RPTR ZAMORA

EDTR CRYSTAL

THE GREAT FIREWALL AND THE CPP'S EXPORT OF ITS TECHNO-AUTHORITARIAN SURVEILLANCE STATE

Tuesday, July 23, 2024

House of Representatives,

Select Committee on the Strategic Competition Between

the United States and the Chinese Communist Party,

Washington, D.C.

The committee met, pursuant to call, at 9:33 a.m., in Room HVC-210, Capitol Visitor Center, Hon. John Moolenaar [chairman of the committee] presiding.

Chairman Moolenaar. The select committee will come to order.

Well, good morning, everyone.

Today we are here to discuss a topic of important strategic value: the Chinese Communist Party's Great Firewall.

The Great Firewall is a dystopian censorship regime designed to advance near-total societal control over the Chinese people.

With an army of censors boosted by artificial intelligence and other cutting-edge technology, it monitors all information and expression within China, rapidly stamping out anything that diverges from the party line.

The Great Firewall also controls all contact between Chinese citizens and the outside world. Information is stopped from flowing into China, and the Chinese people are not allowed to get information out. Facebook, X, Instagram, and YouTube, and any platform you could watch this hearing on, are blocked.

Behind the Great Firewall, the CCP has the Chinese people trapped in a parallel reality, where they are fed a steady stream of propaganda tightly controlled by Xi's authoritarian regime. The CCP has turned the internet, designed as a tool of freedom, into the ultimate tool of control.

As it has grown more powerful, the party has only expanded its ambition to maintain total control. In fact, despite spending historic amounts on a massive military buildup, the CCP still spends more on internal security than it does on its military.

Unfortunately, the CCP's quest for control does not stop at China's borders. The CCP is rapidly exporting its surveillance technology abroad, enabled by state-backed champions like Huawei, Hikvision, and ZTE.

It has found plenty of buyers. From the tyrannical Maduro regime in Venezuela

to the ayatollahs of Iran, the CCP exports its malign technologies to help authoritarian governments control the internet and oppress their populations.

Not only does this undermine human rights globally, but threatens America's national security by creating a network of pro-CCP governments that increasingly owe their hold on power to the CCP.

Over the last year and a half, the Select Committee on the CCP has worked tirelessly to champion the rights of the Chinese people to speak freely.

We have held hearings where dissidents and Chinese students have described violent threats they have faced right here in the United States, and we have called loudly for an end to their oppression.

We have tried to break the barriers between the Chinese and American people, but the Great Firewall stands in the way.

Today, the select committee will again champion the rights of the Chinese people. This hearing will focus on the ways we can expose the Chinese people to the "irresistible power of unarmed truth," a phrase first used by Russian author Boris Pasternak and repeated by former President Ronald Reagan in 1988 as his dream for people trapped behind the Iron Curtain.

The CCP fears that power and spends tens of billions of dollars on global propaganda and censorship to control it. We should set it free and give the Chinese people unfettered access to the truth.

This means countering Chinese censorship with honest information and fighting the CCP's export of surveillance technology worldwide. It also means ensuring transparency at home. Whether in Hollywood or Silicon Valley or on college campuses, CCP censorship has no place in America.

What the CCP fears most is the Chinese people learning the truth -- the truth

about the Uyghurs, about Taiwan, Tiananmen Square, COVID-19, the Chinese economy, corruption -- and worst of all, the truth about the CCP itself. Why? Because they know their rule is built on lies.

What Reagan observed in Berlin is still true today: "This wall will fail. For it cannot withstand faith; it cannot withstand truth. The wall cannot withstand freedom."

What was true of the walls of concrete and barbed wire will be true of walls of code.

I am grateful to our three incredible witnesses here today who will discuss how we can repeat Reagan's success and ensure that, once again, freedom is the victor.

With that, I would recognize our Ranking Member Krishnamoorthi.

[The statement of Chairman Moolenaar follows:]

******** COMMITTEE INSERT ********

Mr. Krishnamoorthi. Thank you, Mr. Chair.

Last year, this committee looked at the CCP's message about an alternative reality where democracy is failing and autocracy is on the rise.

Next, we examined in our "Discourse Power" hearing how the CCP promotes that message outside of China.

Today, we look at how the CCP spreads its message inside of China, not only through propaganda but also by stifling alternatives to its messaging through censorship, surveillance, and its so-called Great Firewall, which is the most sophisticated system of internet censorship anywhere in the world.

The CCP censorship is dangerous because by denying discussions of human rights and alternatives to its negative messaging about the U.S., the CCP creates a controlled society that is more supportive of its aggression toward the U.S. and our allies, partners, and friends, including Taiwan.

Almost 25 years ago, President Clinton argued that giving China full access to our market would help create a future of greater openness and freedom for the people of China.

Unfortunately, that prediction was wrong, because instead of allowing greater openness and freedom, the CCP used China's growing wealth and access to technology to build the world's most sophisticated surveillance state, which it now exports to other countries.

Today, the CCP spends more on its domestic security services than it does on its military, and it spends a lot of this money on surveillance cameras. It is estimated that of the 1 billion surveillance cameras in the world, half of them, a whopping 500 million surveillance cameras, are in China alone.

Here you can see the city of Wukan, which once was called China's "democracy village" because for several years it was allowed to elect its own leaders.

Unfortunately, the CCP ended this experiment in 2016 and now blankets the village with surveillance cameras like the five you see here. You can count them, five on one lamp post.

The CCP also spends its money on the technologies and surveillance bureaucracy behind its Great Firewall, which experts say has achieved industrial-scale censorship by blocking IP addresses, contorting online conversations, and filtering website data.

In recent years, the CCP has started actually shrinking the number of Chinese website domains, which are down more than a third from their peak in 2019, as you can see here, dropping from roughly 51 million domains in 2019 to about 32 million in 2023.

In contrast, the number of domains in the U.S. in that same time period doubled, it has grown dramatically, and that is not much different around the world.

Motivating the CCP's police state is its fear of Chinese citizens holding their leaders accountable, like they did in Wukan's democratic experiment. In fact, at one time online expression flourished for years in China as netizens found creative ways to evade the Great Firewall.

One of our witnesses, Mr. Xiao Qiang, compared this period to "Star Wars: Episode IV -- A New Hope," where many fought for a future of greater openness and freedom from the repression of an authoritarian regime. But according to Mr. Xiao, since Xi Jinping came to power in 2001, it has been more of this, "Episode V -- The Empire Strikes Back."

Under Xi Jinping, the CCP has put even more eyes on the street and online, and it doesn't intend to stop at Chinese borders. As Xi said in 2018, the countries that take command of the internet will win the world.

We cannot allow the CCP to command the internet, which was designed to connect people, not to divide and control them.

Whether it is countering the CCP's export of authoritarian technologies or standing by the Chinese people in their fight for freedom of expression, we must make sure that freedom and openness, both in society and online, prevail over censorship and control.

This is a fight the U.S. cannot afford to lose.

Thank you, and I yield back.

[The statement of Mr. Krishnamoorthi follows:]

******** COMMITTEE INSERT ********

Chairman Moolenaar. Thank you.

If any other member wishes to submit a statement for the record, without objection, those statements will be added to the record.

We are now privileged to be joined by a great panel of witnesses who have been on the front lines of this important issue.

Our first witness is Mr. Nat Kretchun. He is the vice president for programs at the Open Technology Fund, a congressionally funded nonprofit organization that supports the development and deployment of anti-censorship, privacy, and security technologies for populations living under repressive information censorship regimes.

Our second witness is Dr. Zack Cooper. Dr. Cooper is a senior fellow at the American Enterprise Institute, where he studies the U.S.-China competition.

Finally, we are joined by Mr. Xiao Qiang. A physicist by training, Mr. Xiao became a human rights activist after the Tiananmen massacre and is the founder and editor-in-chief of China Digital Times, a bilingual China news website designed to aggregate, contextualize, and translate online information from and about China.

Thank you for being here, gentlemen.

And with that, I want to welcome all the witnesses.

Thank you all for being here.

And, Mr. Kretchun, you are now recognized for your opening remarks.

STATEMENT OF MR. NAT KRETCHUN, SENIOR VICE PRESIDENT FOR PROGRAMS, OPEN TECHNOLOGY FUND; DR. ZACK COOPER, SENIOR FELLOW, AMERICAN ENTERPRISE INSTITUTE; AND MR. XIAO QIANG, FOUNDER AND EDITOR-IN-CHIEF, CHINA DIGITAL TIMES

STATEMENT OF NAT KRETCHUN

Mr. Kretchun. Chair Moolenaar, Ranking Member Krishnamoorthi, distinguished members of the committee, thank you for inviting me to testify.

The Chinese internet today is unrecognizable from the internet we all know here. It has been roughly 15 years since Google and much of the free and open internet was blocked in China and replaced by CCP-controlled domestic platforms, such as WeChat and Weibo.

An entire generation has grown up never knowing the internet beyond these platforms. They don't long for the global internet because, by design, they have never meaningfully experienced it.

In that time, the CCP has spent billions of dollars to erect a complex technical architecture to isolate over a billion people from the global internet.

However, its ability to control information has less to do with blocking access to foreign websites and far more to do with its success creating an entirely new ecosystem and reengineering its population's online behavior.

This is the fundamental challenge we are faced with today.

OTF was established over a decade ago to help journalists and human rights defenders counter online censorship. During that time, the cat-and-mouse game of

internet freedom has remained fundamentally unchanged. Even in countries considered to have advanced information controls, like Russia and Iran, people still download circumvention tools to access the global internet.

Internet freedom solutions are developed based on the assumption that overcoming censorship is simply a technical impediment that once addressed will meaningfully restore free online expression.

However, this assumption no longer holds in China. The CCP is not simply building an ever-greater firewall. It has undertaken a much more ambitious project, erecting multiple layers of self-reinforcing technical and social controls, the result of which is not a globally recognizable internet with key redactions but a wholesale substitution of an entirely distinct online ecosystem.

This ecosystem is characterized by the substitution of global platforms for domestic alternatives. Although highly censored, these platforms are extremely compelling. They are well designed and content rich.

As a result, most Chinese internet users have little reason to explore beyond China's own social media universe.

What this substitution does is provide China's censors with a huge home field advantage. The amount of control that can be asserted through WeChat and other platforms is far beyond what is possible on the open internet.

