ms. Bingen, is turning over to cyber space. This is what war looks like. That is the first aspect of it. In cyber space, there are no boundaries, there are no borders. We are all in on this together, and you can't go it alone. You need to have allies. I put together a bill, the U.S. Taiwan Advanced Research Act, that essentially creates a closer relationship in the cyber space with our allies. Can you just speak to that? As far as how can the United States grow our relationships with others that, let's say, are not traditional relationships? Yes, we have our five eyes and we have got those relationships that have had for a long time, but other places like Taiwan, what are your thoughts on growing that, in particular in the cyber space?

Ms. BINGEN. Well, Congressman, first, if I can go back to your Taiwan point, and thank you very much for visiting. I had the chance to go there in January as well. On Taiwan, if I can say, the arming is incredibly important, giving them a greater defensive capability. It includes not just the tangible weapon systems, but the training that goes along with it. I think there's much more capacity there for increased training opportunities with our forces.

The other point that you raised on Taiwan is every day they are in this cognitive disinformation war with China, with the CCP. So that the more that we can do to help them and highlight or create transparency around those disinformation campaigns is important.

On the cyber front, you're absolutely right on the allies. You know, these are areas, and this ties back into China's Belt and Road Initiative. They are doing a lot to try to get their infrastructure and make others more dependent on them. Where that leads to is other countries—not only their ability to surveil and steal data, but also they're advancing their techno authoritarian norms and standards. So I think that there are things we can do on the international front, threat sharing, but also building norms much more akin to how we see the world and how we want the internet to be operated, data to be protected than the Chinese model.

Mr. GONZALEZ. I think it is very clear to point out that the People's Republic of China are the aggressor. You know, I spent 5 years in Iraq and Afghanistan, Chairman Pfluger has also been at war. I think it is safe to say we don't want war. We want to prevent a war. Part of that is showing that we are going to stand firm with our allies to prevent those.

Thank you, Chairman.

I yield back.

Chairman PFLUGER. The gentleman yields.

The Chair now recognizes the general lady from Nevada, Ms. Titus.

Ms. TITUS. Thank you very much, Mr. Chairman.

Before I ask my specific question, I would like to say that I agree too with Mr. Correa, and it also was brought up by our last speaker that we need to do more. We don't do more by cutting the small foreign aid budget that we have in place now, we do more by investing more. You mentioned Belt and Road. You know, China is investing all across Africa, they are building ports in Lima, they just bailed out Sri Lanka. You know, that is what we are up against. If we walk away, that is not going to be helpful in these difficult areas.

But I want to ask you the question, we just heard this week about China saying that there is a potential conflict or confrontation if we don't put on the brakes. Now, I wonder just what that means for us. Is it an existential threat? Is it saber-rattling? Is it nuclear war? What does that mean? How should we be gauging that? What should we be doing in response besides shoring up Taiwan or trying to make these investments that seem to be fairly difficult to get people to support? Anybody?

Mr. EVANINA. So I'll start.

Ms. TITUS. OK.

Mr. EVANINA. I would say the narrative to the recent statement by the Chinese minister is a false narrative that we need to put

on the brakes. We should start asking them to minimize their aggression, right. Not only here in the United States but with our allies and friends around the world. I think they're really great at putting us in the bucket as being the aggressors. As we've heard from our distinguished Congressman and Congresswoman, that's not the case, right. I think we, as the United States, diplomatically have to do a better job, a more effective job of making sure the world knows that they are the aggressors, because I think their narrative—and they have a great propaganda program, as we heard, and they will use that to show us as the aggressors.

Ms. TITUS. General, how would you compare the threat by China to the threat internally, our homeland threat by domestic terrorists compared to China? If we are looking at where our priorities should be?

