INFORMATION CONTROLS, GLOBAL MEDIA INFLUENCE, AND CYBER WARFARE STRATEGY

HEARING

BEFORE THE

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

ONE HUNDRED FIFTEENTH CONGRESS
FIRST SESSION

THURSDAY, MAY 4, 2017

Printed for use of the
United States-China Economic and Security Review Commission
Available via the World Wide Web: www.uscc.gov

UNITED STATES-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

WASHINGTON: 2017

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

CAROLYN BARTHOLOMEW, *CHAIRMAN*
HON. DENNIS C. SHEA, *VICE CHAIRMAN*

Commissioners:

ROBIN CLEVELAND	HON. JONATHAN N. STIVERS
HON. BYRON L. DORGAN	HON. JAMES TALENT
HON. CARTE P. GOODWIN	DR. KATHERINE C. TOBIN
DR. GLENN HUBBARD	MICHAEL R. WESSEL
DANIEL M. SLANE	DR. LARRY M. WORTZEL

MICHAEL R. DANIS, *Executive Director*

The Commission was created on October 30, 2000 by the Floyd D. Spence National Defense Authorization Act for 2001 § 1238, Public Law No. 106-398, 114 STAT. 1654A-334 (2000) (codified at 22 U.S.C. § 7002 (2001), as amended by the Treasury and General Government Appropriations Act for 2002 § 645 (regarding employment status of staff) & § 648 (regarding changing annual report due date from March to June), Public Law No. 107-67, 115 STAT. 514 (Nov. 12, 2001); as amended by Division P of the "Consolidated Appropriations Resolution, 2003," Pub L. No. 108-7 (Feb. 20, 2003) (regarding Commission name change, terms of Commissioners, and responsibilities of the Commission); as amended by Public Law No. 109-108 (H.R. 2862) (Nov. 22, 2005) (regarding responsibilities of Commission and applicability of FACA); as amended by Division J of the "Consolidated Appropriations Act, 2008," Public Law Nol. 110-161 (December 26, 2007) (regarding responsibilities of the Commission, and changing the Annual Report due date from June to December); as amended by the Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015, P.L. 113-291 (December 19, 2014) (regarding responsibilities of the Commission).

The Commission's full charter is available at www.uscc.gov.

July 27, 2017

The Honorable Orrin Hatch
President Pro Tempore of the Senate, Washington, D.C. 20510
The Honorable Paul Ryan
Speaker of the House of Representatives, Washington, D.C. 20515

DEAR SENATOR HATCH AND SPEAKER RYAN:

We are pleased to transmit the record of our May 4, 2017 public hearing on "China's Information Controls, Global Media Influence, and Cyber Warfare Strategy." The Floyd D. Spence National Defense Authorization Act for 2001 § 1238, Pub. L. No. 106-398 (as amended by the Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015 § 1259b, Pub. L. No. 113-291) provides the basis for this hearing.

At the hearing, the Commissioners heard from the following witnesses: Xiao Qiang, Adjunct Professor, School of Information, University of California, Berkeley; Margaret Roberts, Assistant Professor of Political Science, University of California, San Diego; Sophie Richardson, China Director, Human Rights Watch; Dan Southerland, Former Executive Editor, Radio Free Asia; Shanthi Kalathil, Director, International Forum for Democratic Studies, National Endowment for Democracy; Sarah Cook, Senior Research Analyst for East Asia, Freedom House; Chris C. Demchak, Grace M. Hopper Professor of Cyber Security and Director, Center for Cyber Conflict Studies (C3S), U.S. Naval War College; and James A. Lewis, Senior Vice President, Center for Strategic and International Studies. The subjects covered included the mechanisms the Chinese government uses to censor information in China, China's repression of journalists, China's influence on media in the United States and other countries, and China's views of norms in cyberspace. It specifically examined the effectiveness of Beijing's information control mechanisms, the methods employed by Internet users in China to circumvent these mechanisms, and Chinese acquisitions of U.S. film studios and cinemas. Additionally, this hearing explored Beijing's view of Internet sovereignty and Chinese computer network operations doctrine.

We note that the full transcript of the hearing will be posted to the Commission's website when completed. The prepared statements and supporting documents submitted by the participants are now posted on the Commission's website at www.uscc.gov. Members and the staff of the Commission are available to provide more detailed briefings. We hope these materials will be helpful to the Congress as it continues its assessment of U.S.-China relations and their impact on U.S. security.

The Commission will examine in greater depth these issues, and the other issues enumerated in its statutory mandate, in its 2017 Annual Report that will be submitted to Congress in November 2017. Should you have any questions regarding this hearing or any other issue related to China, please do not hesitate to have your staff contact our Congressional Liaison, Leslie Tisdale, at 202-624-1496 or ltisdale@uscc.gov.

Sincerely yours,

Carolyn Bartholomew
Chairman

Hon. Dennis C. Shea
Vice Chairman

cc: Members of Congress and Congressional Staff

CONTENTS

THURSDAY, MAY 4, 2017

CHINA'S INFORMATION CONTROLS, GLOBAL MEDIA INFLUENCE, AND CYBER WARFARE STRATEGY

Panel III: Beijing's Views on Norms in Cyberspace and China's Cyber Warfare Strategy

INFORMATION CONTROLS, GLOBAL MEDIA INFLUENCE, AND CYBER WARFARE STRATEGY

THURSDAY, MAY 4, 2017

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

Washington, D.C.

The Commission met in Room 2255 of Rayburn House Office Building, Washington, DC at 9:30 a.m., Chairman Carolyn Bartholomew and Commissioner Larry M. Wortzel (Hearing Co-Chairs), presiding.

OPENING STATEMENT OF CHAIRMAN CAROLYN BARTHOLOMEW HEARING CO-CHAIR

CHAIRMAN BARTHOLOMEW: All right. Good morning, everybody. Thank you so much for appearing today to our witnesses and thank you to the audience for coming. It's an important topic. We have some old friends among us, which is always wonderful to see. One of these days, of course, I'd love to have people come in and say, well, we don't have anything to testify about because the problems have all been solved. But we are definitely, definitely not there.

So welcome to the fifth hearing of the U.S.-China Economic and Security Review Commission's 2017 Annual Report cycle.

Our first panel will address censorship and Internet controls within China. The Chinese Communist Party, as most people know, relies on what is known as the Great Firewall, an assortment of sophisticated electronic censorship and surveillance mechanisms, to monitor online activity within China's borders.

It prevents web users within China from accessing foreign ideas, which the Party regards as an ideological threat. It also allows the CCP to maintain effective control over the news by blocking sensitive stories.

Curious web users in China have learned to "climb the Wall" and access forbidden information, but the Party has increasingly made it more difficult to do so. In addition to maintaining a firm grip on what ideas are allowed to penetrate China's borders, the Chinese government assiduously engages in what it calls "public opinion guidance," using state-sponsored content spammers to intervene in online discussions in order to distract from sensitive topics.

The activities of these spammers were not previously well understood, but thanks in part to leaked internal communications from a local Chinese propaganda department, and to the work of our witnesses, recent research has been able to shed more light on this issue.

The CCP's censorship and control of the Internet violate Article 19 of the Universal

Declaration of Human Rights, which says: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

For people who wonder why we in the United States should care if the Chinese people have access to the free flow of information, I will note that Chinese restrictions on information have an impact on our economy, functioning as a trade barrier by, among other things, keeping U.S. companies from reaching Chinese consumers.

They also threaten our national security, fueling a rise in Chinese nationalism and depriving Chinese citizens of a fuller understanding of differing views on situations where escalating tensions raise serious concerns about the potential for conflict.

In our second panel today, we'll hear about an issue that has been a growing topic of concern here on Capitol Hill: Beijing's efforts to manipulate global coverage of China, including its attempts to increase its own soft power by gaining influence over the American film industry.

The Chinese leadership sees American soft power as a major obstacle to China's rise. To counter this aspect of "soft power," the CCP seeks not only to prohibit negative portrayals of China in popular culture but also to curtail positive depictions of the United States while incentivizing Hollywood to portray China positively.

Acquisitions by Chinese companies of cornerstone companies in the U.S. film industry have economic and security implications for the United States. The Commission has followed this topic for some time, including in our most recent Annual Report to Congress, which recommended reforms to strengthen the Committee on Foreign Investment in the U.S., CFIUS.

We will also hear about the current situation for journalists in China, both foreign and Chinese, who have in recent years been subjected to markedly increased harassment by the Chinese government.

In addition to cracking down on investigative and independent journalism within China, the Chinese government has redoubled its efforts to develop the international presence of state-approved Chinese reporting in order to make sure that foreign news coverage of China in peripheral countries stays on message.

We look forward to hearing about these very important topics from our esteemed experts, and we especially look forward to hearing their recommendations for Congress. I would also like to thank the House Foreign Affairs Subcommittee on Asia and the Pacific for helping to secure today's hearing venue and will turn to my co-chair, Dr. Larry Wortzel, for his opening remarks.

PREPARED STATEMENT CHAIRMAN CAROLYN BARTHOLOMEW
HEARING CO-CHAIR

Hearing on "Information Controls, Global Media Influence, and Cyber Warfare Strategy"

Opening Statement of Carolyn Bartholomew
May 4, 2017
Washington, DC

Good morning, and welcome to the fifth hearing of the U.S.-China Economic and Security Review Commission's 2017 Annual Report cycle.

Our first panel will address censorship and Internet controls within China. The Chinese Communist Party relies on what is known as the Great Firewall, an assortment of sophisticated electronic censorship and surveillance mechanisms, to monitor online activity within China's borders. It prevents web users within China from accessing foreign ideas, which the Party regards as an ideological threat. Additionally, it allows the CCP to maintain effective control over the news by blocking sensitive stories. Curious web users in China have learned to "climb the Wall" and access forbidden information, but the Party has increasingly made it more difficult to do so. In addition to maintaining a firm grip on what ideas are allowed to penetrate China's borders, the Chinese government assiduously engages in what it calls "public opinion guidance," using state-sponsored comment spammers to intervene in online discussions in order to distract from sensitive topics. The activities of these spammers were not previously well understood, but thanks in part to leaked internal communications from a local Chinese propaganda department, recent research has been able to shed more light on this.

The CCP's censorship and control of the Internet violate Article 19 of the Universal Declaration of Human Rights: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." For people who wonder why we in the United States should care if the Chinese people have access to the free flow of information, I will note that Chinese restrictions on information have an impact on our economy, functioning as a trade barrier by, among other things, keeping U.S. companies from reaching Chinese consumers. They also threaten our national security, fueling a rise in Chinese nationalism and depriving Chinese citizens of a fuller understanding of differing views on situations where escalating tensions raise serious concerns about the potential for conflict.