On these platforms, censorship is faster, more nuanced, and more complete; surveillance is harder to avoid; and party messages are spread more forcefully by committed Little Pinks.

For those who want to look for information or connections that are unavailable on domestic platforms, precisely how to do so is far from simple. The Chinese Government has engaged in a novel project of meta censorship to obscure even the possibility of

circumvention from its own citizens.

They have criminalized circumvention tools and thoroughly blocked discussion of how to download them. Domestic search engines don't index censored sites.

App stores, notably those run by Apple and Google, remove thousands of apps at the request of the Chinese Government, including most internet freedom tools.

And as if these obstacles weren't enough, it is only then that users must contend with the Great Firewall, which, as was mentioned, remains the world's most advanced national filtering system.

From the vantage point of an average Chinese user, it has become increasingly difficult to even imagine what exists beyond China's domestic ecosystem, much less discover how to access it.

The end result is a dramatic change in user behavior. As researchers at Stanford concluded after they gave students in Beijing circumvention tools, even with these techologies few students used them to access the global internet unless they were actively incentivized to do so.

The era in which we could reasonably assume that most Chinese citizens could and would naturally seek out uncensored content is, unfortunately, over.

Traditional circumvention tools, such as VPNs, remain an important part of any internet freedom strategy. However, moving forward, we must adopt an updated approach that fosters more purposeful connections between information seekers and information providers.

While China's internet substitution model provides its citizens with the bread and circuses of contemporary online culture, what it intentionally omits remains in demand when people know how to seek it out.

In the same Stanford study I mentioned a second ago, researchers found that

Chinese students who were exposed to the global internet maintained a lasting demand for politically sensitive content and circumvention tools.

There is no single unifying policy solution to peel back the layers of China's information controls, but some key starting points are:

Internet freedom tool developers will need to more intimately understand and design around the technical limitations and socialized online behaviors of users in China;

Creators of objective, otherwise unavailable content will have to seek out connections with their audiences in less traditional online spaces;

Apple, Google, and other U.S. technology companies must end their current practice of aiding CCP censorship efforts;

And to counter the normalization of techno-authoritarianism, we must join with like-minded partners to advance a vision of a free global internet despite the realities of fracture and fragmentation.

It took the CCP decades and billions of dollars to engineer a socially and technologically distinct online environment. The elements of any effective response will necessarily take patience, time, and significant resources.

While I have focused today on the domestic implications of China's information controls, we are already seeing other governments adopt these same strategies.

If we don't contest China's model of internet substitution at its source, we will be unable to counter it where it spreads.

The scale of the challenge is immense and yet unquestionably worthwhile. There is no message the U.S. could deliver that is more credible or more powerful than helping facilitate Chinese citizens' own search for the truth.

Thank you, and I look forward to your questions.

[The statement of Mr. Kretchun follows:]

******** COMMITTEE INSERT ********

Chairman Moolenaar. Thank you.

Dr. Cooper, you may now proceed.

STATEMENT OF ZACK COOPER

Mr. Cooper. Chairman Moolenaar, Ranking Member Krishnamoorthi, and distinguished members of the committee, thank you for inviting me to testify today.

As this committee has highlighted, the Chinese Communist Party has developed and implemented the most sophisticated censorship and surveillance apparatus in the world.

What has happened in the last few years, however, is not a simple evolution of the party's tools and techniques; rather, it is a whole new threat to internet freedom, not only in China but beyond.

Not only is the Communist Party gathering enormous amounts of data on the Chinese people, at the same time it is actively eliminating Chinese-language portions of the global internet. Chinese-language websites now account for just 1.3 percent of the global total.

As a result, the Communist Party now knows more about its people than ever before, but the Chinese people know less about the outside world, and indeed, even their own domestic realities. This information asymmetry is no accident.

The Communist Party's strict information controls do tremendous harm to the people of China, but I want to focus my remarks here today on the effects on Americans.

Increasingly, the Great Firewall is not only an obstacle for the Chinese people but also a roadblock for U.S.-China relations. U.S. Ambassador to China Nick Burns recently

warned that Chinese leaders, quote, "say they are in favor of reconnecting our two populations, but they are taking dramatic steps to make it impossible." He cited the Chinese Government's efforts to, again, quote, "denigrate America to tell a distorted story about American society, American history, American policy," end quote.

In short, efforts to stabilize the U.S.-China relationship are now bedeviled by the Communist Party's censorship and disinformation apparatus.

Moreover, if the Chinese economy continues to stumble as a result of the Communist Party's poor management, Beijing may feel that it has to rely more on nationalism to bolster domestic support.

If this occurs, the Communist Party might lean even more heavily into blaming the United States for China's own woes. Setting the record straight will be critical to guard against this strategy.

Moreover, techno-authoritarian tools developed by Beijing will not stay in China. Over the last decade, the Chinese Government has exported censorship and surveillance technologies to over 80 countries worldwide. These tools and techniques will be adopted by autocrats from Russia to Iran to Venezuela and beyond. And through multiple international, technical, and standard-setting bodies, the Chinese Government is attempting to reconfigure foundational elements of the internet.

In short, the Communist Party's information controls not only harm the Chinese people but also obstruct their ties with American counterparts and threaten to proliferate around the world.

Now is the time for us as a Nation to rise to meet this challenge. I want to quickly outline four recommendations with which we could do so.

First, the United States needs an ambitious moonshot project on internet freedom. One estimate suggests that the Communist Party spends on the order of

$10 billion per year to develop and refine its system of surveillance and control. U.S. internet freedom efforts receive much less than 1 percent of these resources. We must do more. The time to act is now, before these systems proliferate globally.

Second, we should insist that American companies do more to counter information controls. Some major U.S. companies restrict access to virtual private networks and other apps in China while allowing the Communist Party to replace these networks with ones that the party can covertly monitor. Companies must disclose major cybersecurity incidents; they should have to do the same when they enable foreign censorship and surveillance.

Third, the United States should insulate itself against censorship and surveillance here at home. The Communist Party has long barred most American media companies from operating effectively in China, yet the United States has few reciprocal protections.

U.S. media companies themselves should be required to disclose when they disseminate information or accept payments provided by entities affiliated with designated foreign adversaries.

Fourth, the Congress should conduct additional and should support additional research on Chinese censorship and surveillance.

We need a deeper understanding of the tools and techniques that the Communist Party is using if we are to understand the evolving nature of the threat that it poses. Detailing the Communist Party's information control strategy is fundamental to building an effective U.S. Government response.

The information competition with China is not a minor aspect of the relationship but rather a central pillar. Xi Jinping often references Mao Zedong's exhortation to, quote, "seek truth from facts." But increasingly, the Communist Party has become focused on reconstructing facts to hide the truth.

I, therefore, thank the committee for bringing these issues to light, and I commend your efforts to build an ambitious bipartisan agenda in this area.

Thank you.

[The statement of Mr. Cooper follows:]

******** COMMITTEE INSERT ********

Chairman Moolenaar. Thank you.

Mr. Xiao, the floor is yours.

STATEMENT OF XIAO QIANG

Mr. Xiao. Thank you, Mr. Chairman and respectable members of the committee. I want to thank you for giving me this chance to address this very crucial topic.

Let's start from the Great Firewall. The chairman's opening statement already said the Great Firewall is the broader definition. Both include the domestic censorship and also as a gateway, the technology apparatus.

Let me start with a little bit narrow definition of the Great Firewall, which is that is a nickname. Now the Chinese Government gave it an official name publicly. It is called the State Data Cross-Border Security Gateway, and that is a collection of institutions and technologies, both hardware and software, that serve as the national censorship apparatus in the PRC that restricts those websites, which opening statements already mentioned.

Let me also say, the central government organ or party organ is called the Cyberspace Administration of China, CAC. That is the agency for internet regulation, censorship, oversight, and control. And the CAC reports to the Central Cyberspace Affairs Commission led by Xi Jinping himself. And since 2008, CAC directly managed this apparatus called the Great Firewall.

Let me also say that in the more broader sense now the Great Firewall, the CCP always sought to legitimize the regime by shaping public discourse, mobilizing support, and suppressing dissent.

I will give you one example. In 2015, leaked documents revealed that the Chinese Government mobilized over 10 million college students through the Communist Youth League for their so-called "online public opinion struggle" tasks.

And then all the companies, internet service providers, data analysis companies, and social media platforms in China contribute to this digital control, Sina, Weibo, Toutiao, Kuaishou. They employ thousands of censors to remove illegal content, so-called, and often outsource to companies. One is called Beyondsoft, which employs over 8,000 workers.

But what is the Great Firewall, that critical piece of a gateway? Because the entire censorship propaganda mechanism in China, controlling both traditional and social media, relies on the Great Firewall for this information security. Without it, the suppressed content could become accessible again by the Chinese public.

Now, we also talk about circumvention of the Great Firewall. There are tens of millions of Chinese internet users using VPNs or homemade tools, open source tools, to circumvent the Great Firewall.

But also, the Great Firewall itself enhances its blocking capabilities through methods like active probing and specialized responses and pushing to criminalize such circumvention efforts.

Let me give you one example in this hearing, which is a blogger called Ruan Xiaohuan. He is a cybersecurity specialist. He began an anonymous blog called ProgramThink in 2009. The blog provided cybersecurity advice, methods to bypass the internet censorship, and political commentary critical of the CCP.

The blogger dared the CCP to catch him, using his cybersecurity expertise to evade capture for 12 years. Millions of Chinese netizens admired him as a legend and hero, cheering, worrying, praying, and crying for his fate.

In May 2021, Ruan was arrested by Shanghai police. In February last year, he was sentenced to 7 years in prison for, quote, "inciting subversion of state power."

And I want to use this opportunity to call on American Congress Members to nominate him, along with Peng Lifa, the "Bridgeman," the protester at Sitong Bridge on October 13, 2022, the two of them, for the 2025 Nobel Peace Prize in support of the Chinese people's struggle for human rights.

And now let's talk a little bit about the surveillance technology. We already talked about how they export, PRC exports civilian technology. Let me give you two examples.

In November 2020, the U.S. Treasury's Office of Foreign Assets Control sanctioned this company called the China National Electronics Import and Export Corporation for giving Venezuela the Chinese version of the Great Firewall. But who is the chief scientist of that Chinese company? Fang Binxing, the father of the Great Firewall.