General GUASTELLA. Well, ma'am, the threat to the United States from China is the most grave threat we have faced in our lifetime, certainly since the cold war. The reason why is we have an economic superpower that's stealing our technology, that's leaping ahead on weapons that can strike us right here in the homeland or deny our objectives overseas in defense of Taiwan. If we let them continue at this pace, and we don't answer that, we will find ourselves in a very uncomfortable position as Americans, which is watching U.S. service members lose fights.

So, to me, the existential threat posed by China and—the CCP is absolutely the largest threat to the United States. We have to realize it. They are approaching us at any seam they can find, any way in. The balloon was a seam that they exploited. There's 100 other seams that's been discussed here. I think it's time that we wake up. It's a Sputnik moment for us here, and I think we need to realize that as an American society.

Ms. TITUS. Just continuing with this down the panel, how about the CHIPS Act? We often hear that China is not the enemy, they are the competitor. Has this helped in any way to deal with the problem that we are now making chips at home instead of being so dependent on them economically?

Ms. BINGEN. One aspect on the CHIPS Act that I would like to highlight is really the national security piece to it. When we look at was that 80-plus percent of the world's chips, including everything that we use from commercial to our weapon systems, are manufactured within the First Island Chain. We've talked also here about the military threat. We and the Taiwan semiconductor facility, we need to look at building greater resiliency in our industrial bases and our manufacturing capacities. So that for me was a big benefit of CHIPS Act.

Ms. TITUS. Would you like to add to this conversation?

Mr. JOST. Sure. Thank you, Congresswoman.

To go back to your original question about the pathways by which we would be most likely to see Chinese aggression, it is my view that the most likely avenue would be over a Taiwan scenario. If one thinks about how to deter that, there are two primary things in place that the United States has in our strategy. The first is a credible reassurance to Beijing that the status quo will not change, because if Beijing thinks that it is backed into a corner and has to choose either losing Taiwan or launching a very risky and even

low-probability-win war, it's quite possible one can imagine them choosing the latter. So that credible reassurance portion is important.

The other portion of deterrence, which relates to the CHIPS Act, is the change in the balance of power. So another way in which deterrence could fail is if over time shifts toward Beijing's favor in the probability that they would win a conflict would prompt them to act, even though the cost of the risk would be high. That's why it's so important to ensure that the U.S. defense industrial base, through things like the CHIPS Act, is closely protected.

Ms. TITUS. I can't see a clock. Is my time up?

Well, just real quickly, is there anything specific we need to do next, like building off of the CHIPS Act other than going on CODELs to Central America?

Mr. EVANINA. Congressman, if I may just amplify the great comments here.

I think on the CHIPS and Science Act, two things need to occur. More of that type of legislation that really partners our U.S. Government legislative body funding with U.S. corporate sector. No. 2, the CHIPS and Science Act must be protected now from ideation to development of new technologies. If we don't protect it, you're going to be hearing hearings in 5 years saying how did all the technology from CHIPS and Science Act gets stolen and in the hand of the Chinese?

So two things can be true.

Ms. TITUS. Thank you.

Thank you, Mr. Chairman.

Chairman PFLUGER. The gentlelady's time has expired.

The Chair now recognizes for the final question, Mr. Crane.

Mr. CRANE. General, this question is for you.

A second ago you were talking about how you were concerned about the age of the fleet, is that correct? Then also you were talking about how China continues to steal our intellectual property. Is that correct as well? How do we stop that, General?

General GUASTELLA. Well, the theft of intellectual property is something that probably goes beyond what I can comment on. But step No. 1 is realizing that it's happening and ensuring not only the prime contractors, but the subcontractors that develop our defense systems have the appropriate resiliency in hardening. The best way for us to counter China is to invest. You know, the investments the Department of Defense has made for the last 20 years to fight the wars we've been in are not necessarily the investments that are going to make us successful against dealing with a peer competitor like China. So it's important that we transform our investment to the areas that most concerns them, which is our ability to hold targets at risk in their homeland and our ability to deny them their objectives visa vis Taiwan. So we can deter them through punishment and we can also deter them through denial. That happens by investment in the Department, in the domains that are most critical facing a peer competitor, aerospace.