In the second panel, we will hear about an issue that has been a growing topic of concern on Capitol Hill: Beijing's efforts to manipulate global coverage of China, including its attempts to increase

its own soft power by gaining influence over the American film industry. The Chinese leadership sees American soft power as a major obstacle to China's rise. To counter this aspect of "soft power", the CCP seeks not only to prohibit negative portrayals of China in popular culture but also to curtail positive depictions of the United States while incentivizing Hollywood to portray China positively. Acquisitions by Chinese companies of cornerstone companies in the U.S. film industry have economic and security implications for the United States. The Commission has followed this topic for some time, including in our most recent Annual Report to Congress, which recommended reforms to strengthen the Committee on Foreign Investment in the United States.

We will also hear about the current situation for journalists in China, both foreign and Chinese, who have in recent years been subjected to markedly increased harassment by the Chinese government. In addition to cracking down on investigative and independent journalism within China, the Chinese government has redoubled its efforts to develop the international presence of state-approved Chinese reporting in order to make sure that foreign news coverage of China in peripheral countries stays on message.

We look forward to hearing about these very important topics from the esteemed experts we have here today, and we especially look forward to their recommendations. I would also like to thank the House Foreign Affairs Subcommittee on Asia and the Pacific for helping to secure today's hearing venue.

I would like to turn now to my co-chair Dr. Larry Wortzel for his opening remarks.

OPENING STATEMENT OF COMMISSIONER LARRY M. WORTZEL HEARING CO-CHAIR

HEARING CO-CHAIR WORTZEL: Good morning. I want to join Chairman Bartholomew in welcoming you and all the experts who have joined us today.

The third panel today will address Beijing's views on norms in cyberspace and China's cyber warfare strategy. The Chinese government advocates for a concept known as "Internet sovereignty" in which countries have the right to control their part of cyberspace. And it also asserts that Internet governance should be the purview of national governments and no other actors, which really contrasts with the "multi-stakeholder" model that the United States and certainly others in Europe currently use and is in place. And it would mean that the Internet is no longer a virtual common.

The Chinese government has declared that cyberspace and space are now the "new commanding heights in strategic competition." That means war starts there.

In 2015, the end of 2015 and through last year, the Strategic Support Force was established as part of the ongoing reform and reorganization of the Chinese military. Its missions include network warfare and other forms of cyber operations, information warfare, including propaganda and media warfare and legal warfare, electronic warfare, and space missions.

And Chinese military writings refer to offensive, defensive and reconnaissance activities in the network domains. And they intend to get into an adversary's networks, reconnoiter them, and do what they can to take them out.

We're going to seek insights into these developments in today's hearing so the Commission may provide Congress with some recommendations on the topic.

Just to remind you that the hearing will be posted on our website at www.uscc.gov. You'll find a lot of our annual reports, our staff reports there, and links to news about China. The next hearing will be on June 8 on "China's Relations with Northeast Asia and Continental Southeast Asia," and I have the honor of introducing our first panel experts. So I'll do that right now.

PREPARED STATEMENT OF COMMISSIONER LARRY M. WORTZEL
HEARING CO-CHAIR

Hearing on "Information Controls, Global Media Influence, and Cyber Warfare Strategy"

Opening Statement of Commissioner Larry M. Wortzel
May 4, 2017
Washington, DC

Good morning. I join Chairman Bartholomew in welcoming and thanking the experts who have joined us here today.

The third panel of today's hearing will address Beijing's views of norms in cyberspace and China's cyber warfare strategy. The Chinese government advocates for a concept known as "Internet sovereignty" in which countries have the right to control their part of cyberspace. It also asserts that Internet governance should be the purview of national governments and no other actors, a view which contrasts with the "multi-stakeholder" model, supported by the United States and others, that is currently in place. That would mean that the internet would not be a global virtual common.

The Chinese government has declared that cyberspace and space are "new commanding heights in strategic competition." In 2015, the Strategic Support Force was established as part of the ongoing reform and reorganization of the Chinese military. The force's missions include network warfare and other forms of cyber operations, electronic warfare, and space missions. Chinese writings refer to "network warfare," which encompasses offensive, defensive, and reconnaissance activities in the "network domain" or "network space."

We seek insights into these and other developments related to the subject of today's hearing so that the Commission may provide the Congress with recommendations.

As a reminder, the testimonies and transcript from today's hearing will be posted on our website at www.uscc.gov. You will find a number of other resources there, including our Annual Reports to Congress, staff reports, and links to important news stories about China and U.S.-China relations. The Commission will be holding its next hearing on June 8th on "China's Relations with Northeast Asia and Continental Southeast Asia."

I will now introduce the experts on this hearing's first panel, which will discuss China's domestic information controls and their implications.

PANEL I INTRODUCTION BY COMMISSIONER LARRY M. WORTZEL

We're going to start with Professor Xiao Qiang of the School of Information at Berkeley, University of California-Berkeley, a place that we all know supports free speech.

[Laughter.]

HEARING CO-CHAIR WORTZEL: Didn't the free speech movement start there? For those of us that are that old.

[Laughter.]

HEARING CO-CHAIR WORTZEL: He's the founder and editor-in-chief of China Digital Times, and his website tracks Chinese censorship.

Professor Xiao was the executive director of the New York-based NGO Human Rights in China through the '90s, and he received a MacArthur Fellowship in 2001. He runs Berkeley's Counter-Power Lab, which is an interdisciplinary faculty-student group researching innovative technologies to expand the free flow of information in cyberspace.

He has a Bachelor of Science degree from the University of Science and Technology in China and studied astrophysics at Notre Dame. We're very happy to have him back. He's been here many times, and he's a good friend of the Commission.

We'll hear after that from Dr. Margaret Roberts. This is Dr. Roberts' first time, I think.

CHAIRMAN BARTHOLOMEW: You're among friends.

[Laughter.]

HEARING CO-CHAIR WORTZEL: We're gentle on this topic. As long as you don't say anything we don't like.

[Laughter.]

HEARING CO-CHAIR WORTZEL: Dr. Roberts is an adjunct professor in the Department of Political Science at UC-San Diego--a great location. You should invite us out. Her research focuses on better measuring and understanding the political information strategies of authoritarian governments with a specific focus on censorship and propaganda in China. She's developed widely used methods for automated content analysis in the social sciences, and she holds degrees from Stanford and Harvard.

Thank you for being here.

And the third panelist is another person that we rely on and has been here many times--Sophie Richardson. She's the director, China Director for Human Rights Watch. She's a graduate of the University of Virginia and the Johns Hopkins-Nanjing Program--near and dear to my heart--and Oberlin College.

Dr. Richardson is the author of a number of articles on domestic Chinese political reform, democratization, and human rights in Cambodia, China, Indonesia, Hong Kong, the Philippines and Vietnam. She's also the author of China, Cambodia, and the Five Principles of Peaceful Coexistence, which examines China's foreign policies since the 1954 Geneva Conference, and it really is a remarkable piece of work of great interviews of policymakers.

We told you that we don't have this sophisticated timing system.

CHAIRMAN BARTHOLOMEW: We're going back to the analog day.

HEARING CO-CHAIR WORTZEL: We're going to hold up a sign.

[Laughter.]

HEARING CO-CHAIR WORTZEL: And I'll relay it. If you don't notice, if you're busy-

COMMISSIONER WESSEL: He's going to jump up.

HEARING CO-CHAIR WORTZEL: He's going to jump. All right. So it will be seven minutes, and then there will be plenty of time for questions and answers.

Thank you very much. And Dr. Xiao, it's you

OPENING STATEMENT OF MR. XIAO QIANG, ADJUNCT PROFESSOR SCHOOL OF INFORMATION UNIVERSITY OF CALIFORNIA, BERKELEY

MR. XIAO: Good morning, Chairman, Commissioners, everyone. It's an honor to be here again in front of this important Commission among my distinguished fellow panelists.

Ever since assuming the power, Chinese President Xi Jinping has made China's cyber sovereignty a top priority in his sweeping campaign to bolster regime security.

Over the course of the last four years, Xi's government has issued numerous regulations that increase restrictions on Internet communications and tighten the control of free flow of information.

Just two days ago, on May 2, the Cyberspace Administration of China issued a comprehensive update to regulations requiring all websites that distribute news, including websites, apps, forums, blogs, microblogs, public accounts from WeChat, instant messaging tools, and Internet broadcasts, to obtain government licenses.

The rules also require domestic businesses that want to set up a joint venture with foreign partner or accept foreign funding to get permission from the State Internet Information Office.

Another major development in the Chinese government's control of online public opinion in recent years is to utilize mass numbers of "Internet commentators," or we just mentioned as content spammers. In Chinese, we call them "Fifty Cent Party." That refers to the Internet commentators who are organized and often paid by the government to write on line in favor of government policies, attacking public intellectuals, boosting Xi Jinping's image, or monitoring netizens' activities, often using a fake identity.

In 2015, an anonymous Chinese Twitter user leaked actually five archives of the email communications of propaganda officials in different parts of China, including Communist Youth League branch in charge of all universities in Shanghai, another one in charge of all universities in Fujian, and a local Internet Information Office in Jiangxi Province.

These important leaks shed light on the secret work of the Fifty Cent Party. These archives include correspondence, photos, directories of Internet commentators, summaries of the commentary work, and records of the online activities of specific individuals, among other documents, ranging from 2002 to 2015.

From those leaked documents, it is clear that in recent years, the Chinese government has mobilized over ten million college students through its Communist Youth League organization to take on such--they call it--"online public opinion struggle" tasks.

China Digital Times, my website, has set up a website called fiftycentsleaks.info to publicize these leaked emails, making them accessible and searchable by the general public outside of China.

As part of our efforts--let's see. Quick. For the Chinese government, the censorship and propaganda go hand in hand with the violence, physical force, including police visits, arrests, targeted personal attacks through state media. The intensified measures are aimed to shape public opinion and rationalizing, internalizing and legitimizing the Party's primacy and its monopoly of power.

A critical component of Chinese government's information control infrastructure, the so-called Great Firewall of China, has been constantly updated. A research project from my

Counter-Power Lab at the School of Information, UC Berkeley, has systematically measured the blocking technology deployed by the Chinese Great Firewall in recent years.

On our HikingGFW.org website, we have displayed domain names of 1,382 blocked websites, compiled from top 10,000 globally ranked websites. Of course, we all know that, including YouTube, Google, Facebook, Flickr, Twitter, and WordPress.