And only last month, or 2 months ago, in Myanmar, the military junta deployed a new system that can intercept and decrypt web traffic, blocking applications and blocking VPNs.

Who provided that technology? Chinese company again, the same company that the U.S. just sanctioned, and, again, that is the chief scientist of the Great Firewall, Mr. Fang Binxing.

Finally, let me just say, we are in the internet -- not only internet but AI age. Previously introduced me to -- I said -- used the "Star Wars" two episodes, the "New Hope" and "Empire Strikes Back." But now we are on the next episode. Unfortunately, it is not called the "Return of the Jedi." I called it, "The Emperor Got AI."

AI can be the force for the good, but it also can be used for surveillance, censorship, manipulation. As technology that relies heavily on the centralization of

massive data, AI tends to empower centralized autocratic governments rather than the decentralized democratic system.

The PRC is the most powerful and most technologically advanced dictatorship. By using these technologies, the CCP consolidates its power at home while weakening democratic competitors abroad. The CCP is providing the world with a blueprint for establishing a digital totalitarian state and presenting a real threat to world peace.

So we must work in solidarity to defend and preserve freedom and dignity at home and globally. This is one of the greatest challenges we must meet in this 21st century, and I include six of my recommendations and policy in my written statement.

Thank you.

[The statement of Mr. Xiao follows:]

******** COMMITTEE INSERT ********

Chairman Moolenaar. Thank you.

Mr. Xiao, what do you think would happen if the Great Firewall ceased to exist and information flowed freely in China?

Mr. Xiao. The People's Republic of China will no longer exist given enough time. Let me put it this way. Why do they really, really want to block using the Great Firewall? Because just like the Berlin Wall, without that wall the other half of the city of Berlin will walk across to freedom. And for the Chinese people, that if the Great Firewall is not there to stop the people to access information, they will seek freedom online in their heart and minds.

Dr. Cooper and also Mr. Kretchun described particularly the sort of alternative or the parallel cyber reality in China, but that so-called cyber reality doesn't really hold water if the Great Firewall is really down.

And let me also say this. This is fundamentally about legitimacy of the Chinese Government. They cannot answer the question who elected them, who they represent, and who participates in the daily decisions. If those questions are being openly asked and a debate can be freely sort of let people to express, then fundamentally the Chinese Communist Party's legitimacy is undermined.

So in this way, Xi Jinping is correct to say that information security is his regime security and that that regime is critically held up by the Great Firewall.

Chairman Moolenaar. Dr. Cooper, why do you think the CCP is investing so much in this Great Firewall? And why is controlling information at home and abroad so important to their strategy?

Mr. Cooper. Well, I think Mr. Xiao put it really well. At the end of the day, the party's legitimacy doesn't rest on the support necessarily from the people for the policies

that it is pursuing, especially when those policies don't appear to be working.

You look at what has happened to the Chinese economy the last few years, you look at the increase in political repression, and it is hard to say that the Communist Party is delivering for its people, but it is very clear that the party has become more reliant on information controls.

And so I think at home, increasingly, we are probably going to see the party rely more and more on information control rather than actually being able to deliver for the Chinese people, and that downward cycle is probably going to get worse.

I would just say, abroad, I do think this idea that China needs to make the world safe for autocracy, as some people have said, makes sense. And, ultimately, there is no way for China to do that without trying to pacify the criticism that it sees from the outside world.

And so I would expect that we would see China try and proliferate the tools and techniques that it has. It is already doing this. But I think we are maybe at the first phase of a strategy that will go well beyond that ultimately.

Chairman Moolenaar. And then, Mr. Kretchun, what should be done to enhance the flow of information across the Great Firewall? You have mentioned there is no one policy. But what would it take to effectively combat the CCP's surveillance and censorship?

Mr. Kretchun. Yeah. I think from the United States' perspective, it is going to take a lot more focused coordination across a lot more of the agencies and different actors that we have on our side.

The way that China has designed its information control system is to try to ensure that most Chinese citizens never even hit the Great Firewall, that they are mostly trapped inside of this domestic ecosystem of WeChat and other kind of giant platforms.

And since that is the case, we are going to have to be able to more nimbly reach in to find folks with the kind of solutions we can offer in terms of circumvention tools, to be able to provide uncensored, truthful content to folks where they are on the internet they have been socialized into and lead them back out into the global internet, which at this point they have kind of lost the muscle memory of.

Chairman Moolenaar. And, Dr. Cooper, do you have a thought on that?

Mr. Cooper. Well, as Nat just said, I have the honor to be the chairman of the board of the Open Technology Fund, and I think the kind of work that OTF has been doing has been incredibly important in this area.

But I do think the scale at some point does matter. The Chinese Government is putting billions and billions of dollars into this year after year. I think, increasingly, this has to be a central pillar of our own strategy, too, even if we are not going to spend that kind of money.

I do think that we have to be talking about significant investments over time or else the closure that we are seeing in China will get worse. And it won't stay in China; it will expand to other authoritarian states.

So that is why I said I think this is time for a moonshot. We need a major societal decision that this is something that we have to deal with over the next decade or two.

Chairman Moolenaar. Thank you.

Ranking Member Krishnamoorthi.

Mr. Krishnamoorthi. Thank you, Mr. Chair.

Nobody understands the Great Firewall better than the Chinese people who, despite the CCP's denial of human rights and despite the CCP's aggressive rhetoric about the U.S. and our allies, still find ways to talk about censored topics.

For example, when the CCP blocked the #MeToo hashtag, activists in China began

using the Chinese characters "me too," which you can see here, which mean "rice rabbit." Now they even use rice and rabbit emojis to get around the censors.

Mr. Kretchun, Chinese netizens often use these kind of techniques to discuss sensitive topics, correct?

Mr. Kretchun. That is correct.

Mr. Krishnamoorthi. Let me show you another image. This is the image of the "Tank Man" from the Tiananmen Square massacre. This is also censored in China, correct, Dr. Cooper?

Mr. Cooper. Yes.

Mr. Krishnamoorthi. But some Chinese citizens do know about Tank Man, including from U.S. broadcasters like Voice of America; hence, they developed memes like this one to discuss what happened at Tiananmen Square.

Mr. Kretchun, the CCP eventually detected these ducks and actually blocked searches for "big yellow duck." Isn't that right?

Mr. Kretchun. That is correct.

Mr. Krishnamoorthi. Chinese-language content produced by VOA, which is critical for countering the CCP's narrative of aggression, gets almost 2 million views every day. Unfortunately, funding for VOA has flatlined, and this year its China program received just about $15 million, which is roughly the annual cost to operate -- let alone buy -- two F-35 fighters.

Mr. Kretchun, increasing funding for VOA and programs like Radio Free Asia would help Chinese citizens get better access to non-CCP messaging and lower support for aggression towards neighbors and friends, right?

Mr. Kretchun. I think so.

Mr. Krishnamoorthi. Now I want to turn your attention to this woman, her name

is Cai Xia, who famously managed to evade the censorship. She once taught at the CCP Central Party School but was expelled from the party after comparing Xi Jinping to a, quote, "gang boss."

Mr. Xiao, Ms. Xia expressed these views in a recording that went viral inside of China, right?

Mr. Xiao. That is correct.

Mr. Krishnamoorthi. Ms. Xiao says that a trip in Spain in 2008 was when she became fully aware of the CCP's repression and realized the need to speak out.

Mr. Kretchun, it is these kinds of people-to-people ties and exchanges that, in my opinion, are among our best tools for combating CCP censorship. Would you agree with me?

Mr. Kretchun. Most certainly.

Mr. Krishnamoorthi. Unfortunately, the number of Chinese students studying in the U.S. has dropped almost 30 percent in just the last few years.

So, Dr. Cooper, even as we compete with the CCP, we need to increase student and other exchanges with the Chinese people. Isn't that right?

Mr. Cooper. I agree with that. I think student exchanges are an asymmetric advantage for the United States.

Mr. Krishnamoorthi. Hundred percent.

Let me turn to my final topic, namely the CCP's export of surveillance technologies.

The first problem is the security concerns with the technology itself, for instance, the existence of backdoor access by the CCP.

But the second problem is that the CCP exports its surveillance tech to bad guys all over the world, such as the military junta that overthrew Burma's democratically elected

government in 2021.

Dr. Cooper, Chinese companies like Dahua Technology, which the U.S. sanctioned for supporting the CCP's human rights abuses in Xinjiang, are selling advanced surveillance cameras to the Burmese junta, right?

Mr. Cooper. Yes.

Mr. Krishnamoorthi. And the junta is using these cameras to help arrest and imprison pro-democracy activists, correct?

Mr. Cooper. Yes, I believe they are.

Mr. Krishnamoorthi. Here is a picture from a Dahua showroom in Burma advertising some of the tracking software in December 2022. So we have a sanctioned Chinese company selling advanced surveillance technology to a sanctioned regime.

When dictators around the world know they can rely on the CCP to support them when they are under U.S. sanctions, they are strengthened and enabled to commit more human rights abuses.

Thank you, and I yield back.

Chairman Moolenaar. Thank you.

Representative Wittman.

Mr. Wittman. Thank you, Mr. Chairman.

I would like to thank our witnesses for joining us.

Mr. Kretchun, I wanted to get your perspective. The depth and breadth of what China is doing around the world many times is facilitated by American companies. In fact, many times they get coopted or they feel like they have to be compelled by the CCP because of the 1.4 billion people in China.

Would you agree that those technology companies have been coopted and that they are actually enabling, in many ways, the key enforcers of the Chinese Communist

Party's surveillance state? And if you do agree with that, what should we do to hold these companies accountable or to make sure there are consequences for them enabling the CCP?

Mr. Kretchun. Yeah, absolutely. At the very least we see that they are, at this point, not cross-pressured. They are feeling CCP pressure to remove the kinds of internet freedom apps that OTF funds to help develop and basically taking the tools out of Chinese citizens' hands that would allow them to get around censorship and surveillance, and it is a huge problem.

And beyond that, we haven't found good ways to compel them to help better support the development of internet freedom technologies or the funding of those technologies, because at the end of the day, a lot of the tools that those are built on point back to some big American companies who, at this point, are profiting from them.