Mr. CRANE. Thank you, General.

My next question is for Mr. Evanina.

A moment ago, you were raving about the capabilities and dominance of the U.S. Intelligence Agency. I think that probably every-

body up here would agree how impressive our intelligence agencies are and have been over the years. My question for you, sir, is are you aware of the lack of trust in our intelligence agencies by U.S. citizens?

Mr. EVANINA. Congressman, yes, I am, and it's a concerning issue.

Mr. CRANE. Yes. You are aware that there is a select committee on the weaponization of the Federal Government up here right now?

Mr. EVANINA. Yes, sir, I'm aware of that.

Mr. CRANE. You know, I represent some amazing people in Arizona, rural Arizona. They love this country. One of the most patriotic districts in Arizona. I myself am a Navy Seal. I joined the Navy after 9/11 and I served for 13 years. I love this country. I want our intelligence agencies to be strong. I think they need to be strong for good reason. But I am going to tell you right now, sir, when when we when we read years after the fact that, you know, 50 former national intelligence folks, several heads of the CIA claim that the Hunter Biden laptop is Russian disinformation, only to find out years later what we all knew, that it wasn't, that is alarming to a lot of Americans, and it makes us lose trust in our intelligence agencies.

For me, when I look at a guy like you that has done everything that you have done, as intelligent as you are, I know that has got to piss you off. If there are 50 former Navy Seals out there lying to the American people and I found out about it, that would piss me off because it undermines the community that I hold so dear. I am sure you probably have a very similar endearment to your community. Am I correct in assuming that?

Mr. EVANINA. You're correct, sir.

Mr. CRANE. What do you think we do about that, sir? How do you think we regain the trust with the American people and our intelligence agency?

Mr. EVANINA. Congressman, I think you bring up a very valid point that not only reaches the current events of today with our intelligence and law enforcement community, but also impacts the recruiting of future generations of women and men who want to serve in the U.S. Government intelligence and military apparatus. I think that is the core element.

I think two things have to happen. No. 1, there has to be complete transparency of things that happened in the past. But more importantly, with the great things that women and men are doing, we have to be more proactive in getting out to your district and other districts at the local level.

Secondarily, there has to be some transparency of what's real and what's not real with the narrative reporting that we have seen in the media. I think that's the obligation of law enforcement intelligence agencies to be forthwith of declassification and transparency of what's going on.

Mr. CRANE. Real quick, Mr. Evanina, if it seemed like I was coming after you today, I apologize for that. It is nothing personal at all. I love this country, and I am tired of losing faith and trust in the institutions and the organizations that as a little kid I had as-

pired to and I upheld. I know I am speaking for a lot of Americans when I say that, brother. OK.

Last question I have real quick is for Ms. Bingen.

You said that war with China was not certain. Can you expound on that a little bit? Please tell us all how, in your opinion, we can avoid war with China.

Thank you.

Ms. BINGEN. Absolutely, Congressman.

I want to say that the cause isn't lost, and there are things that we as a Nation can proactively do. So, for example, continuing to invest in a strong defense, ensuring our forces are ready, is a signal and a deterrent. Making sure that we invest in resilience, resilient networks so that if the CCP decides to launch an attack, it will have a less effect on our networks and our infrastructure. Superior technology. A former secretary of defense I worked for would always say, we never want to send our sons and daughters into a fair fight. With the technology theft happening, we are very much at risk of sending our sons and daughters into a fair fight. So superior technology and agility in terms of how we use that technology. Then ensuring that we have a network of allies and partners. This is a weakness that the CCP has that we have. Sir, with all of your service, you know that we fight in coalitions, and it is important to make sure that our allies are with us and partners are with us and not with China.

Mr. CRANE. Thank you.

I yield back.