One thing worth noting is that such censorship and propaganda efforts are most effective when Internet users are not aware of such manipulation and control. Once exposed, these efforts, including the deleting online contents, blocking foreign websites, and polluting the online information environment through the Fifty Cent Party, can also expedite the demise of public trust in the government. This is one of the major consequences of censorship and a primary challenge facing the Chinese government today.

The government's pervasive and intrusive censorship system also generates massive resentment among Chinese netizens, and I'll just give you one example. A month ago, Tsinghua University professor of sociology Sun Liping, who has 5.2 million followers on his Weibo account, posted an essay. The essay's title is "Between Civilization and Barbarism, We Must Not Lose our Way." As an influential public intellectual in China, Professor Sun asked the following powerful questions in his essay, still on China's Internet. I'm going to read three of his sentences:

The transfer of power may be reached via a river of blood, or it may be achieved through a procedure and election that have the approval of the people. Is there any doubt which is civilized and which is barbaric?

Public affairs may be handled by a small group acting arbitrarily, or with broader participation, thus embodying the will of more people. Is there any doubt which is civilized and which barbaric?

In social life, one group of people can have the power to discriminate against and oppress another, or everyone can coexist equally. When genuine equality cannot be realized, at least equality in the sense of the law and of rights can be guaranteed. Is there any doubt which is civilized and which is barbaric?

I quote these voices because it is true that due to the Internet control across all platforms in past four years, there is a clear decline in the lively discussion of social causes in the Chinese social media, as Freedom House 2016 report clearly stated. I agree.

However, beneath the surface of these constantly increasing and intensified control measures, digital activism has been and remains a vital driver of change in Chinese society. The erosion of the Party's old ideological and social control is underway. There are still hundreds of millions of Chinese netizens creating new content with raw materials of their suffering, fears, dreams, and hopes, and sharing their common experiences on social media every day.

There are still millions of grassroots' voices, public opinion leaders, digital activists, and an insurgent community of circumvention practitioners who constantly expand the free flow of information in Chinese cyberspace. It remains to be seen when resistance and rejection become significantly stronger than compliance and acceptance whether government's control of communication and repressive efforts will still be sustainable in the long run.

So I have one recommendation which is simple: I would like to use this opportunity to urge the Congress to significantly increase the Internet freedom funds to support the efforts of

civil society countering the development of repressive Internet-related laws and regulations, researching key threats of Internet freedom, and developing technologies that provide or enhance access to the Internet Thank you, Commission.
.

PREPARED STATEMENT OF MR. XIAO QIANG, ADJUNCT PROFESSOR SCHOOL OF INFORMATION UNIVERSITY OF CALIFORNIA, BERKELEY

Hearing on "Information Controls, Global Media Influence, and Cyber Warfare Strategy"

Testimony before
The U.S.-China Economic and Security Review Commission

May 04, 2017

My name is XIAO Qiang. I am an adjunct professor at the School of Information of UC Berkeley, and the principal investigator of Berkeley Counter-Power Lab, an interdisciplinary faculty-student research group focusing on Internet freedom, based in the School of Information, UC Berkeley. I am also the Founder and Editor-in-Chief of China Digital Times, an independent bilingual news website about China. Over the last 14 years, I have been documenting Chinese government censorship, tracking the impact of emerging social media and online activism, especially in the form of "cultural resistance," and developing cloud-based technologies which can circumvent the Great Firewall. It is an honor to be among my distinguished fellow panelists, in front of this important commission.

Ever since assuming power, Chinese president Xi Jinping has attempted to legitimize the authority of the Communist Party by introducing far-ranging measures to enforce party's rule, including gaining firm ideological and informational control over the media and Internet. Xi has made China's "cyber sovereignty" a top priority in his sweeping campaign to bolster "regime security". In March 2014, the Chinese Communist Party established the Central Leading Group for Cyberspace Affairs with President Xi Jinping as chairman. In November 2016, the country's first cybersecurity law was adopted which requires internet companies to conduct increased surveillance of their networks, conduct mandated security reviews of their equipment, and to provide data to government investigators when requested, among other stipulations. Several foreign business groups opposed the law out of fear of being shut out of various sectors in China.

Over the course of the past five years, Xi's government has issued numerous regulations that increased restrictions on internet communications, and aim to tighten control over news dissemination channels, including social media and mobile phone applications.
Just two days ago, on May 2, 2017, the Cyberspace Administration of China issued a comprehensive update to regulations requiring all websites that distribute news—including "websites, apps, forums, blogs, microblogs, public accounts, instant messaging tools and internet broadcasts"—to obtain government licenses. The rules mark the first comprehensive update to such regulations in 12 years and come into effect on June 1. The rules also require domestic businesses that want to set up a joint venture with a foreign partner or accept foreign funding to get permission from the State Internet Information Office. Also in other recently issued

regulations, CAC requires "network providers and products" used by people who might touch upon "national security and the public interest" to go through security reviews.

Another major development in the Chinese government's control of online public opinion in recent years is to utilize mass numbers of "internet commentators," otherwise known as the "Fifty Cent Party." In China, when major events unfold, a combination of government directives, keyword filtering, post deletion, paid pro-government commentary, and other forms of censorship and propaganda guides the narrative in the direction that the state determines. The name "Fifty Cent Party" refers to internet commentators who are organized and often paid by the government, to write online in favor of government policies, attack "public intellectuals," boost Xi Jinping's image, and monitor netizens' activities, often using fake identities.

In 2015, an anonymous Chinese Twitter user leaked archives of the email communications of propaganda officials in different parts of China, including a Communist Youth League branch in charge of all universities in Shanghai and a local Internet Information Office in Jiangxi Province, which shed light on the secretive work of the "Fifty Cent Party." These archives include correspondence, photos, directories of "internet commentators," summaries of commentary work, and records of the online activities of specific individuals, among other documents, ranging from 2002 to 2015. From those leaked documents, it is clear that in recent years, the Chinese government has mobilized over ten million college students through its Communist Youth League organization to take on such "online public opinion struggle" tasks. China Digital Times has set up a website fiftycentsleaks.info to publicize these leaked emails, making them accessible and searchable by the general public outside of China.

As part of our efforts to monitor and expose censorship, we also track censored content, using tools to archive deleted Weibo posts. Over the past five years, China Digital Times has collected over 2700 leaked censorship instructions from various government bodies, issued from 2004 to 2017. The directives are issued to website managers and editors, often orally, to limit or guide reporting on sensitive subjects, and then leaked online by journalists or others who have a vested interest in free speech. We also have detected and published over 2500 keywords banned from Sina Weibo search results. Among these keywords are 157 words on the subject of the Tiananmen Massacre.

For the Chinese governmet, censorship and propaganda go hand in hand; "consent" and intimidation are backed by the use of physical force, including police visits, arrests, and targeted personal attacks through state media against those who are simply expressing their political views online. According to Freedom House' 2016 report, "as in past years, dozens of domestic internet users were investigated for digital crimes from disseminating misinformation to promoting tools to circumvent censorship, and one Uyghur teenager was reported to have been imprisoned for life for watching banned videos on a cellphone." These intensified censorship and information control measures are aimed at shaping public opinion and rationalizing, internalizing, and legitimizing the Party's primacy and its monopoly of power through public discourse in China.

Finally, as a critical component of the Chinese government's information control infrastructure, the so-called "Great Firewall of China" has been constantly updated in order to restrict transnational internet connections and block potentially subversive sites. A research project from my Counter-Power Lab at the School of Information, UC Berkeley has systematically measured the blocking technology deployed by the Chinese Great Firewall in recent years. On the HikingGFW.org website, we have displayed domain names of 1382 blocked websites, compiled from Alexa's top 10,000 globally ranked websites. These websites include YouTube, Google, Facebook, Flickr, Twitter and WordPress. Early this year, the Ministry of Industry and Information Technology started a campaign against unauthorized internet connections, including virtual private network services that enable internet users to bypass the Great Firewall.

One thing worth noting is that such censorship and propaganda efforts are most effective when Internet users are not aware of such manipulation and control. Once exposed, these efforts, including deleting online contents, blocking foreign websites and polluting the online information environment via the "Fifty Cent Party," can also expedite the demise of public trust in the government. This is one of the major consequences of censorship and a primary challenge facing the Chinese government today.

The government's pervasive and intrusive censorship system has also generated massive resentment among Chinese netizens. This is true especially since the advent of Weibo and WeChat in recent years. Keyword filtering, post deletion, closing of user accounts, and real name registration policies have not been able to fully control online political discussion and public opinion. In fact, censorship often fuels netizens' determination to discuss sensitive topics. As a result, new forms of social resistance and demands for greater freedom of information and expression are often expressed in coded language and implicit metaphors, which allow them to avoid outright censorship.

As one of the latest examples of such coded-resistance, since last year, an ordinary Chinese family name "Zhao" became popular political lingo, conveying subversive meaning in social media conversatons. Originally named after a landlord family in Chinese writer Lu Xun's novel, The True Story of Ah Q, "Zhaos" now refers to someone enmeshed in China's power structure. For millions of netizens who are commonly using this new term, looking at China as "Zhao country" sheds light on the true nature of power. What's more, the use of "Zhao family" represents resistance to false patriotic propaganda, and dissatisfaction with the current political situation.

According to Qiao Mu, a former associate professor of communications at Beijing Foreign Studies University and a well-known political commentator on Chinese social media, this is an example of "a rebellious deconstruction of official language in the Internet age." It converts the terms from the relatively narrow role of expressing resistance to the much broader one of conceiving how the world really is, and offers a way to change the status quo. When "Zhao country" is used specifically as a jab at the regime, it is a tool with a purpose and can be

countered with a return jab. But when it reflects and expresses normality, much more is at stake. The question of an alternative worldview and new political identity emerges. There, in those myriad corners, such "resistance discourse" can begin to rot the foundation on which bullying and corruption rest, and "prepare the ground" for more significant change. By egaging such "cultural resistance," Chinese netizens overcome the powerlessness of their solitary despair, they became "citizens of the information age," and produce an alternative discourse that has the potential to overwhelm the censorship and propaganda capacity of the Chinese state. One can even hope that regime change, when it eventually arrives, will be more likely to be peaceful than violent insofar as the ground for it has been softened.