And in terms of what we should be doing, I think Dr. Cooper has some fabulous recommendations for ensuring that at the very least disclosure happens when these kind of companies aid and abet censorship and surveillance efforts in the CCP. But in a better world, they wouldn't be engaged in those behaviors at all.

Mr. Wittman. Very good. Thank you.

Dr. Cooper, let me go to you, and I want to follow up on Ranking Member Krishnamoorthi's assertion about the exportation of this technology.

We know that China, the Chinese Communist Party, is one of the most advanced states as far as how they prosecute advanced technologies for surveillance and really repression of their own people. They look to export that because they don't believe in the rule of law. They like to enable other governments that operate the same way that they do.

Now, let me ask this. Give me a sense of your priority, where we should look at,

that is the most immediate threat of places where this technology is being exported. And then what should we do to respond to this exportation?

We talked a little bit about that. Mr. Kretchun talked a little bit about it. But I want to know, what is the most immediate threat? And then what can we do as a Nation, policy-wise and as a Congress, to most immediately impact that?

Mr. Cooper. Well, thanks for that, Congressman Wittman.

I think this is absolutely crucial. And I would say, you could think of sort of a tiered approach to different countries that adopt Chinese surveillance and censorship technology. There is a hard core of highly autocratic countries, your Venezuelas, your Cubas.

Frankly, I don't think we have got a lot of leverage in most of those countries. We can use sanctions to try and limit their ability to gain access to Chinese systems. But at the end of the day, they are probably going to be able to circumvent those.

You have then got an outer layer, which is countries that are maybe leaning in an autocratic direction or have some leaders who are highly corrupt who would prefer to have the censorship technology. I think in those places we can actually be quite effective when we are focused on intervening with those countries early on in the process.

I would say there is also a third layer, which includes some close democratic allies of the United States. You know, China's safe cities approach is something that has gotten traction in France.

So I would start there at the outer layer and work our way in over time. I think if we can explain and make transparent what the Communist Party has done with these tools that a lot of people in those countries will think that those tools shouldn't be able to be used either by their governments or by companies in their countries.

Mr. Wittman. Very good. Thank you, Dr. Cooper.

Mr. Xiao, I want to ask, we see as this digital authoritarianism is expanded around the world that I think there are some opportunities for us to point out where the weaknesses are in those systems, and the only way that that happens is through the people in those countries, or as we also heard, examples of people within China that are speaking out and pushing back against this.

How can the United States either enable those folks that are speaking out or undermine the use of these digital tools of authoritarianism.

Mr. Xiao. There are several aspects to answer this question, but let me actually start from the voice of the Chinese people even under the repression, that they use the coded language, they use satires.

But also there are -- let me just give you an example of what kind of are the voices on China's internet and being censored and reappear outside of China, such as China Digital Times on my website.

Well, let's start from this. Even back to your first question, why the Great Firewall is so important for the Chinese Communist Party? Because as an autocratic system it has the common feature, which is "few rules many, but in the name of many." They cannot tell Chinese people the truth. They said, "Oh, we do this for you, for Chinese people."

Well, think about this. In the dynasties that the next legitimacy of emperor is because of the bloodline, but today's dynasty cannot do that. North Korea is inherited by the blood, but it is called Democratic People's Republic of Korea. And China is called the People's Republic of China. It is not people's; it is not a republic.

And to hear the quote that online went viral in China and has been thoroughly deleted, and what did this post say? It says, "Oh, those peoples are a miracle."

The People's Daily, which people do not read; People's Great Hall, where people do not meet; people's government, where peoples do not rule; people's court, where people see no justice.

These kind of voices are common knowledge in China, but without an alternative that they are being repressed by this digital authoritarianism and actually also being confined in cyberspace by the Great Firewall.

Now, the respective ways to respond to this, including the technology piece, if the Chinese regime seems -- the Great Firewall is so critical to it, it has invested so much resources and technology to it, even to undermine that effort to getting the Chinese internet users to access more freedom of information, it requires a much larger budget and resources to build up a counter-technology.

And I am naming one, not just VPNs, decentralized generative AI tools, the new AI tools that actually are another threat to the Chinese Government control of the ideology and online contents.

But if, right now, these generative AI tools are in the big U.S. companies' hand, there is a Chinese company doing that, but they have to censor their content again, their result will not really meet the demand of the Chinese population if there is an alternative decentralized AI tool that could be made.

Mr. Wittman. Thank you, Mr. Chairman. I yield back.

Chairman Moolenaar. Representative Kim.

Mr. Kim. Yeah. Thank you, Mr. Chair.

Dr. Cooper, I would like to start with you. You said something that -- I guess I kind of missed it when I read through your testimony, but you said it and it really stuck out to me.

If I get this right, you are saying that right now about only 1.3 percent of global

websites are Chinese-language websites, and that is down from 4.3 before, about a decade ago? Is that correct?

Mr. Cooper. That is correct.

Mr. Kim. So just so I get this right, you are not just talking about what the Chinese people have access to, you are just saying, like, they have actually been deleted from just writ large in the internet across the world. So it is not just about censorship within China, but it is being deleted and in many ways removed from all of us to be able to access. Is that correct?

Mr. Cooper. That is exactly right.

Mr. Kim. Yeah. Thank you for that. I thought that that was a really interesting nother component of this, not just about what the Chinese people are accessing but just the richness of what we hoped is in the internet for all.

I wanted to try to kind of -- I guess, Dr. Cooper, maybe I will start with you. I guess I am just trying to get a sense of, like, how does someone understand or measure how much of the internet is being restricted or how much -- it is hard for me to really conceptualize what all is actually being restricted from the Chinese people through this action by the CCP. Do you have an understanding of how to process that?

Mr. Cooper. Well, my fellow panelists may have other views on this. But I think there are a lot of tools that you can use to look at different elements of this.

So, one, for example, the Open Technology Fund helps to support is on app censorship, and you can go on and you can literally see on the Google Play store, on the Apple App Store what is censored. And it is a tremendous amount of stuff, and it is many of the apps that not only Americans use all the time but that others around the world use.

So I think it is going to differ from domain to domain, but it is a tremendous

amount not just on the internet but also these other tools that people use to access information.

Mr. Kim. Yeah. I want to just pivot and just kind of focus in on something that has been kind of touched upon, but just we are on the advent of this new era of innovation with AI, as has been referenced in different ways, but I would like to dig in a little deeper.

Mr. Kretchun, I thought you had a really powerful diagram on page 3 really showing the concentric circles here of some of this, helps me understand this.

I mean, some of my concern is that when we look at large language models and what we have seen so far with AI, what we see if this trend continues is honestly a lot of users having less direct access to websites and a lot more information being put together and assembled for them.

And in some ways I worry that that kind of falls into that CCP-controlled domestic platform's area if they are able to develop that kind of thing that I think Mr. Xiao was worried about on that front.

So I guess I see this as sort of double-edged, and I would like to -- I will turn to you, Mr. Xiao, afterwards to talk about what kind of threats that could pose to the CCP.

But I would love to just start with you, Mr. Kretchun. Is this going to make things potentially much, much worse in terms of the ability to censor?

Mr. Kretchun. Absolutely. I mean, the really kind of pernicious -- for me kind of the most dystopian part about the way that the CCP has set up its information control regime is just how self-reinforcing it is and how it really does create kind of, like, interestingly, memory holes. To your point about a shrinking internet, there are just fewer sources where those things can be found.

So when you have taken people -- initially, when it was just like, "Oh, we will

censor websites we don't agree with, new websites will pop up," that is a cat-and-mouse game that can be played from both sides.

Once people are sequestered into platforms that can be much more easily controlled by the CCP, all of a sudden everything you see kind of reinforces a central narrative, and it becomes really hard because everyone is subject to the same controls to say anything different.

Then, as you say, as large language models take over in the way that we, like, have answers curated for us, if those large language models are trained only on censored data or data that, like, has those memory holes well ingrained in them, then anything that model --

Mr. Kim. They don't have to be reactionary in that way. They are actually just removing that from the knowledge base of the large language models and --

Mr. Kretchun. Precisely.

Mr. Kim. Mr. Xiao, I guess you had mentioned that AI tools could be a threat to the CCP, I think you were saying maybe because maybe their large language models might not be able to do all that people want it to do because it is going to have a limited amount of info. But I would love for you to just explore that a little bit more for us here.

Mr. Xiao. Yeah, let me give you an example.

China actually is the only other country that has a tech ability of AI that they are developing those large language models. So, as Mr. Kretchun was saying, that is a parallel universe. The Chinese users are using a Chinese model.

The difference is they are trained by different data and also under the different supervised training, which is in China the censor will just monitoring the outcomes.

But there is a difference between the two models if you are trained differently and by different data, and why those differences are so crucial, because AI is so vast that

it answers any commonsense questions.

I will give you an example. What is patriotism? What is love of country? If you use OpenAI, ChatGPT, then the answer to love your country is different than love your government. It is different than the state. Yeah. It is different than love your culture.

But if you use the Chinese, under the PRC propaganda materials are trained. The crucial point, every day they are trying to confuse in people's mind is love China equals love Chinese Communist Party equals love Chinese culture equals Chinese people. They run them together. Logically, it doesn't make any sense.

Mr. Kim. Yeah.

Mr. Xiao. But they use whole propaganda and censorship to make that only available in the Chinese-language space and Chinese AI which answered that.

Mr. Kim. Yeah. Well, my time has come to a close, so I will yield on back. But I think that is an important thing for this committee to explore.

Chairman Moolenaar. Thank you.

Mr. Luetkemeyer.

Mr. Luetkemeyer. Thank you, Mr. Chairman.

I appreciate the commentary this morning and the discussion. I want to take a little bit different tack here this morning.

Some of you have talked about how we can impact what is going on in China, and a couple of you in your testimony, written testimony as well as verbal testimony this morning, talked about investment in China.

The Chinese talk -- well, I think Mr. Cooper said they invest billions into their internet. So a question is, where do they get their money from?

We have had a number of discussions in this committee before, and there were

witnesses that testified that we, the Americans, are giving a lot of the capital they need to be able to do this.

And, to me, I think a couple ways we can effect this is to sanction some of the folks, not be able to invest in certain companies.

I think one of you made that recommendation, I think Mr. Xiao in his testimony, as well as prohibit investment in Chinese companies, period. So I have got some bills to do that.