Mr. GOLDMAN. All right. So we have some logistical changes here. The Chairman had to step out. So I am going to ask unanimous consent for Ms. Jackson Lee to be recognized for 5 minutes.

Mr. MAGAZINER. We are in trouble now.

Mr. GOLDMAN. We are both freshmen, so bear with us.

Mr. MAGAZINER. Yes, all right.

Mr. GOLDMAN. Unanimous consent for Ms. Jackson Lee to be recognized.

Mr. MAGAZINER. I recognize Ms. Jackson Lee.

Ms. JACKSON LEE. Well, to both of the Chairman and the Ranking Member, I am very pleased to be able to join you. From my perspective, you are two distinguished Members of Congress. Thank you for your service, thank you for your military service.

Before I start, I think because we are in Homeland Security allow me just to put on the record that to be able to compete with China, I think it is extremely important that we assert our democratic values, our values, the strength of our values, our competitiveness. Maybe we will have an opportunity to get the answer to why I believe it is public now, all of the personal data of so many Washingtonians, Members of Congress, House and Senate have been breached. I don't believe that we have had any determination of who breached it, but we certainly want to be on top of those elements, be they commercial or be they a foreign country, from exposing private data of members of the House and Senate who have the responsibility of governing this Nation. I wanted to put that on the committee's record because I am incensed about it and hope that we will have some involvement ultimately in assessing that situation.

But this is a very important hearing, and I want to begin by raising this question. I will have a second question, and I think, gentlemen, I will be finished. But I want to raise the question, Dr. Jost, you have described the evolution of the Chinese Communist Party's thinking when it comes to China's role around the world. We know that in recent years, the CCP has set its aims at developing China-centered and -controlled global infrastructure, transportation, trade, and production networks. They tolerate no diversity when they go into countries. It is China, China, China. They don't even use the indigenous people. China is competing with the United States in a global competition over government values. We have to win the world over by saying that our values of trade and otherwise are much better than theirs.

So how successful are China's efforts? What actions can the Federal Government take to out compete the Chinese Communist Party? Frankly, I think we are a nicer, but I also think that if you interact with us, you will have the benefits of investment in your own country, and you will have the benefits of long-term recovery.

Many of you know that we passed the CHIPS and Science Act—close to my heart as a former member of the Science Committee—which invests $280,000,000,000 to increase domestic semiconductor production. I am excited about that. Some of that may even come to Texas.

Unfortunately not these gentlemen here, I don't think—that 90 percent of our friends on the other side of the aisle did not vote for it, but I know that they are probably working with it in their districts.

So, Dr. Jost, would you share that with me? I would love to have Ms. Bingen to answer that question as well.

Dr. Jost, would you please?

Mr. JOST. Thank you, Congresswoman. These are really excellent questions and I thank you for them.

So you raised the issue of difference in government values, and I agree, although I should note that we do have some common interests, if not common values. China and the United States both want to see their populations live prosperous lives, for example, and both sides want to see the world address some of the challenges of global climate change.

That being said, it is very true that the two countries have stark differences in the way they see the relationship between state and society. The protections that we have in the United States by which citizens enjoy civil liberties and can organize against the state in order to keep its power in check are simply not present there. It is true that China, indiscriminately, or without considering the types of behaviors that the target regime or the target state is conducting, will invest in it. You mentioned the Belt and Road initiative. This is certainly one of the keystone portions of China's efforts.

I do agree that the nature of the regime in that target country is quite important. We do have some research that suggests that economic statecraft that China uses, for example, is less effective when the target country is democratic. There's an intuitive logic there, of course, because if individuals, just like in the United States, can mobilize against their government, if they are in collu-

sion with the Chinese Communist Party for illicit gain, they can hold them accountable. So I think that is a mechanism by which we can indirectly shape China's ability to use the Belt and Road in the way that you are describing.

Ms. JACKSON LEE. Ms. Bingen.