Let's also take a look at some other recent examples that demonstrate the widespread online resistance in Chinese society today. In June 2016, 78 scientists from the Chinese Academy of Science submitted a joint statement to Chinese President Xi Jinping, urging the authorities to loosen control over the web and grant them expanded access. On March 1, 2017, Chinese educator and agriculture scientist Luo Fuhe issued a proposal to speed up access to foreign websites. In the proposal, Luo complained of the scientific and economic cost of current internet controls, citing long load times for some valuable sites and the unreliable VPNs or even foreign travel to which many researchers resort. His suggested remedies included a general unblocking of academic and scientific resources, and greater clarity around remaining controls with the compilation of an authoritative list of "negative foreign sites." Even in the case of news, he added, information should not be blocked simply because it is "contested."

What's significant about Luo's seemingly moderate proposal is that he is also a current vice-chair of Chinese People's Political Consultative Conference, a political consultative body that meets annually alongside the National People's Congress. It is also interesting as Luo's approach is apparently aimed at rallying public opinion to put pressure on the government to act. Otherwise, he could have used the traditional approach of submitting his proposal without making it public.

In Spring 2017, Tsinghua University Professor of Sociology Sun Liping , who has 5.2 million followers on his Weibo account, posted an essay titled "Between Civilization and Barbarism, We Must Not Lose Our Way." As an influential public intellectual in China, Professor Sun asked the following powerful questions in his essay:

> The transfer of power may be reached via a river of blood, or it may be achieved through a procedure and election that have the approval of the people. Is there any doubt which is civilized and which barbaric?
>
> Public affairs may be handled by a small group acting arbitrarily, or with broader participation, thus embodying the will of more people. Is there any doubt which is civilized and which barbaric?
>
> In social life, one group of people can have the power to discriminate against and

> oppress another, or everyone can coexist equally. When genuine equality cannot be realized, at least equality in the sense of the law and of rights can be guaranteed. Is there any doubt which is civilized and which barbaric?

I am quoting these voices of online resistance to demonstrate the following trend I have observed in Chinese cyberspace over the past decade: despite the intensified state censorship and information control, the rise of the internet and social media has increased the ability of Chinese citizens to produce their own messages and consistently contest the Chinese government's ideological control and propaganda. But it is also true that due to the stricter internet control across all platforms in past four years, there is a clear decline in the lively discussion of social causes which used to characterize popular microblogs.

However, beneath the surface of these constantly increasing and intensified control measures, digital activism has been and remains a vital driver of change in Chinese society, and the erosion of the Party's old ideological and social control is underway.
There are still hundreds of millions of Chinese netizens create new content with the raw materials of their suffering, fears, dreams, and hopes, and sharing their common experiences on social media everyday. There are also millions of grass-root voices, public opinion leaders, digital activists and an insurgent community of circumvention practitioners who constantly push to expand the free flow of information in Chinese society. It remains to be seen when resistance and rejection become significantly stronger than compliance and acceptance, whether government's control of communication and repressive efforts will still be sustainable in the long run.

Conclusion:

I would like to use this opportunity to urge the Congress to significantly increase the Internet freedom funds to support the efforts of civil society countering the development of repressive internet-related laws and regulations, researching of key threats to Internet freedom; and developing technologies that provide or enhance access to the Internet.

APPENDIX 1. Proposal to Improve and Increase Speed of Access to Foreign Websites

(Ahead of the recent Two Sessions meetings of the National People's Congress and the Chinese People's Political Consultative Conference in Beijing, 2017, CPPCC vice-chair Luo Fuhe raised a proposal on improving the speed of access to foreign websites. Propaganda authorities ordered websites to immediately find and delete coverage of Luo's proposal, which framed an argument for liberalization of China's intense internet controls in terms of scientific progress and economic development.)

The Fifth Plenary Session of the CCP's 18th Central Committee systematically discussed "Five Great Development Concepts." Included among these was the important topic of Open Development. In his 2015 Government Work Report, Premier Li Keqiang debuted the concept of "Internet Plus," emphasizing its importance in the context of Open Development, and expressing hope to use the internet, the internet of things, 24-hour design and other means to drive traditional industries to create a new economic growth point. Normal State Council meetings also focused on the construction of high-speed broadband internet, proposing that "increased speed and reduced fees can improve people's lives and also reduce the cost of entrepreneurial innovation, and provide strong support for 'Internet Plus'." We wholeheartedly endorse this development concept, and recognize that the establishment of fast, efficient, and free-flowing international and domestic network environments will become an important method to better implement the concept of Open Development, and to promote the economic and social development of the nation.

However, the current trend is that the speed of accessing foreign websites from within China is becoming increasingly slow. This will have an enormous impact on China's social and economic development, and on scientific research, and so we need to elevate our concern. For example, connections to the Food and Agriculture Organization of the United Nations or many foreign university websites are all very slow, opening a single page needing a minimum of 10-20 seconds. Some foreign university websites require a half hour or longer before finally loading. The research needs of many domestic expert scholars and graduate students require them to purchase circumvention software in order to access foreign websites. Some international students visiting family back in China are unable to complete and file required forms because they are unable to open their foreign university websites. Some expert scholars working in China must use their weekends or vacations to go to Hong Kong or other places to visit sites required for their research. Firms in China who visit foreign sites and find it very slow also have complaints: in September 2016 the German Chamber of Commerce in China conducted its annual confidence survey of German businesses in China, which showed network supervision, slow access to overseas sites, and a lack of intellectual property protection to be unfavorable restricting factors. This year, Taiwanese delegates to the CPPCC and major leaders of the forum also reported in an informal discussion that many sites couldn't be accessed normally from the mainland. Additionally, some well-known foreign search engines do not operate normally in China.

The following factors lead to slow domestic access of overseas sites:

1) China's outbound internet bandwidth is not sufficient. China's access to the global internet

has bandwidth restrictions, known as international gateway. The greater the bandwidth, the faster the connection to foreign websites. With the steadily increasing number of internet users, China's present international internet gateway bandwidth is clearly insufficient. According to CNNIC data, by the end of 2015, China's backbone international export bandwidth was 5,392,116Mb/second, an increase of 30.9% from 2014; but, the per capita bandwidth was only 4.04Kb/sec. This data is only 1/12 of the world's per capita main bandwidth, and only ½ of Africa's.

2) Internet supplier restrictions. Currently, there are very few providers of international network acceleration services, and they cannot meet network access needs. At the same time, mobile internet users are increasing rapidly. Ministry of Industry and Information Technology statistics show that at the end of 2015 China had reached 946 million mobile internet users, of which over 900 million were cellphone internet users. As a result, many network providers have switched their service focus to mobile terminals, making computer network speed improvement more of a challenge.

3) Strict internet supervision. According to provisions related to the State Council's "Regulation on Internet Information Service Management," and "Regulation on Telecommunications of the PRC," China inspects and blocks certain foreign websites, mainly targeting search engines which refuse to filter results in accordance with Chinese laws and regulations; social networking sites which allow illegal domestic organizations to publicize their activities; as well as propaganda sites for hostile forces and terrorist groups. While we agree that the monitoring and blocking of foreign websites cannot be neglected as part of government efforts to protect the nation's peace and stability, we must also note that many foreign sites are not political, such as common websites for research, education, news, etc. In the interest of domestic scientific research, these foreign sites are a preferred source for obtaining the latest and most accurate information. If these sources cannot be accessed smoothly, the accuracy and timeliness of studies cannot be guaranteed. At present, there are many influential foreign news channels among the sites that have been checked and blocked, sites that are key for both retrieving and publishing information. It is worth debating the fact that all of this information is cut off simply because some of it is contested.

For these reasons, I raise the following suggestions:

1) Increase the outbound internet bandwidth. Increase investment and efforts in network service hardware infrastructure construction, accelerate submarine fiber optic cable construction, and take another step towards raising the outbound internet bandwidth. This would also encourage China's telecommunications companies and IT service firms to build networks and servers overseas, and to provide network infrastructure and acceleration services.

2) Encourage operators to increase attention to computer terminal speed upgrades. Rapidly develop the supply of international network acceleration services, encourage network

operators to consider computer terminal speed, increase the use of computer network bandwidth, and raise the speed of accessing foreign sites.

3) Establish an authoritative list of negative foreign sites. Websites that contain content in violation of the "Regulation on Internet Information Service Management," and "Regulation on Telecommunications of the PRC," and other relevant laws and regulations should be on the list; they need to be strictly regulated and blocked from access; regarding non-political websites, especially foreign university and research sites frequently visited by expert researchers and scholars, lift access restrictions and inspect them regularly; regarding neutral websites including search engines, news, technology, etc., filter sensitive content and carry out regular inspections in order to increase the efficiency of utilizing foreign internet resources. At the same time, websites with content that varies from page to page should be treated differently. Narrow down the negative list to specific webpages for more precise control over content access.

(Source: http://chinadigitaltimes.net/2017/03/translation-censored-proposal-ease-internet-control/)

APPENDIX 2: Deconstructing Family and Country: The Bankruptcy of Patriotism in "Zhao Country"

Xiyu Xuefan

1. As a country of powerful officials, it's an indisputable fact that China is practicing bigwig capitalism. It's been years since the name "Celestial Empire" replaced "China." A deconstruction that serves as a redefinition must always come close to the essence. Recently, there's also been the expression "your country," which is the kind of demarcation that gradually creates distance. In short, fart people are at odds with this country's identity, no matter if you call it New China, the republic, our country, or the motherland.

The benefits paid out after the death of farmer Xu Chunhe demonstrated how difficult, disappointing, violent, and costly it can be for a country's "underclass" to demand its rights. Education, medical treatment, retirement, and housing are four huge mountains to the ordinary citizen, and those mountains can crush them. Recently, a rural girl with good grades in her second year of high school committed suicide by jumping off an overpass because she was hungry. An ordinary woman who couldn't afford to seek medical treatment guiltily gave way to her illness. Left behind children commit joint suicide. Capsizing, exploding, collapsing… On one hand, calamity rains down on ordinary citizens, and on the other hand, the Big Guy is out seeing the world and spending money. The Red Empire looks a lot like the Celestial Empire of the Qing. It's as if they're all abiding by the royal teaching that one should "prefer the company of foreign countries over domestic slaves." Otherwise, there wouldn't be talk on the street of how "the U.S. can use China's money, Africa can, South Korea can, the government can, the officials can, the rich second generation can, and the mistresses can; it's only the common people who can't use it." But while "Celestial Empire" may fit the current dynasty, it's from the Qing. In this age where reality is bigger than imagination, using something just once dooms it to transience.