So I think, Mr. Kretchun, let's start with you. Would you like to comment on that?

Mr. Kretchun. From the OTF perspective, I mean, we come at this from a relatively technical perspective. And in that sense, like, there are lots of places where you would want to be very careful about essentially either U.S. investment in the kind of firms that we know will blow back into creating better surveillance and censorship technologies that, as Dr. Cooper said, will inevitably be proliferated into a lot of other states who are seeking information control solutions, like the PRC is putting together.

Mr. Luetkemeyer. Dr. Cooper, would you like to comment on that?

Mr. Cooper. Yeah. What I would just say briefly is, I think there is an important role for outbound investment legislation, and I know many of you have been leaders on this issue.

I think, as regards the censorship and surveillance question, the outbound investment limitation should for that purpose be focused on those companies that are engaged in the most pernicious behavior, either within China or outside.

And so I do think there is a logic to restricting the ability of Americans or American companies to invest in companies that we know are infringing on the rights of people, whether they are in China or in Venezuela or beyond.

Mr. Luetkemeyer. Mr. Xiao, you have mentioned in one of your recommendations, I believe, to prohibit or minimize investment. It looked to me like, why are we trying to help the company -- the country that is trying to take us over? I mean, it makes no sense to me. If this were Nazi Germany, would we be investing in that? I don't think so.

China is our mortal enemy here and we are continuing to fund them. We need to be stopping all investment, in my mind, and sanction them.

What do you think about that comment?

Mr. Xiao. Well, my expertise is not global economy. In that sense I am not sort of qualified to recommended the sort of blanket assumption.

But my recommendation is by targetively sanction or block the incoming investment of those companies, the Chinese companies who are playing a crucial role, that on those large-scale digital authoritarian tech, including the censorship and the surveillance and manipulation.

And I actually added two more sanction recommendations in my written testimony, let me just state it. I used the example of cyber -- the security expert, Chinese Fang Binxing, who is widely known, publicly known in China to be the father of the Great Firewall. As I said, he is the chief scientist of those U.S.-sanctioned companies who are exporting technologies around the world.

Not only those companies should be prevented, the U.S. investors who invest, but those individuals, including the scientists who played a crucial role to develop those technologies, and educational institutions should be sanctioned and blacklisted by the United States.

RPTR DEAN

EDTR SECKMAN

[10:31 p.m.]

Mr. Luetkemeyer. One quick question. One of you made the comment the country that takes command of the internet will rule the world. I think some of this goes back to artificial intelligence. I mean, that is where we all seem to go back to. I have got a hearing right after this one in another committee with regards to artificial intelligence. It scares the heck out of me. It is a wonderful tool, on the positive side. But it can be manipulated in a very, very negative way. Scares the dickens out of me. I think the Chinese, if they beat us in AI, we are in really big trouble.

I have only got 10 seconds left. So I yield back, Mr. Chairman. Thank you very much.

Chairman Moolenaar. Thank you. We are going to break briefly so that members can go and vote. And we will plan to reconvene shortly after the vote series wraps up. My staff will be in contact with member offices on timing.

And, without objection, this committee meeting is in recess, subject to call of the chair.

[Recess.]

RPTR DEAN

EDTR SECKMAN

[11:11 a.m.]

Chairman Moolenaar. Welcome back. The committee hearing is now reconvened, and we will now complete member questions.

Representative Carson, you are now recognized for 5 minutes of questions.

Mr. Carson. Thank you so very much, Chairman.

This question is for everyone. I would like for you all to elaborate on the risks of the CCP's surveillance and censorship activities on U.S. companies intellectual properties and data security in the global market. Are there any examples in your mind of successful initiatives by our international partners to counter the CCP's efforts and what collaborative efforts are in place between the U.S. and our global partners?

Mr. Cooper. Well, I think this is an incredibly difficult issue for us to even find information about, because many of the companies as, you know, they are doing business very differently in China than they do anywhere else. We just had a few days ago Microsoft assert that individuals cannot use anything other than an iPhone in China now. And I think pretty clearly that was because of surveillance concerns. But we actually don't know a lot about how most companies operate in China because those companies are quiet about what they do, because a lot of those American companies want to continue to do business in China and have to adjust their activities to comply with Communist Party requirements. So I think there is actually a limit on what those of us outside the business community know about how many American businesses that do business in China are operating.

Mr. Xiao. I wanted just to add another aspect, which is if the Chinese tech

companies are building a lot of digital infrastructures around the world -- I will give you an example ZTE. Right, it operates in over 50 countries, providing fiberoptic cables, mobile networks, data services in Turkiye, Sri Lanka, Sudan, you name it, Laos. Those 1- companies also have capability of collect and control data globally and enhancing that AI data analysis and in control models. In other words, those countries who are using the Chinese digital infrastructure are -- expose themselves to the -- not only espionage but even further manipulation and control. This is a global threat. And it is not always in U.S. territory itself, but giving -- it is of competitive nature between the United States and China. In a global market and geopolitics, the policymakers must take that into concern.

Mr. Kretchun. And, yeah, just to add a final point, one really interesting thing that we have seen become ever more true about the CCP's surveillance and censorship apparatus is that it is now portable. When you take your phone from China to America or anywhere else, that follows you in a lot of ways. There are data trails back to China when you have those apps installed and when basically your phone is set up as a Chinese national would have their phone set up, they now bring that censorship and surveillance with them in ways that could have unintended consequences --

Mr. Carson. Thank you.

Thank you, Chairman. I yield back.

Chairman Moolenaar. Thank you. Representative Barr.

Mr. Barr. Chairman, thanks for holding this hearing, excellent hearing, important, important oversight here.

Dr. Cooper, let me ask you a little bit about -- follow up on this outbound investment strategy that we are working on. Currently, Huawei and Hikvision are both listed on Treasury's non-SDN Chinese military industrial complex list and DOD's 1260H

Chinese military company list. Currently, however, being named on these U.S. lists has little or no effect on these companies' operations or operations abroad. What would be the effect on these companies if the U.S. subjected them to full blocking sanctions or implemented a U.S. investment prohibition? Do you think this would be helpful to include in an outbound bill?

Mr. Cooper. I think it would be effectively impossible for them to operate if they were not able to access Chinese banks. And so I do think if there were blocking sanctions put on, that would be essentially a kill stop potentially for some of those firms that do business globally.

Mr. Barr. And again sanctions is a way with precision to really impede their surveillance authoritarianism, digital authoritarianism. Is that fair to say?

Mr. Cooper. Yes, it is.

Mr. Barr. What would be a reason that Treasury would not currently designate those companies which are so integral to the techno-totalitarian surveillance activities of Beijing?

Mr. Cooper. Well, the bottom line is that the Treasury Department has not used sanctions as a tool against China for frankly most of the last two decades. I was in the White House doing sanctions work about 20 years ago, and Treasury didn't want to use those tools then. And, in general, I think the Treasury Department has been hesitant to use them now?

Mr. Barr. Well, we might want to change that. Let me ask any of you to describe the Chinese central bank digital currency has integrated into its digital authoritarianism. Can anyone speak to how China seeks to use the digital Yuan as a way to surveil its people?

Mr. Xiao. I can say in a very broader sense the -- currently, that initiative is not

taking a full scale as the Chinese Government would want it to be. However, for those already being experimented in different cities in the different sectors of societies, it is absolutely true that will use China's digital Yuan, then the state has the bank potentially to track every financial activities you do, yeah. You have zero privacy under that system.

Mr. Barr. So this is why the United States should not adopt a central bank digital currency, right, because we don't want to counter China by becoming more like China. And we are hearing reports from within China that the plan is to pull all the physical currency out, have a digital central bank digital currency, have the central government of China and the CCP monitor financial activities. And then, if they control that, then they can shut down the people's capabilities of how they spend their money or even take some of their own funds away from them.

Mr. Xiao. In a way they are already doing that with -- through the help of transit tech companies using those online payment systems, those kind of shut down the blocking -- taking as a form of punishment. It is already happening in the Chinese financial -- but if the central Chinese digital Yuan does that, that would give much more power, which is a terrifying future.

Mr. Barr. It is a terrifying future.

Real quick on the Taiwan guidance, the PRC guidance regarding Taiwan, that includes allowing the death penalty for individuals who are deemed advocates of Taiwan independence. I am co-chair of the Congressional Taiwan Caucus. To any of our witnesses, given that Taiwan recently inaugurated a democratically elected president, how is PRC using its surveillance capabilities to surveil or jail pro-Taiwan individuals in China?

Mr. Xiao. This raised another very important question, which is the PRC state extended their ability not only surveillance but cyber attack way beyond the PRC borders,

that whether your Taiwan independence or other activists or political figures or even, you know, any other sector to, if the Chinese state targeted you, their espionage, particularly the cyber attack goes -- leaves no space as a state power. Therefore, it is not just the citizens of Taiwan needs to watch what do they do, their activities around the world, but anyone who, if the PRC identified as their enemy. So that costs the United States and any sovereign states to give a strong measure to protect their own citizens and to counter that kind of beyond PRC border attack.

Mr. Xiao. Thank you.

I yield back.

Chairman Moolenaar. Thank you.

Representative Auchincloss.

Mr. Auchincloss. Great hearing, Chairman, thank you. And thank you to our witnesses.

I will cosign my friend from Kentucky's statements about us not needing to mimic the ideology or tactics of the Chinese Communist Party to outcompete them.

One of democracy and freedom's great ideological strengths is that it does not need to rely on propaganda to succeed. It wins in civil society on its own merits. And, in free and fair elections this year, Taiwan demonstrated that. Leaders in the Chinese Communist Party see Taiwan as simply the largest and most organized dissident group in China, and they made many sophisticated attempts to sway voters through mis- and disinformation throughout the campaign season, and it didn't work. We must learn from Taiwan's examples of resilience and build on them.

Mr. Qiang, am I pronouncing that correctly?

Mr. Xiao. Yes.

Mr. Auchincloss. In your testimony, you recommend Congress support new

circumvention technologies and decentralized AI tools through increased access to resources, research, and collaboration opportunities. As you set up the China Digital Times, what circumvention resources did you find most helpful?