Ms. BINGEN. Congressman, if I can add, you mentioned it exactly right. China has a playbook that they are using with the Belt and Road. We've seen it. The ports and 5G are examples. The ports where they go into countries. Djibouti is a great example where they go in, they operate the commercial port, they kick out the locals, they build up military infrastructure, and then it's a greater threat to the region and to our national security interest. So we see that happening across the globe.

We as a government—we say formally—but the government needs to figure out how do they bring all their different tools of national power to the table to provide alternatives. Some of the areas we have been talking about today are on the technology front. I have a space background. I would offer as an example, our commercial space innovation sector right now is phenomenal. We are using our space technologies, our data, in ways well beyond national security, understanding the climate mapping, countering illegal fishing. This is soft power for Americans and for our companies. So ways that we can leverage some of these newer technologies while clearly protecting and ensuring that they don't fall into the hands of the CCP, but working with our allies and partners across the globe who want to work with us in these areas, figuring out ways to get that kind of information to them. Opening up markets for our businesses so they are not just relying on U.S. Government is also important.

Ms. JACKSON LEE. Let me thank you all so very much. I think it has been established that the Belt and Road technology, or approach, is a danger to the framework of democracy of this Nation. We need to use that power of our values and, of course, of our technology. I like commercial space just because I am a NASA aficionado and space exploration is crucial. Dr. Jost, thank you for that framework that we can utilize.

This is an important hearing, and I thank you, gentlemen for yielding, and I yield back to the Chairman.

Mr. GOLDMAN. Thank you, Ms. Jackson Lee.

I want us to thank the witnesses for their valuable testimony and Members for their questions today. I also want to thank the Members of the subcommittee. We may have some additional questions for the witnesses and we would ask the witnesses to respond to these in writing. Pursuant to committee rule VII(D), the hearing record will be open for 10 days.

Without objection, this subcommittee stands adjourned.

[Whereupon, at 10:44 a.m., the subcommittee was adjourned.]

APPENDIX

QUESTION FOR WILLIAM R. EVANINA FROM RANKING MEMBER SETH MAGAZINER

Question. Can you expand on your recommendation for the creation of an Economic Threat Intelligence entity, to combat corporate espionage and the theft of IP? What need would such an entity address and how should it be structured (e.g., what agencies should be involved and how it should be staffed) to be most effective?

Answer. Response was not received at the time of publication.

QUESTION FOR TYLER JOST FROM HON. DANIEL S. GOLDMAN

Question. Dr. Jost, in your written testimony, you mention that the Chinese government "is interested in using its capabilities to . . . promote narratives that are consistent with its interests" and that "propaganda is deeply embedded in the Chinese Communist Party's institutions." How does anti-Asian hate crime in the United States and some of our political leaders regularly trafficking in xenophobic and racist rhetoric strengthen the CCP's propaganda efforts around the world?

Answer. China's global messaging campaigns routinely draw attention to racism, including anti-Asian racism, in the United States. One illustration of this is found in reports published by China's State Council Information Office on "human rights violations" in the United States. The version of this document released in February 2022, for example, cited anti-Asian hate crimes in the United States as evidence of "deeply entrenched racism in the United States" that was "spreading along with the novel coronavirus."

The goal of such messages is presumably to deflect criticism of China's own human rights record by shaping global public opinion toward the United States, particularly toward the sincerity of American commitment to human rights.

While we know that such criticisms are commonly featured in China's global messaging campaigns, there is comparatively little scholarly research that directly evaluates their effectiveness in terms of shaping global public opinion. To my knowledge, there have been no peer-reviewed studies to date that have systematically evaluated whether China's efforts to call attention to xenophobia and racism in the Unites States achieves the Chinese Communist Party's goal of shaping global attitudes. Congress might consider funding future academic research that is able to more definitely measure the effects of China's overseas propaganda.

Please do not hesitate to contact me if I can be of further assistance.