2. Downstairs from my home is a nursery school franchise. Every day when it's time to raise the flag, I hear this kind of mania: "I love China, I love the five-star red flag …." This isn't unusual. Patriotism is a lifelong process of brainwashing that starts from infancy. Thus, love of country is equated to love of government, and tyrants are really great liberators. The inability to distinguish between despotic totalitarianism and universal democracy, common sense and heresy, human rights and sovereignty, is the result of brainwashing. Even so, whatever is forcibly implanted, the concepts that accompany this indoctrination can only be violent, coercive, and false. They confound black and white, they rape the truth. But as soon as the truth slips out, it will be deconstructed, and endlessly deconstructed, until it is put back together.

Patriotism is the first victim of rape. To whom does the country belong? If a country has no civil liberties, to whom can it belong? Just as Great Ancestor Mao said, "That which is fake is fake. The disguise should be stripped away." Currently, the new term "Zhao Country" is an excellent deconstruction of our country, the republic, and New China. Deconstruction is the dismantling of something to reveal its true essence. "Zhao Country" comes from Lu Xun's "True Story of Ah

Q," in which the young Master Zhao passes the imperial examination at the county level, and Ah Q also wants to boast a bit. He immediately gets a slap on the face from old Master Zhao, who says, "Are you also worthy of the surname Zhao?"

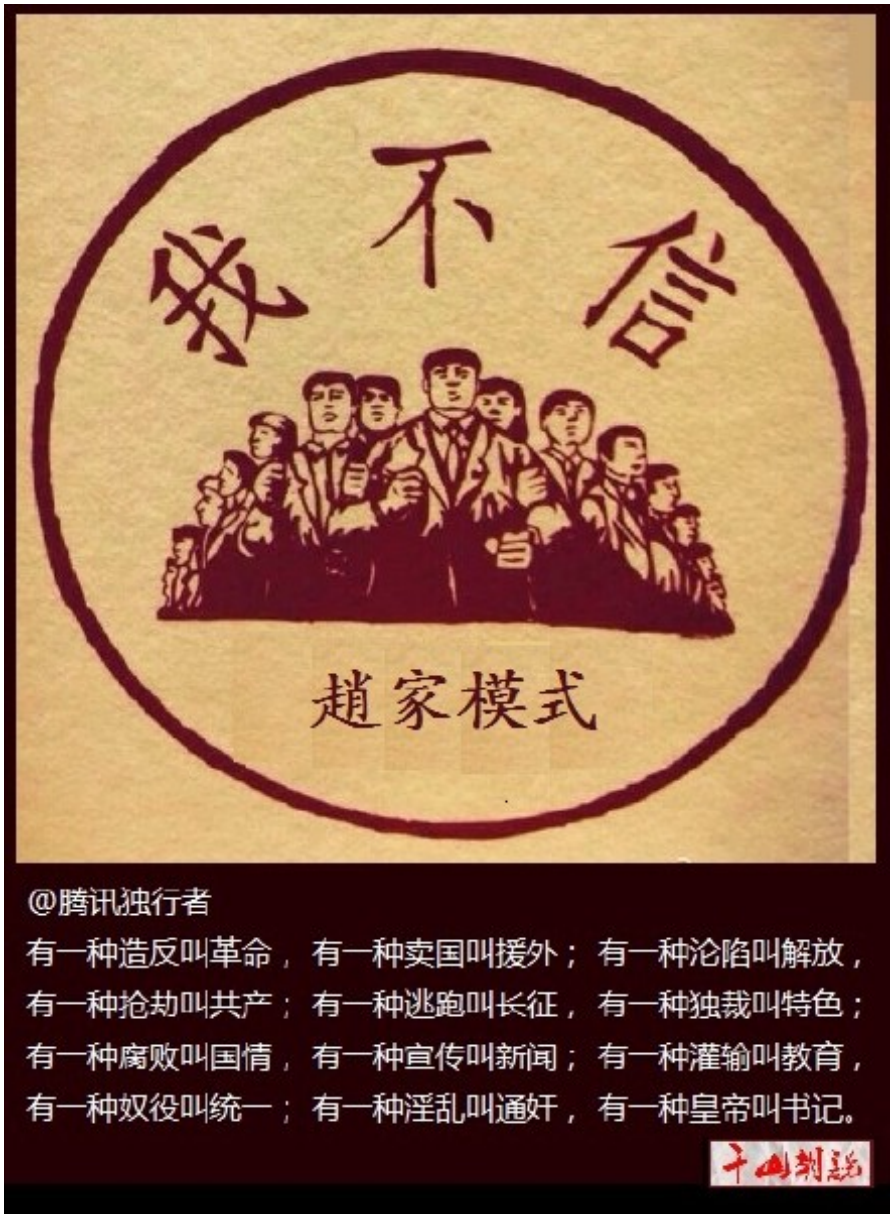
The master's household and country will categorically forbid a slave from taking a cut of its ill-gotten gains. Otherwise, Empress Dowager Ci Xi could have made it a national policy to "prefer the company of foreign countries over domestic slaves." The Big Guy's ceaseless scattering of money appears to have the same origin. Wang Shi's recent anger over the purchase of thousands of shares by Baoneng's Yao Zhenghua is the result of the inertia of the master and his power. In the past, business was a matter of you selling and me buying. There was a contract and a transaction, and it was fair and reasonable. But even so, if you were from a family that sold produce, and you wanted equal footing with me, suddenly anger would arise in the Wang Shis of the world, who represent the influential. You thought that because you have money now, you could assume the surname Zhao? Ha! In the eyes of the red bigwigs, slaves are slaves, lowly slaves. And it's like Captain Bo's disdain for Xu Ming. What position does Xu Ming have, and position do I have?

3. The saying "we are the successors of communism" has gone viral. Busybodies ask the question, when will our succession take place? Hehe, that's a question to ask Heaven. When it's your turn for succession, will you also be worthy of the surname Zhao? There's no need to mention that positions serving the renminbi are scarce. It's a red latrine full of people squatting. When patriotism was considered a concept of devotion, no one was denied access to it, but as soon as it became an appeal for profit, it could only be a weapon in the hands of the powerful. All the powerless fart people are the meat on the chopping board. Patriotism—"love for the cooking pot"—is a joke for willing fools. Someone else can dupe you, but if you believe it, you're a real idiot, because your surname isn't Zhao. The house belongs to the Zhaos, and so does the country.

The "love for the cooking pot" dream of volunteer fifty centers, and all ordinary citizens, should be put to rest. Deconstructing "love for the cooking pot" to reveal Zhao Country could be called a total overhaul. This is an inspired work of borrowism, where creativity has deconstructed something limitlessly, to the point where it comes very close to its true appearance. The fifty centers who say, "if you aren't a patriot, get out of China" are dejected slaves earning their measly fifty cents. Passing yourself off as a master is categorically unsuccessful: "Are you also worthy of the surname Zhao?" As soon as this is raised, these dog-like slaves surrender their weapons. This dynasty, when deconstructed using the Zhao Country method, could be overhauled, and all the fakery would end as bridges go back to being bridges, roads go back to being roads, the Eight Banners go back to being the Eight Banners, the slaves go back to being the slaves, the fart people go back to being the fart people. This would also put the halo back over patriotism. Just as the slaves of the Qing Dynasty couldn't say "my great Qing" but instead had to say "your great Qing," Zhao Country, and the industries of the people of Zhao Country, would already be demarcated. As with the separation of a natural moat, the powerful would be

clearly distinguished, and just like that, the dust would settle in the most remarkable and definitive way.

December 30, 2015



I Don’t Believe in the Zhao Family Model

There’s a type of rebellion called a revolution,

there’s a type of betrayal of country called foreign aid;

there’s a type of capture by the enemy called liberation,

there’s a type of robbery called communism;

there’s a type of retreat called the Long March,

there’s a type of despotism called a characteristic;

there’s a type of corruption called national spirit,

there’s a type of propaganda called news;

there’s a type of indoctrination called education,

there’s a type of enslavement called unification;

there’s a type of promiscuity called adultery,

there’s a type of emperor called a secretary.

(Source: http://chinadigitaltimes.net/2016/01/translation-zhao-country/)

Appendix 3: Sun Liping: Between Civilization and Barbarism

Tsinghua University Professor of Sociology Sun Liping last week launched the WeChat public account "Sun Liping's Social Observations." In his first post, he provides an introduction to his new channel of expression, translated below:

Introduction to Sun Liping's Social Observations

I am naturally lazy and slow to react. Now that WeChat is ubiquitous, and under the persuasion and goading of my friends, I've finally come to try this out.

Winter is gone and spring is here. One after the other, the black swans fly. Perhaps we are living in an era of more and more confusion, more and more uncertainty. The world, life, demand that we keep coming back to understand them, to recognize them.

That people have different opinions on myriad social phenomena is perfectly natural. But differing opinions cannot be grounds for exposing past mistakes and breeding hostility. Society needs a voice of calm and reason. A point of view, whether it is right or wrong, more often than not enhances our perception of life.

As of four or five years ago, I no longer publish lengthy articles in academic journals or in standard media. But fragments of thought rush forth from time to time. I hope this WeChat public account may serve as a platform for constructive discussion of and communication about social phenomena.

May China, and the world, progress.

==========

Following the introduction, Sun reposted a recent essay of his inspired by global events, offering his readers a warning on the importance of maintaining commitment to social progress. That essay is also translated in full:

Repost of Essay from a Few Months Ago: Between Civilization and Barbarism, We Must Not Lose Our Way

In contrast to barbarism, civilization is the accumulated progress of culture, behavior, lifestyle, and institutions for the betterment of humanity.

The general contours of civilization and barbarism are indisputable. If we deny this, then there is no right or wrong in the world.

A few days ago, I said, "In the face of dazzling change, as we struggle to agree on what is right, we must not blur one essential boundary—that which divides civilization and barbarism." I'd like to talk a bit about this now.

Trump's rise to power. Brexit. The reassessment of political correctness. The resurgence of populism. The whole world has become confused, as if clear prospects had turned into a chaotic mass. What I want to stress is that we must not get lost during this unpredictable, dizzying time. If developed countries have some potential to lose their way, that is a price we cannot pay.

Several months ago I posed questions on China's sense of direction, the elite's sense of security, and the common people's sense of hope. In the new international climate, these questions, the first in particular, seem more real.

Amidst all this, if at a certain place and time right and wrong are hard to discern, it is key that we not muddy one essential coordinate, that of civilization and barbarism.

There are those who do not recognize civilization, who say that civilization and barbarism are relative. This is relativistic sophistry.

Do we not recognize the difference between living well and living poorly? The difference between happiness and suffering? Defined in contrast to barbarism, civilization is the accumulated progress of culture, behavior, lifestyle, and institutions for the betterment of humanity. Human history is the process of moving from barbarism to civilization. Of course I must admit that no one can guarantee what the endpoint will look like.