Mr. Xiao. Well, the circumvention to the firewall actually really doesn't required extraordinary high tech. There is a plenty of those open-source Chinese developers homemade tools that are serving the Chinese internet uses even rights now.

Mr. Auchincloss. Are they readily available, though, to the average consumer of --

Mr. Xiao. That is the difficult part because the Chinese authority is cracking down on any spreading of their tools. In the same market, there is also the commercial VPN companies and the U.S. Government's funded tools development, such as the open tech fund.

Mr. Auchincloss. Yes.

Mr. Xiao. The issue is really how to get those tools to the individual internet users at a scale -- up against the Chinese authorities' repressive efforts.

Mr. Auchincloss. We need to get a whole app store inside the great firewall.

Mr. Xiao. That we cannot, even Apple, you know, those companies are taking VPN app down. And also I add one more thing to the committee that, because there is actually a strong demand for those VPN circumvention tools, the Chinese government in addition to a firewall, they develop their own VPNs to give to a large significant number of Chinese users so the Chinese state can have monitoring the data and also putting another layer of filtering into those kind of Chinese VPNs.

Mr. Auchincloss. I did not realize that. So it is state-supported VPNs that are in fact funneling that information right back to the politburo --

Mr. Xiao. Yes. For example, you use that -- there are plenty people using that

state VPN. They can search on X, but they cannot access to the Voice of America --

Mr. Auchincloss. Mr. Kretchun, then, the rapid response fund provides emergency support to independent media outlets, journalists, human rights defenders facing digital attacks, helping individuals and groups stay safe. How can the open technology fund solicit for these kinds of support systems and help what Mr. Qiang is trying to do?

Mr. Kretchun. Yeah, it is absolutely a challenge and one that we are attempting to improve our tooling all the time. So, as Xiao said, it is incredibly important to have tools that meet the Chinese users where they are. Because, as you say, you can't just go to an app store and download them very easily now. We are trying to make sure that, for the kinds of developers and human rights advocates who can access our funding, that that is available and as kind of rapid and as secure as we can possibly make it. And then, in terms of kind of trying to find ways to inject more secure technology and solutions into ecosystems where Chinese users are already finding these solutions is really important.

Mr. Auchincloss. You need viral adoptions, though, this is a -- fundamentally this is a consumer technology and so it has got to be virally adopted. And how do you create that viral flywheel through a repressive digital regime? I mean, has anybody cracked the code on that one?

Mr. Kretchun. Unfortunately, no one has cracked the code at scale. And I think part of what we are going to have to do is devolve that a little bit, because there is not going to be a silver bullet anymore, but what we can do is understand specific user groups within China who have specific use cases and needs and design tools for them, which will, like, allow us to fly a little bit more below the radar of a control system that is designed specifically to prevent virality.

Mr. Auchincloss. Well, because you want -- competition is going to induce the

best product for what people want to use, right, you are going to get that feedback loop with the consumer.

Mr. Kretchun. Absolutely.

Mr. Auchincloss. Final question, again for you Mr. Kretchun, technology at scale fund supports the large-scale circumvention and secure communication technology needs of the U.S. Agency for Global Media's broadcasting networks, including Radio Free Asia. Nearly all those satellites, though, are owned by only 25 companies worldwide, very few of which have open-source technology through the extremely high cost of R&D long-term maintenance. Would it be helpful to have a Federal challenge which allows Federal agencies to pay only for success?

Mr. Kretchun. So the [inaudible] doesn't actually work with satellite technologies; it more runs VPN technologies. But effectively that is how that fund functions for VPN; it only pays for success. It offsets the user carrying costs of VPN users in highly restricted areas. So our partners come to us and say, "Okay, this is how many users we were able to support and here is your per-user cost of those," and that is what we are reimbursing against. So effectively that is what we are doing; we are incentivizing tools who can carry users in the hardest places.

Mr. Auchincloss. Are you concerned at all about the concentration of satellite ownership. Is that something that we need --

Mr. Kretchun. Oh, I mean, it certainly is an issue that we have to pay close attention to. From the OTF perspective, it is not a technology we are able to piggyback on in China yet, but we are exploring in a lot of other places and how that market developed in China and in fact how chip sets evolved to see, like, if we don't need bay stations and that sort of thing, like, that would be an important thing to pay attention to even though it is not operational today for us.

Mr. Auchincloss. I yield back. Thank you for the indulgence, chair.

Chairman Moolenaar. Representative Newhouse.

Mr. Newhouse. Thank you, Mr. Chairman. I want to thank the three witnesses to day for their testimonies on how the CCP strategically executes its great firewall strategy to control its domestic population as well as expand its authoritarian sphere of influence campaign abroad. These abuses of centralized power through surveillance technologies truly go against everything Western civilization has been fighting for since the creation of our free marketplace of ideas. Unfortunately, the CCP's great firewall strategy, in my humble opinion, goes far beyond just the control of information and possesses deadly implications for the rest of the world. For example, as many of you know, this committee's recent investigation unveiled how the CCP directly subsidizes, awards, incentivizes, protects, and invests in chemical companies responsible for producing 97 percent of the fentanyl in the world, much of that pouring through our southern border, contributing to killing more than 110,000 Americans every year. The CCP allows the illegal export of these deadly chemicals to occur while simultaneously censoring content about domestic fentanyl sales on the internet. In other words, the CCP knowingly protects its domestic population from deadly fentanyl, as they profit off poisoning of Americans.

Chairman Moolenaar has given me the opportunity to lead the select committee's working group along with Mr. Auchincloss from Massachusetts and address this issue by mobilizing legislative efforts.

So I have got two questions on this subject. Let's start with Dr. Cooper. If the CCP truly wants to prohibit fentanyl sales and exports on their highly regulated internet platforms, how quickly could this occur? And does their inaction or lack of cooperation constitute drug warfare?

Mr. Cooper. I do think that the party after the November meeting between Biden and Xi made a commitment to follow through on fentanyl that they have not executed. I think this is quite clear. You can talk to officials within the administration, and they expected to have more cooperation from the Chinese.

I don't know how fast they could crack down, but I think it is quite clear that officials on our side feel that there is a lot more that China could do that it is not doing today.

Mr. Newhouse. Any thoughts on whether or not this is drug warfare on their part?

Mr. Cooper. Well, I definitely think that it is an effort -- well, that it enables efforts to damage the United States in fundamental ways. When I go talk about China across the country, not infrequently do I have someone show up in the audience who has lost a child to fentanyl, and I am sure you have the same experience. I have talked about this with senior Chinese former officials and some current officials. I think some of them understand the damage that this is doing, and I don't think the party has responded in a way that they absolutely should have.

Mr. Newhouse. So, Mr. Kretchun, Mr. Qiang, thoughts?

Mr. Kretchun. I don't have too much more to add beyond what Dr. Cooper has said other than to essentially reassert that, yeah, that is the kind of topic that is incredibly well censored in the Chinese domestic space. It is a thing that, like, when we are analyzing different censorship trends always come up as one of the things that is very tightly controlled so we can definitely cosign with that one.

Mr. Xiao. I second that. With respect to looking at it is that the Chinese public not aware this is one of the important issues between the two countries, the United States and China. Chinese -- being kept not only completely in the dark but often being

fed with opposite stories and narratives. That giving this challenge even much harder to address.

Mr. Newhouse. Yes. Again, thank you all. Appreciate the contributions to this important subject.

Mr. Chairman, I yield back.

Chairman Moolenaar. Thank you.

Representative Brown.

Ms. Brown. Thank you, Mr. Chairman.

The Chinese Communist Party has no equivalent of First Amendment protections for the 1.4 billion people under its control. The freedom of speech enshrined in our Constitution is not respected, recognized, or realized by the CCP. So let's not pretend otherwise.

Every internet-connected device in the People's Republic of China is watched and controlled by the CCP. Groups like the Uyghurs and other minorities are surveilled, tracked, and spied on 24/7 by their government. This is not a terrifying TV show; it is real life. Global independent media sites and search engines, such as Google, have been banned in China for over a decade. That is how scared the CCP is of the independent free flow of information and the legitimate exchange of ideas and knowledge.

So, Mr. Kretchun, can you give us some perspective on what it is like to live under the digital repression implemented by the CCP?

Mr. Kretchun. Ma'am, to your point, it really does differ based on who you are. If you are in Xinjiang, it is an entirely different world. That has become a laboratory for the kind of information and controls that the panel has been describing today. It is a horrible marvel of data collection, synthesis, and cross-referencing in a way that really is a pretty complete surveillance state in a way that is unreplicated at this point anywhere

else.

With that said, for many people in China, it is that softer control that actually is just as pernicious because they live in what feels like a very content-rich, robust ecosystem of WeChat, and yet there are massive holes in that that are not even apparent. So the experience can vary widely. But, to your point, the surveillance and censorship is pervasive everywhere.

Ms. Brown. And can you tell us how effective are people living in China getting around the CCP's online censorship? How does it compare to say the people living under Kim's regime as you mentioned in North Korea?

Mr. Kretchun. It is a very different control strategy between North Korea and China. China is one that is connected to the internet. They are basically developing technical ways to do things that we basically thought were impossible. In North Korea, they have made much more draconian deletions. You have to have essentially a state-produced device that is open by default and is surveilable by default. The CCP has to find ways to take an iPhone and get around the security protections that are inherent in that device. And so what they have done is used essentially platforms like WeChat and others and then also network-level controls to be able to do that at a massively aggregated level than in a kind of more on device, you know, slightly more straightforward way that the North Koreans approach it.

Ms. Brown. Thank you. And my last question is, what could the United States and Congress do to further support the efforts of human rights groups, the press, and everyday people to access the internet freely within China?

Mr. Kretchun. The -- if the kinds of circumvention tools that OTF funds that Xaio and others have built are to be successful, they need to come along with really good, well-targeted, well-packaged content that folks are looking for because, at the end of the

day, there is information competition, even if we are attempting to allow users in China to take their own journeys to that content. And so the more that we can invest in the production of very good, objective news and make sure that it is packaged and distribution is taken into account when it is put together -- we are past this era of, "Oh, if you build a really good website, you will get Chinese users come see it." You have to now break that down and make sure you are delivering it to those users and giving avenues to assess it that actually comport with the way that they interact with each other daily online.

Ms. Brown. Thank you very much. I think we all need to pay attention to the digital repression occurring in the CCP. In the People's Republic of China, the internet is a weapon, and free speech is seen as a threat, monitored, restricted, and a tool of further CCP indoctrination. This has implication for our freedoms and rights in the United States where everyday people are denied access to information on what is happening on the ground in China and to talk freely with friends and relatives abroad. Our Nation and this committee are united in pointing out this glaring hypocrisy in working to protect and promote internet freedom around the global.

And, with that, Mr. Chairman, I yield back.

Chairman Moolenaar. Thank you.

Representative Dunn.

Mr. Dunn. Thank you, Mr. Chairman.

I want to thank each of the witnesses for their testimony today. It remains incumbent on us in Congress to fortify our information systems against this Chinese Communist Party dystopian export of state-sponsored censorship and surveillance in the United States. We must pave this path forward for -- in this area for America and the free world. We cannot allow the PRC to dominate our critical industries and threaten

our information systems.

The CCP heavily invests in the most advanced techo-totalitarian surveillance state in the world and simultaneously created a very large military. Why did they do this? Because they are a government who fears its own people most of all.

One of the CCP's top strategic priorities is to control Chinese citizens, including what they say, what they know, and what they do. This is because controlling Chinese people is essential to everything else they want to control from Taiwan to Xinjiang to Hong Kong.

This is also their greatest potential vulnerability: Truth is their Kryptonite. It would be foolish of us not to seize this opportunity to leverage this in our strategic competition. Routinely aware that the CCP is not content to stop at China's current borders, and they have invested billions of dollars to construct a global information ecosystem that prop ups, promotes propaganda, and facilitates censorship, and exports these surveillance technologies and capabilities of the governments, both through state-owned and through nominally private Chinese companies, such as Huawei, Hikvision, Dahua, and ZTE, much of this is coordinated with the Belt and Road and digital silk initiatives, including the CCP's advocacy of digital sovereignty. So, once these systems are sold at absurdly low prices, these surveillance technologies are used to gather vital information for the CCP to monitor and suppress activists, dissidents, and ordinary citizens. The CCP frequently uses that technology brought to gather information about all of us and our governments, and it includes incredibly detailed personal data, fingerprints, blood samples, and other things. I look forward to working with my colleagues to ensure that the United States remains free. We all want to serve the country and preserve a free society. We cannot let this authoritarian state undermine us.

Mr. Kretchun, as you mentioned your technology, American technology companies in your testimony, technology companies like Apple and Google, seem to have contributed toward the enforcement of the CCP surveillance state. If so, how should we stop them?

Mr. Kretchun. Yeah, the way that they are doing that is in this -- basically enabling this practice of metacensorship. So, at the one hand, we are attempting to build tools that would allow Chinese citizens to get around these digital controls and safe while doing so. And, yet, the way that still in China, everywhere else, people attempt to access these tools is through app stores. And when the app stores systematically remove apps that allow that, apps at the behest of the CCP, that is takes away an avenue where folks might be able to reclaim some agency and actually seek out the kinds of information that they are systematically denied in the domestic sphere.

As I mentioned before, I think Dr. Cooper's recommendation around disclosures for Apple, Google, other American tech companies who are facilitating the censorship and surveillance apparatus in China is a low bar. We would much rather have it not happen at all, but that is at least a starting point.

Mr. Barr. Thank you.

Dr. Cooper, where is the CCP's export of digital authoritarianism most concerning to the United States interest and security? And maybe a little bit about how we should respond.

Mr. Cooper. Well, it is a tough question because it is in 80 countries around the world. And I think there are so many of these places that we should be deeply concerned. But the places I would start are the societies that are sort of on the edge, right? Teetering where a little bit of information control might sway them away from democracy towards more autocratic or corrupt systems. And so I think if we are going

to prioritize certain governments, that is certainly where I would begin. Those countries that are on the edge where some amount of censorship and surveillance is going to make a fundamental difference in how they are governed going forward.

Mr. Dunn. Thank you very much, Dr. Cooper.

I have questions for Mr. Qiang, but my time has elapsed, and so I will submit those in written format.

Thank you very much, Mr. Chair. I yield back.

Chairman Moolenaar. Thank you.

Representative Steel.

Mrs. Steel. Thank you, Mr. Chairman.

And thank you to all the witnesses. You know, China is the biggest threat, not just to the United States, but, you know, you see all over the world African countries and South America and, you know, in the Pacific regions, and they are building all over, and they try to take over.

So CCP censorship and surveillance includes the great firewall allows the CCP to censor foreign websites, international media sources, and digital applications to block its citizens from the world. I have experienced firsthand the CCP using online activity and physical whereabouts of Chinese citizens to block one of its citizens from connecting with family members in southern California. This is unacceptable. We should be alarmed that CCP uses its power to track their own citizens' movements and predict their activities, especially playing around in the United States.

So, Dr. Cooper, the CCP has routinely violated international standards related to intellectual property rights, subsidization, and overcapacity, and yet they do not abide by the international norms and rules, and that has brought them to current economic positions and not playing any fair games in trade, and I am on the AI task force. You

know what? They are the most dangerous ones right out there. So how can global leaders hold China transparent and accountable in its international system that is free, open and fair.

We have been asking these questions constantly, and there is just no certain answers. Like, you know what? You are the experts. So, if you can give us some of the answers, so that we can stop them, and how we are going to do it.

Mr. Kretchun. So my view is that targeted pressure on China is unlikely to stop the massive activities that you are talking about, right? Intellectual property action, et cetera. I am not saying that we shouldn't support targeted action against companies and other entities engaged in those behaviors. We should. But I would not expect them to be successful.

I do think at some point the United States has to both take actions to protect ourselves against those risks by closing certain elements of our economy that are most at risk to those behaviors while also threatening to increase the pain on China. That is the only thing that has shown to bring Beijing to the table to talk seriously about these issues. So I think it has to be a mix of targeted measures against bad behavior going after specific individuals, specific companies, but also some pressure at the higher political level. Without that, I don't think Beijing will change its activities.

Mrs. Steel. Sanctioning those high official names and, you know, those --

Mr. Cooper. Can I give you one example that I know the committee has done important work on? Solar cells, right? American companies invented a huge amount of the advanced solar cell technology in the world. The intellectual property was stolen by China. We have Department of Justice cases in which we indicted multiple people affiliated with the Chinese Government for doing this. And, yet, we have allowed the Chinese companies who benefited from that stolen technology to sell the solar cells back

into the United States. I can't for the life of me figure out why we have allowed this to happen. So I think there are just some basic steps that we should be taking to protect ourselves. It might not change Chinese behavior on the whole, but we have to start somewhere.

Mrs. Steel. Well, Chinese behavior, the stealing is much cheaper and faster. That is the way it is.

If Xiao Qiang -- if I pronounced your name wrong, I am sorry -- why should those who are concerned about the human rights abuses by the CCP worry about their work with other authoritarian regimes around the world? Is the CCP working with the Communist leaders to grow our repression efforts? Because my both parents fled from North Korea, and I work with Vietnamese Government very closely and North Korea. I mean, these countries that they are actually following what China does. I mean organ harvesting to just everything there. And you know what? We really have to stop that what China has been doing. So what do you thinking that we really have to do?

Mr. Xiao. Thank you. Not only North Korea and the Vietnam, and I mentioned China forming the allies on the censorship authoritarian website with Russia, with Iran. They come together. And China a far leading economic power and technology power providing those services and setting examples and protecting them as well. In this context, United States also needs to look for strategic allies. And, in this particular surveillance and censorship, the counter battle that not only just the United States protecting its own sector and protecting its own people, but working with allies to compete at the global market, and that, a global internationalized competition, is the context. And the countries that share the same value has a much stronger reason to work together.

Mrs. Steel. So we have to work with our allies, and we have to defend our allies,

and that means we have to have a very strong defense here. So thank you so much for coming. And I yield back.

Chairman Moolenaar. Thank you.

Representative Hinson.

Mrs. Hinson. Thank you, Mr. Chairman.

We know China's main export of the surveillance technology goes to Uyghur, burgeoning nations and democracies. And it is clearly a blatant attempt by the CCP to extend its surveillance state globally and really undermine these countries' efforts to move toward democracy. We have seen that play out time and time again. And it should be concerning to everyone.

We have talked a lot in this committee in previous hearings about how this is kind of an all-encompassing, multipronged strategy by the CCP. They export these surveillance technologies as well, kind of like cedes. They handpick governments that fit their criteria to suppress those personal freedoms. They are utilizing initiatives, like BRICS, that diplomacy to further spread that influence, ultimately creating that kind of force of control and influence around the world.

So, Mr. Cooper, what do you think we can be doing to really prevent these so-called seeds of surveillance from being spread and taking root in these vulnerable democracies and countries? How can we really help support them in safeguarding sovereignty, personal freedoms, and making sure they don't cede that to the CCP?

Mr. Cooper. Well, part of the problem, as you know well, is the Chinese offerings are so cheap compared to anything offered by most of the rest of the world. They are cheap because they are subsidized and because the party has an interest in having that technology spread. But I do think in some countries which are strategically important, the United States is going to have to think with its allies and partners about

finding ways to provide that technology at a cheaper price. That may mean some amount of subsidization.

At the very least, what we should be doing everywhere, though, I think is bringing transparency to what Chinese practices are, which is why this committee's hearing is so important. So many countries don't even understand what they are signing up to when they sign up to the digital Silk Road. They think they are just getting wonderful cheap technology. They don't understand that it is bringing with them this censorship and surveillance apparatus. And so I think if we can help tell that story, it will deter some foreign governments and some -- corrupt leaders in nondemocratic countries from accepting those technologies.

Mrs. Hinson. Right. And, obviously, we have been telling that story about the technology that, even here in the United States, we have these vulnerabilities from Huawei, ZTE, some of these bad actors. Do you think we are doing enough to analyze these technologies coming into our country to ensure that they don't contain Chinese surveillance? Obviously, we passed the law for rip and replace. We are trying to find additional funding to make sure we can continue to execute on that. But do you think that there is more that we need to be doing here at home?

Mr. Cooper. My personal view is that TikTok is a pretty good example of how serious we are about Chinese technology, right? We have a world in which the Chinese would never allow a major American social media company to operate in China. And, yet, the dominant app used by young people in the United States is a Chinese-engineered app. It is unbelievable that we have allowed this to continue. So, if we take that as the test of our seriousness, I think we are failing.