In an example I have given before, there are often land disputes in the countryside. There are some places that resolve these disputes through archaic community battle, but today more locales rely on modern law. Is there any doubt about the distinction between the civilized and the barbaric in this case?

On a grander scale, international conflict can be solved through endless warfare, or it can be resolved by establishing international organizations, signing treaties, and negotiating compromise. Is there any doubt which is civilized and which is barbaric?

The transfer of power may be reached via a river of blood, or it may be achieved through a procedure and election that have the approval of the people. Is there any doubt which is civilized and which barbaric?

Public affairs may be handled by a small group acting arbitrarily, or with broader participation, thus embodying the will of more people. Is there any doubt which is civilized and which barbaric?

In social life, one group of people can have the power to discriminate against and oppress another, or everyone can coexist equally. When genuine equality cannot be realized, at least equality in the sense of the law and of rights can be guaranteed. Is there any doubt which is civilized and which barbaric?

I could come up with an endless list of such examples.

Of course, I agree that not every situation is black-and-white. For instance, Buddhists, Christians, and atheists clearly have different understandings of life and its meaning. But the broad outlines of civilization and barbarism cannot be denied. If we deny this, then there is no right or wrong in the world.

I will say it once again: between civilization and barbarism, our nation cannot afford the price of losing.

(Source: http://chinadigitaltimes.net/2017/04/sun-liping-%e5%ad%99%e7%ab%8b%e5%b9%b3-civilization-barbarism/)

OPENING STATEMENT OF MARGARET ROBERTS, PH.D., ASSISTANT PROFESSOR OF POLITICAL SCIENCE, UNIVERSITY OF CALIFORNIA, SAN DIEGO

DR. ROBERTS: Great. I'm Margaret Roberts. I'm Assistant Professor at UC-SD. Thank you so much for the invitation to provide testimony today on this really important topic.

Censorship, as we all know, is pervasive in China, and it affects the Chinese public quite a bit, and it has really important implications for the U.S. economy and for U.S.-China relations.

I'm going to base this testimony--I study censorship in China through large-scale social media data sets and through surveys, and I'm going to base this on my forthcoming book and also the research I published in Science and the American Political Science Review.

So I'm going to explain how different segments of the Chinese public are affected differently by censorship. High-profile media producers in China are targeted with threats of punishment for speech, but for most people in China, censorship acts as a tax on information, requiring them to spend more time or more money to access information.

So even though much information is possible to access in China, because it's not easy, censorship reduces the number of people who consume it. Censorship that creates taxes or frictions on information is often less visible than censorship that's created through fear of punishment, and therefore many citizens in China are not aware of censorship even though they are affected by it.

This tax on information distorts the information sector, reducing the competitiveness of censored information, including that from American businesses, and imposing costs on innovation in the Chinese economy.

So when most people think of censorship, they think about fear or punishment for speech, and in China, of course, this is very important, but it's typically targeted toward high-profile individuals like journalists, activists, entertainers, academics, et cetera.

When typical people talk and write about politics in China, for the most part, they are not targeted with punishment for personal or online speech. There's always a small possibility that typical Internet users would be punished for speech, but it's relatively rare.

Instead, average citizens in China are affected by friction that censorship creates on information. Censorship acts as a tax forcing users to spend more time and money to access it. For example, the Great Firewall of China, which blocks foreign websites from Chinese IP addresses, as we've discussed, can be circumvented with a Virtual Private Network, called VPN, but downloading and using a VPN costs time and money.

Social media companies remove social media posts at the direction of the government and they also block keywords where posting or searching for social media posts. And this also acts as a censorship tax.

So in recent work, I've also shown that online propaganda from these leaked directives that Professor Xiao was talking about acts to distract from ongoing events, and this also acts as a tax on access to information.

While it's usually possible to find information about censored events online or to evade censorship by substituting words creatively, it makes it very difficult for people to do this, and so they often do not.

When censorship acts through inconvenience rather than fear, it is less visible to the public, and so they're not as aware of it. A representative survey of urban residents that I did in China revealed that among Internet users, only half know that the Great Firewall exists. Many people are not aware of how censorship influences social media posts they come across, and for those who do come across censorship, many explain it away as an Internet error or a computer problem.

So the fact that censorship of typical citizens is less observable because it imposes taxes on information clarifies why even though censorship is unpopular in China, we don't see widespread backlash. While citizens in China tend to support government regulation of spam, false information, pornography and rumors on the Internet, in large part they do not support censorship of online communication and censorship that infringes on individual freedoms.

However, because users are often unaware of the pervasiveness of censorship, such backlash is less widespread than it would be if censorship were a more salient part of their lives.

Low awareness of censorship also explains why very few Chinese Internet users use VPNs to evade the Firewall. Indeed, surveys show that around only five percent of urban residents in China report using a VPN. And I've corroborated this with online data that measures how Chinese users are actually using blocked social media websites.

Because information beyond the Firewall requires time and money to circumvent, only those who have high demand for information and the increased ability to pay will be willing to evade the Firewall. So from surveys we know that people who are willing to evade censorship have higher incomes, are more educated than those who do not evade censorship. They also have more interest in foreign information, they're more likely to work for a foreign enterprise, have traveled abroad, or are more interested in politics.

Overall, those who evade censorship are the economic and political elite. They're interested in information over the Firewall and they're willing to seek it out. In this way, the Firewall acts as a regressive tax, allowing those with more capabilities to access information but largely keeping out those who don't have the knowledge or resources to facilitate evasion.

The U.S. government could focus on calling censorship for what it is--for what many people in China--how it affects many people in China, which is a tax on information. In addition to the U.S. government's efforts to shed light on the human rights implications of censorship, which are really important, the government should also bring attention to the ways in which censorship distorts the domestic and international market for information.

In its 2016 Annual Report, the USTR labeled China's Great Firewall as a trade barrier. And practically this is true. The Great Firewall lessens the competitiveness of blocked foreign websites in China by requiring that Internet users spend time and money to access these websites.

Since the U.S. economy is a fast and growing information sector, censorship functions as a barrier to trade and has large impacts on American businesses. But also like any trade barrier, censorship also hurts firms working domestically within China. Surveys by the American Chamber of Commerce show that the vast majority of U.S. companies operating in China report the inability to access certain websites from China hurts their business.

But censorship also imposes huge uncertainties on future business prospects of Chinese social media companies, and scientists in China have largely complained about the Great

Firewall that stifles innovation and disrupts knowledge. So every time we see that there are crackdowns on VPNs in China, we also see entrepreneurs and intellectuals in China online complaining about these crackdowns and reporting on how they hurt the development of the Chinese economy.

So the reduction of censorship in China would not only be better for U.S. business, it would also help the Chinese economy as well. Perhaps by framing censorship as an economic cost, as well as a human rights issue, which it is both, we would be able to better make the case why all parties would benefit in reducing barriers to information.

HEARING CO-CHAIR WORTZEL: Thank you very much.

PREPARED STATEMENT OF MARGARET ROBERTS, PH.D., ASSISTANT PROFESSOR OF POLITICAL SCIENCE, UNIVERSITY OF CALIFORNIA, SAN DIEGO

Hearing on "Information Controls, Global Media Influence, and Cyber Warfare Strategy"

Testimony before
The U.S.-China Economic and Security Review Commission

May 04, 2017

Introduction

Thank you for the invitation to provide testimony to the U.S.-China Security and Economic Commission on the topic of China's global media influence and censorship. Censorship is pervasive in China and affects much of the media that the Chinese public regularly consumes. As such, it has important implications for the Chinese economy, U.S. companies in China and U.S.-China relations.

In this testimony, I explain how different segments of the Chinese public are affected differently by censorship. While high-profile media producers in China are targeted with threats of punishment for speech, for most people in China censorship acts like a tax on information, requiring them to spend more time or money to access it. Even though the information is possible to access, because it is not easy, censorship reduces the number of people who consume it. Censorship that creates taxes or frictions on information is often less visible than censorship that is created through fear of punishment, and many citizens in China are not aware of censorship even as they are affected by it. Even though many people in China do not support censorship and are angered by it when they observe it, because of the low visibility of censorship and the inconvenience it causes, only a small proportion of the public takes the time to evade censorship restrictions. Only during moments of crisis or when habits are suddenly broken is a broader segment of the public willing to take the effort to seek out censored information.

In this testimony, I will first overview the different types of censorship in China. I will then explain how different segments of the Chinese public experience censorship and how they view censorship when they are asked about it or become aware of it. Next, I will outline the types of people who are willing to evade censorship in China and the moments in which a larger proportion of the public are likely to circumvent censorship. Last, I will provide policy recommendations that follow from these observations. The framework and much of the research in this testimony come my forthcoming book, *The Censorship Tax: How Citizens Respond to The Market for Information Within China's Great Firewall* and from work that my co-authors Gary King and Jennifer Pan and I have published in *Science* and the *American Political Science Review*.[1]

Mechanisms of Censorship in China

[1] Roberts (2014), Roberts (2018), King, Pan and Roberts (2013, 2014, 2017).

The Chinese government uses a variety of censorship methods to control information in the traditional and online media. I divide the Chinese government's methods of censorship into three main categories: fear, or censorship that threatens punishment; friction, or censorship that imposes costs on information access and spread; and flooding, or censorship through distraction or dilution of information.

Fear includes any censorship method that intimidates or punishes speech with the purpose of inducing self-censorship. Censorship laws are sufficiently ambiguous in China so that they can be used to target a wide-range of media and social media users.[2] However, in practice, fear is used to selectively target high-profile individuals like the journalists, activists, entertainers, academics, and those with large online followings. While the incidence of punishment for speech has increased under President Xi Jinping, who has expanded and tightened censorship laws, most of the focus of Xi's censorship crackdown has still been aimed at high-profile individuals within the media and online. In recent years, many journalists, social media users with large followings, and activists have been sentenced to prison or otherwise reprimanded because of their speech.[3]

However, typical people talking and writing about politics in China are for the most part not targeted with punishment for personal or online speech. While there is always a small possibility that typical Internet users and Chinese citizens would be punished for speech, it is rare. Instead, average citizens in China are affected by another category of censorship: friction. Friction includes methods of censorship that do not make information off-limits, but act as a tax on information – forcing users to spend more time or money to access the information. The Great Firewall of China, which blocks select foreign websites from Chinese IP addresses, is the classic example of friction. The Great Firewall can be circumvented with a Virtual Private Network (VPN), but downloading and using a VPN costs time and money. Content filtering – when social media companies in China remove social media posts at the direction of the government --and keyword blocking – where posting or reading social media posts are filtered by keywords -- are other examples of friction in China.[4] While it is usually *possible* to find information about the censored event online, the removal and filtering of social media posts makes information about these events more difficult to find and lessens its spread.