Mrs. Hinson. Well, it is clearly "rules for thee but not for me" in how they act, not only in this space but other spaces as well. Either of our other witnesses care to add

anything to that line of questioning?

Mr. Xiao. I do. Actually, when we talk about the vulnerabilities of the CCP, but I actually wanted to remind the committee members your important work. So apps are a game in this competition, that you have to see, for example, Chinese tech sectors are incredibly innovative and very second to the United States tech sectors, but have a lot of potential producing a lot of products going around the world. And the CCP, we all know, is very good at finding the vulnerabilities of the open societies and manipulate them. We can now just simply sit out and say, "Oh, this is another cold war, and we won the last one, so are definitely going to win this one." There is no guarantee that freedom will prevail unless we make relentless effort and strategy and smart and vigilant. So I just want to say to the committee that you are doing great work.

Finally, that the Chinese Communist Party is using nationalism to mobilize a Chinese mask, and they are using propaganda to mask this nationalism and the CCP rooting in the same thing. But don't estimate -- underestimate the power of nationalism for the individual freedom and such being manipulated in such a digital-controlled environment. So we need to meet that challenge. Thank you.

Mrs. Hinson. Absolutely. Well, on that note, I guess I would follow up with what steps do you think are things that either this committee could do or Congress could do to really counteract that digital propaganda, short of, I mean, just funding, you know, these countermeasures, getting that information out there. But we clearly have a Chinese media state that is colluding with the surveillance state.

Mr. Xiao. Yes. You have the Chinese propaganda state colluding with the surveillance state therefore and with a very strong technology power. That is why we cannot lose this AI competition in this new era. Not only to simply current project funding, but creative thinking and much to the higher level of the measure and that is

what I think the committee you are doing great work. And I hope this hearing is a starting point.

Mrs. Hinson. Thank you. I yield back, Mr. Chair.

Chairman Moolenaar. Thank you.

Representative Cline.

Mr. Cline. Thank you, Mr. Chairman.

Mr. Chairman, the open exchange of ideas is essential to ensuring a free society that can discern what is true without government interference and influence. And it is a central underpinning to the success and human flourishing that has occurred as a result of the American experiment. One thing is for certain: The contents of this publicly held hearing won't be making it through to Beijing. Instead, this hearing will join a long list of censored content, ranging from silly to serious, such as internet memes comparing President Xi to Winnie the Pooh and unfiltered historical accounts of the 1989 Tiananmen Square massacre carried out by the CPP on its own people. This is all due to the vast amounts of resources that the CCP has dedicated to transforming their country into a techno-totalitarian surveillance state to create a great firewall that draws 21st century parallels to the notorious Berlin Wall. The methodology, sophistication, and scale of Beijing's censorship complex utilizes a mix involuntary collection of biometrics, voice prints, facial recognition, and cell phone data combined with dense networks of cameras and so-called convenience police stations in some regions, which has enabled them to surveil, manipulate, or coerce their people to control public debate and prevent challenges to the party's hold on power. However, we have to be cognizant that this troubling authoritarian model is not limited to the PRC's borders as the party has shifted to exporting their tech and censorship know-how abroad.

So, let me ask, Dr. Cooper, besides censoring their own people, focusing in on

exporting surveillance tech abroad, what countries would you say have engaged the most with the PRC in buying this tech? And are there any surprises or notable mentions?

Mr. Cooper. I think a lot of them are going to be the usual suspects: Venezuela, Cuba, obviously Belarus, Russia are going to be more and more reliant on this sort of technology. But there are some surprises, and the place to look first is probably in the safe cities, so-called safe cities projects, which are all around the world. Marseille in France, probably not the kind of place that you would have expected to be looking into safe cities, but this has been attractive in a lot of places. And I think, in many of these locations, the leadership just simply do not understand what they are getting. Safe cities sounds pretty good. I don't think a lot of people would be opposed to that if they don't dig a little further into what is actually being offered.

Mr. Cline. How has the digital Belt and Road initiative changed the geopolitical landscape?

Mr. Cooper. Well, what I would say on digital Belt and Road is that actually the digital Belt and Road -- it used to be sort of the side lines of the all of the infrastructure that China was promising. But, as the amount of money that China has put into Belt and Road has shrunk because the economy is slowing down, the real focus of Belt and Road has become the digital infrastructure side. And so I think, to the extent that we are focused on trying to deal with the challenge that China poses abroad through Belt and Road, the digital aspects of Belt and Road are probably in many ways the most concerning. A typical infrastructure project doesn't give the Chinese the ability to surveil in the future for other governments to censor what their citizens are seeing. Digital Belt and Road is fundamentally different. So I think it has become in many ways the core of what Belt and Road is. And it for us should absolutely be the most concerning aspect of what China is doing through the Belt and Road projects.

Mr. Cline. Do you see the potential or do you detect any perceived weaknesses that you think this initiative could reveal about the CCP that the U.S. could follow up on?

Mr. Cooper. I think there are tremendous weaknesses. For example, we know that Belt and Road promises are about 10 times what is actually delivered. So, you know, most countries, if they are hearing that they are going to get $50 billion of Belt and Road money, they might get 5 if they are lucky. That is a huge, huge failing by China. Some of this is for political reasons, but much of it is just basic economics, right? There is just not as much money to go around in China today as there used to be. So I think that is a weakness. My view, though, is that we can't compete with Belt and Road everywhere. We have to prioritize those places that we think are most strategically important and put our focus on them in a very strictly prioritized way. If we are competing with China in a country, it is almost always the case that we are the preferred provider, right? Countries fall back on China because they don't have other good options. So we have got to be there and provide an attractive alternative.

Mr. Cline. Thank you. I yield back.

Mrs. Hinson. [Presiding.] Mr. Moulton is recognized.

Mr. Moulton. Thank you very much, Madam Chair.

For the United States and China to have a meaningful dialogue for Chinese citizens to understand when the wool is being pulled over their eyes, they have to have access to good information, right? We can't even be on the same sheet of music for having a conversation if one side is living in the dark. And a lot of Chinese citizens are literally living in the dark today.

Mr. Kretchun, in your written testimony, you referred to a Stanford study that found that access to information in itself did not result in Chinese students actively taking advantage of outside information. Only when they were incentivized to do so did they

find uncensored info. So, given the constant cat and mouse game that organizations like yours engage in with the CCP to provide tools for open internet access, another way to expose Chinese citizens to internet freedom is not when they are in their country, but just when they spend time in societies like ours. Is there any indication that, when Chinese citizens who have lived in the United States returned to China, they continue to find ways to access the global internet?

Mr. Kretchun. Absolutely. Some of the most sophisticated circumvention users in China are those who have spent significant time overseas, and not only because they have learned about the kinds of technologies that are available that they can kind of then maintain access to when they are back in China, but also because they have motivation. They have friends. They have entertainment or news sources they are used to consuming. And, when they go back, they don't want to let those go. And so they have not only some knowledge of the tools that can unlock those but also a really strong motivation to continue to access that. And so, when those seeds are planted and folks by, you know, traveling by studying somewhere else, that is one of the most effective ways to actually ensure that that motivation continues.

Mr. Moulton. It is actually a compelling reason to make sure we still bring Chinese students to the United States, even though we obviously have to be concerned and careful that we scrutinize those applications to ensure that we are bringing in Chinese citizens and not Chinese spies.

Tell me, what are other ways that we can plant those seeds, as you say, to motivate other Chinese citizens back at home to want to get the truth?

Mr. Kretchun. I think it is going to be much more incumbent on us to understand the particular needs and what is being systematically denied to smaller subgroups than we are used to working with. Normally, from the OTF perspective, we build a really

good VPN, and then we expect folks to know how to find it and know how to use it and basically resume their lives on the global internet as if censorship didn't exist.

In China, what we are going to have to do is look at much smaller subpopulations, understand those needs, and then how they are attempting to get information already. Folks in China are very resourceful and figure out ways to get a bunch of the information they need when truly motivated, you know. There are tens of millions of internal migrants who effectively don't have the right [inaudible] for where they live. That is a really -- they are systematically denied resources and then also, like, information about that. That is a great population that you could serve important news to, and they already look for it in certain spots. So we need to figure out ways to put the right information in those spots and to take tools that will allow them to access the global internet more fully and meet them where they are already. And that takes a lot more work. That is more expensive on a per-user basis than say uncensoring a user in Iran or Russia, but it is worthwhile.

Mr. Moulton. I think we all have the crazy uncle who gets a conspiracy theory and then tracks this thing down like crazy on the internet, maybe changes his voting habits as a result, right? I would love to see a more proactive strategy to plant seeds, not of conspiracy theories but just seeds of truth in Chinese societies. So, beyond VPNs, are there other tools that we can use to motivate Chinese citizens to want the truth?

Mr. Kretchun. Absolutely. I mean, it will come down to increased support for the kind of news and reporting that frankly isn't being done in a very good systematic way right now. Reporters in general are farther away from Chinese audiences than they have ever been. Having isolated the domestic information environment, it is really hard now to do the job of journalism inside of China, much less disseminate it back in. So ensuring that we are supporting good journalism that is coming out of China and then

innovative ways to put it back in where folks are actually able to find it is going to be a difficult task but one that we really need to focus on.

Mr. Moulton. Dr. Cooper, I am sorry we don't have much time left, but anything to add to this?

Mr. Cooper. I will just say that I think it is absolutely critical that so many of the top reporters on China, they, first of all, have been kicked out of China, but to the extent that they are still reporting on China, the Chinese people can't see the reporting. I mean, just the last few days, there has been an important report about what appears to be some corrupt activity from senior officials associated with major businesses in China, and yet, of course, you can read that; I can read that; but people in China can't. And I think the tools and techniques that we are talking about are the beginning of trying to address that gap.

Mr. Moulton. Thank you. I am out of time. It is hard to imagine corrupt behavior from the senior Chinese officials.

With that ironic statement, I yield back.

Mrs. Hinson. Well, I thank you again to all of our witnesses today. A great hearing, and we have a lot to do, right?

Questions for the record are due one week from today.

And, without objection, the committee hearing is adjourned.

[Whereupon, at 12:03 p.m., the committee was adjourned.]