The Chinese government also uses a third form of censorship targeted toward the public: flooding, or producing distracting media in order to saturate the media environment and out-compete information about events that reflect badly on the government. In a forthcoming article in the *American Political Science Review*, my co-authors and I show that the Chinese Fifty Cent

---

[2] Censorship laws prohibit a wide range of speech, including information that "harms the interest of the nation," "spreads rumors or disturbs social order," "insults or defames third parties," or "jeopardizes the nation's unity." Translation at: "Falling Short: Appendix II: Media Law in China," *Committee to Protect Journalists*, https://cpj.org/reports/2008/06/12ii-2.php/

[3] For a summary of the recent government crackdown on journalists and activists, see ``China Events of 2015." *Human Rights Watch*, https://www.hrw.org/world-report/2016/country-chapters/china-and-tibet.

[4] See King, Pan, and Roberts (2013) and King, Pan, and Roberts (2014) for studies of content filtering. See Hilts et al (2016) and Knockel et al (2017) for a discussion of keyword blocking.

Party – government workers hired to write social media posts pseudonymously at the direction of the government -- introduces approximately 448 million distracting social media posts cheerleading for the Chinese government per year, focused during crisis events.[5] Similarly, Chinese newspapers are instructed to coordinate articles during major meetings and sensitive time periods to crowd out alternative viewpoints.[6] Like friction, censorship through flooding acts as a tax on information by increasing the burden on citizens to distinguish good information from bad information. While it is possible to discount flooded information, doing so requires more effort and time than taking easily accessible information at face value.

Experience with Censorship and Citizens' Views of Censorship

The three categories of censorship – fear, friction, and flooding – illustrate why it is important to distinguish between those who are punished for their speech in China and those who are mostly affected by censorship that taxes information. Those who are under the close watch of government censors – high profile social media users, journalists, academics, and activists – are constantly aware of censorship and regularly navigate the fine line between in-bounds and out-of-bounds topics.[7] They interact with censors who are often their editors and their bosses. Because the government uses the threat of reprimands to control them, censorship is very visible to these individuals and is a regular part of their lives.

For most people in China, however, censorship is much less salient even as they are affected by it. The public in China is less likely to be punished and less fearful of censorship. Instead, the public is affected by taxes on information imposed by the removal of social media posts, introduction of propaganda, and the imposition of the Great Firewall. Many of these censorship methods are invisible and the public is not aware of them. A representative survey of urban residents in China I describe in my book revealed that even among Internet users, only half know that the Great Firewall exists.[8] Recent surveys in 2014 and 2015 suggest that few people report having had their posts or accounts deleted.[9] However, post deletions of others' necessarily affects what information individuals read, and most users will not notice when others' posts go missing. Therefore, many will not be aware of how censorship influences the social media posts they come across online.[10] For those who do come across censorship, many may explain it away as an Internet error or a computer problem and not attribute it to the government.

The fact that censorship of the typical citizen is less observable because it imposes taxes on information rather than creating fear clarifies why even though censorship is unpopular in China we do not see widespread backlash. While Chinese citizens support government regulation of

[5] King, Pan and Roberts (2017).
[6] See leaked directives on the *China Digital Times* website, such as "中宣部：中央政治局集体学习." URL: https://chinadigitaltimes.net/chinese/2012/11/%E4%B8%AD%E5%AE%A3%E9%83%A8%EF%BC%9A%E4%B8%AD%E5%A4%AE%E6%94%BF%E6%B2%BB%E5%B1%80%E9%9B%86%E4%BD%93%E5%AD%A6%E4%B9%A0/
[7] See Stern and Hassid (2012).
[8] Roberts (2018).
[9] Dickson (2016) and Roberts (2018).
[10] For a discussion of the invisibility of censorship, see Knockel et al (2017).

spam, false information, pornography, and rumors on the Internet, they in large part do not support censorship of online communication and censorship that infringes on individual freedoms.[11] When people observe censorship, they are also often angered by it. Surveys show that many people in China report being angry and not fearful when they have a post removed online.[12] In online experiments I have conducted, I have found that those who experience censorship in a lab setting are less likely to support government censorship subsequently.[13] However, because many users are unaware of the pervasiveness of censorship that uses friction and flooding online, such backlash is less widespread than it would be if censorship were a more salient part of their lives, as it is with many media producers.

VPN Use in China

Given that the Great Firewall of China blocks some of the world's most popular websites from China, it is puzzling that very few Chinese Internet users use a Virtual Private Network (VPN) to evade it. Indeed, surveys show that only around 3-5% of urban residents in China report using a VPN.[14] This is corroborated by online data as well: there are around the same number of Twitter users who regularly geo-locate to China as there are users who geo-locate to Hong Kong (where Twitter is not blocked), even though China has around 100 times the online population of Hong Kong.[15] This suggests that the Great Firewall is largely effective in preventing Chinese citizens from accessing blocked websites, even though it can be circumvented.

Why don't Internet users in China circumvent the Firewall? The Great Firewall imposes a tax on information on blocked social media sites – information beyond the Firewall requires time and money to circumvent. Like any tax in an economy, this means that only those who are have high demand for the information and increased ability to pay will be willing to evade the Firewall. For the others, attractive alternatives within China mean that they are less willing to spend the extra effort required to access blocked websites and would rather substitute with websites that do not require a VPN.

This is largely corroborated by survey evidence within China. When Internet users who reported that they did not circumvent the Great Firewall but who knew that circumvention was possible were asked why they chose not to circumvent it, many said that they did not have a reason to, they did not know how, or that it was too bothersome. The draw across the Great Firewall was simply not great enough to overcome the inconvenience in evading it. Very few reported that they were fearful to jump the wall. Instead, users were simply not willing to pay the cost in time and money of evasion.

Consistent with this theory, those who do evade censorship generally have more resources to evade censorship and more reasons to jump the Firewall, making them willing to pay the cost of

[11] Dickson (2016) and Roberts (2018).
[12] Dickson (2016) and Roberts (2018).
[13] Roberts (2018).
[14] See Farris et al (2010). Also calculated in Roberts (2018) to be 5%.
[15] Hobbs and Roberts (2017).

evasion. Those who report in surveys being willing to evade censorship have higher incomes, more education, and are much more likely to be younger than those who do not evade censorship. They also have an interest in foreign information – they are more likely to work at a foreign enterprise, have traveled abroad, and are much more interested in politics and international politics than those who do not use VPNs.[16] Overall, those who were willing to evade censorship are the economic and political elite: interested in information over the wall and willing to seek it out. The Firewall acts as a regressive tax – allowing those with more capabilities to access information, but largely keeping out those who do not have the time, knowledge, or resources to facilitate evasion.

Yet even though many are not typically willing to jump the Firewall in China, there may be some time periods when users are more willing to evade it. When censorship is suddenly imposed on websites that users are accustomed to accessing or during time periods of crisis with low information, users may have higher demand for information across the Firewall. In recent work, my co-author William Hobbs and I have shown that the sudden block of Instagram during the protests in Hong Kong decreased overall use of Instagram from mainland China, but inspired the download of what we believe to be millions of VPNs from China and subsequently expanded use of blocked websites such as Twitter, Facebook, and Wikipedia from China.[17] Because people were accustomed to using Instagram, when it was suddenly blocked they downloaded VPNs to evade the Firewall. Similarly, survey evidence indicates that many more people access VPNs in the few days after crises like the 2015 Tianjin explosion.[18] During crises and protest events, the government may be less able to control the spread of information because the public has a greater incentive to take the time to seek information out. It is no wonder that much of friction and flooding in China therefore seems to ramp up to control information during protest events and crises, as my co-authors and I have shown in work studying the targets of censorship and propaganda in China.[19]

Implications and Recommendations

The Chinese censorship program has important implications for the U.S.-China relationship. First, it imposes an economic cost on both U.S. and Chinese businesses. U.S. firms are blocked by the Great Firewall, which limits their access to the Chinese market. Censorship harms Chinese businesses and innovators. Students and entrepreneurs within China are handicapped by censorship because some of the best technologies in the world are blocked within China. Social media companies in China are burdened with requirements to hire censors in order to comply with government regulations.

Second, censorship has long-term implications for the way in which Chinese citizens view the United States. Because of the taxes censorship imposes on outside information, the Chinese public in large part consumes very different media than that consumed by the Western world.

---

[16] Roberts (2018).
[17] Hobbs and Roberts (2017).
[18] Roberts (2018).
[19] King, Pan and Roberts (2013, 2014, 2017).

Over the long term, the different patterns in media consumption between the U.S. and Chinese public is likely to drive a wedge between these publics' understandings of politics which could increase the likelihood of international conflict.

While we should be concerned about both of these implications, it is more practical to focus policy on the economic impacts of censorship because the effects are tangible and accrue over the short-term. In addition to U.S. government's efforts to shed light on the human rights implications of censorship, the government should also consider treating censorship as a tax on information that distorts the domestic and international market for information. In its 2016 annual report, the U.S. Trade Representative labeled China's Great Firewall as a trade barrier.[20] Practically, this is true – the Great Firewall lessens the competitiveness of blocked foreign websites in China by requiring that Chinese Internet users spend money and time accessing them. Since the U.S. economy has a fast a growing information economy, censorship functions as a barrier to trade that has large impacts on U.S. business. Since there are no similar barriers that the U.S. imposes on information from China, this relationship is not reciprocal.

Like any trade barrier, censorship also hurts firms working domestically in China. Surveys by the American Chamber of Commerce show that 71% of U.S. companies operating in China report that the inability to access certain websites from China hurts their business.[21] Censorship imposes huge uncertainties about the future business prospects of social media companies in China.[22] Scientists in China have complained that the Great Firewall stifles innovation and disrupts knowledge.[23] The reduction of censorship in China would not only be better for U.S. business, but would help the Chinese economy as well.

The U.S. government could focus on calling censorship for what it is – a tax – and revealing the impacts that censorship has on other areas of the economy. More research should be done to quantify the economic impacts of censorship. Censorship is regressive in that it allows highly educated and affluent users in China to access information that their less equipped fellow citizens cannot. How does this impact the development of human capital, inequality in China, and those seeking reliable information about health, the environment, and the Chinese economy? By arming ourselves with knowledge about some of censorship's less well-known but likely pernicious impacts, we will better be able to make a case for why all parties will benefit from reducing the barriers to information.

---

[20] "The 2016 National Trade Estimate Report on Foreign Trade Barriers." US Trade Representative. URL: https://ustr.gov/sites/default/files/2016-NTE-Report-FINAL.pdf

[21] "2016 China Business China Survey Report." The American Chamber of Commerce in the People's Republic of China (2016). URL: https://www.amchamchina.org/policy-advocacy/business-climate-survey/2016-business-climate-survey

[22] "Costs of Censorship Haunt `Chinese Twitter' IPO." *Wired*. April 17, 2014. URL: https://www.wired.com/2014/04/weibo-ipo-cost-of-oppression/

[23] "China's Great Firewall is Harming Innovation, Scholars Say." *Time*. June 1, 2016. URL: http://time.com/4354665/china-great-firewall-innovation-online-censorship/

References

Dickson, Bruce. *The Dictator's Dilemma: The Chinese Communist Party's Strategy for Survival*. Oxford University Press, 2016.

Faris, Rob, John Palfrey, Ethan Zuckerman, Hal Roberts, and Jillian York. ``2010 Circumvention Tool Usage Report." Berkman Center for Internet and Society (2010). URL: http://cyber.harvard.edu/sites/cyber.harvard.edu/files/2010_Circumvention_Tool_Usage_Report.pdf

Hilts, Andrew, Greg Wiseman, Jason Q. Ng, Jeffry Knockel, Lotus Ruan, and Masashi Crete-Nishiata. "Harmonized Histories? A year of fragmented censorship across Chinese live streaming applications." Citizen Lab Report (2016). URL: https://citizenlab.org/2016/11/harmonized-histories-year-fragmented-censorship-across-chinese-live-streaming-applications/

Hobbs, William, and Margaret E. Roberts. "How sudden censorship can increase access to information." Working Paper (2017). URL: http://www.margaretroberts.net/wp-content/uploads/2016/08/selfiecensorship.pdf

King, Gary, Jennifer Pan, and Margaret E. Roberts. "How censorship in China allows government criticism but silences collective expression." *American Political Science Review* 107.02 (2013): 326-343.

King, Gary, Jennifer Pan, and Margaret E. Roberts. "Reverse-engineering censorship in China: Randomized experimentation and participant observation." *Science* 345.6199 (2014): 1251722.

King, Gary, Jennifer Pan, and Margaret E. Roberts. "How the Chinese government fabricates social media posts for strategic distraction, not engaged argument." *American Political Science Review* (forthcoming).

Knockel, Jeffrey, Lotus Ruan and Masashi Crete-Nishihata. "We (can't) Chat: ``709 Crackdown" Discussions Blocked on Weibo and WeChat." Citizen Lab Report (2017). URL: https://citizenlab.org/2017/04/we-cant-chat-709-crackdown-discussions-blocked-on-weibo-and-wechat/

Roberts, Margaret E. *Fear, Friction, and Flooding: Methods of Online Information Control*. Doctoral Dissertation. 2014. URL: https://dash.harvard.edu/bitstream/handle/1/12274299/Roberts_gsas.harvard_0084L_11469.pdf?sequence=1

Roberts, Margaret E. *The Censorship Tax: How Citizens Respond to the Market for Information Within China's Great Firewall.* Princeton University Press, forthcoming 2018.

Stern, Rachel E., and Jonathan Hassid. "Amplifying silence uncertainty and control parables in contemporary China." *Comparative Political Studies* 45.10 (2012): 1230-1254.

OPENING STATEMENT OF SOPHIE RICHARDSON, PH.D., CHINA DIRECTOR, HUMAN RIGHTS WATCH

DR. RICHARDSON: Chairwoman Bartholomew, Co-Chair Wortzel, Commissioners, it's wonderful to be here with you this morning and thanks for inviting us to address the foundational issue of freedom of expression in China, and particularly domestic information controls. I want to briefly summarize our written remarks regarding those trends--which are almost uniformly negative--and share some recommendations.

But first, I want to share an example that we think illustrates the prevailing political winds as we talk about the economic issues and some of the technology that I can't claim to understand. Every year on New Year's Day, Nanfang Zhoumo--or the Southern Weekend, which is one of China's more progressive media outlets--publishes an editorial that sort of summarizes the major events of that year and sort of sketches out aspirations for the coming year, and partly because this is a piece that's very well-known in liberal intellectual circles, it's subject to particularly intensive scrutiny because people know that it's going to get a lot of attention.

So we think of it as a particularly good barometer of what can and can't be said. So in 2004, the editorial explicitly attributed some of China's worst problems that year, including the SARS scare, to limitations, quote, "on citizens and rights," noting that those are, quote, "complimentary to each other."

In 2008, the editorial noted, quote, "individuals are not liberated enough, thoughts are not free enough," and implicitly called for "democracy and freedom and human rights."

By 2013, the editorial no longer referenced citizens or human rights, but rather it addressed then new CCP Chair Xi Jinping's quote, "great rejuvenation and dreams of the Chinese nation."

And by January 1, 2017, the editorial was utterly devoid of any political language and focused only on, quote, "hopes and dreams."

Authorities under President Xi have not contented themselves to simply scrub language they find problematic out of state media outlets, harass and detain domestic and foreign journalists, and globalize their propaganda operations. They've also worked assiduously to control technologies, ranging from the manipulation and censorship of social media platforms like WeChat and weibo, to a broad push for real-name registration for mobile phone users, to imposing new restrictions on Virtual Private Networks.

Slowly, but steadily, these steps are changing what people are inclined to say on line, and how they use technology, and it's not changing for the better with respect to the freedom of expression.

Authorities have also passed a slew of restrictive new laws and regulations, seemingly to create a veneer of legality of extensive surveillance and censorship. Those include the counterterrorism law, the cybersecurity law, and provincial-or-municipal-level regulations. In March 2017, Chongqing--a city of 50 million people--banned the unauthorized use of intervention circumvention tools, and we're especially concerned about this development as previous regulatory efforts to rein in the use of such tools really did focus solely on the providers and not on the individual users, and now both are on the hook.

Earlier this week, a new set of regulations that nobody even seemed to know were

coming put in place a requirement that the top editors of any online news content platform be a PRC citizen, which we assume is a way of controlling what people sign off on publishing.

And I was asked to spend a few minutes in particular talking about Beijing's "social credit system," which has been under discussion since June 2014. The government's intent appears to be the establishment of a national database of all citizens and organizations that logs information not only about their financial trustworthiness--that's the idea of credit that we all think of as really for financial purposes--but also assesses their social and political behavior, including their online speech.

A social credit score or rating may have an impact on multiple aspects of a person's life, not just interest rates or school admissions, but the ability to get a passport, move around the country freely, access a VPN, or rent an apartment, and these are all activities that have been curtailed in retaliation of people who have been critical of the government.

Various local and provincial governments, and some national agencies, have issued policy documents to begin implementing the system, but so far it does remain quite fragmented, and it appears to us that it's more an aspiration rather than a reality. But Guangdong, which is one of the biggest provinces, did start gathering data in early 2015, and in April of this year, Wuhan, Changsha, Hefei, and Nanchang signed an agreement to share and integrate social credit data.

Major Chinese Internet and e-commerce companies, including Tencent and Alibaba, are assisting with these efforts, making it possible that those who use those companies' services could be subjected to social credit ratings.

We think--it's hard to know for sure--authorities want to put this system in place, partly to try to tackle corruption, partly to promote public morality, and partly to increase public confidence in the government, but given China's deeply politicized legal system and its near total lack of enforceable privacy protections, the system does have tremendous potential for abuse.

And a brief word also on the concept of Internet sovereignty. At the United Nations, at the World Internet Forum, and at other international gatherings, China is promoting this vision as an alternative to the open, global vision of the Internet--in effect, trying to get the rest of the world to buy into its legal and technical efforts to control access to independent information, which, of course, in Beijing's view, includes just about anything that's critical of the government, and effectively be able to surveil people on a mass scale.

This is also an approach in which there is no role for civil society or independent actors. It's really governments, and governments alone, who write the rules.

What are the consequences of some of these developments? First, I think there's an incredible asymmetry, again, between what the Chinese government can know about citizens and their behavior and what Chinese citizens can know or say about the government. You know, no rights are secure in that kind of environment, and certainly no corruption campaign is going to succeed, and obviously you've got imbalances, important trade issues.

Second, although citizens and netizens are constantly trying to innovate around censorship, we're afraid that Goliath is winning and finding traction for that approach internationally.

Finally, as China is increasingly exporting this technology to other repressive regimes, it's not just peaceful expression inside the mainland that's at stake. Increasingly, it's peaceful

expression in other parts of the world.

Let me very quickly walk through a few recommendations. I'd certainly associate myself with all the ones that have been made, particularly U.S. support for any sort of innovation against censorship and support for broadcasting efforts, like the BBG.

I think the U.S. Congress should call on U.S. tech companies that do business in China to answer questions about how they respond to Chinese government demands to censor. There are plenty of individual cases, both of American citizens like James Wang but other people who have been imprisoned in the mainland for online speech. Those cases all deserve attention.

And the U.S. should keep pushing China to repeal the laws that seemingly legalize surveillance and censorship.

Thanks.

PREPARED STATEMENT OF SOPHIE RICHARDSON, PH.D., CHINA DIRECTOR, HUMAN RIGHTS WATCH

Hearing on "Information Controls, Global Media Influence, and Cyber Warfare Strategy"

Testimony before
The U.S.-China Economic and Security Review Commission

May 04, 2017

Chairwoman Bartholomew, Commissioner Wortzel, and members of the Commission,

I'd like to thank the Commission for its ongoing attention to human rights abuses in China.

Human Rights Watch has written extensively about restrictions on freedom of information in China for the past two decades, and we welcome the opportunity to address trends in domestic information control under Chinese President Xi Jinping's administration.

Since President Xi came to power in March 2013, the Chinese government has fully subdued the few outspoken domestic print media organizations, and stymied the flow of politically sensitive materials from Hong Kong into the mainland by crushing the Hong Kong publishing industry. It has deftly reined in access to the internet, jailing bloggers who promote progressive, pro-democracy values, and forcing the rest into self-censorship. It has nurtured a massive domestic social media platform – while blocking all foreign competitors – in which the ability for users to spread information is very limited and surveillance is pervasive. It has increased enforcement of real-name registration that makes online anonymity near impossible. It has also blocked an increasing amount of foreign content, and intensified its clampdown on those who provide or use tools to circumvent the blockage.

Nevertheless, numerous Chinese writers and activists have continued to speak out against the increasingly authoritarian government and unwaveringly advocate for freedom and democracy in China.

Xi Jinping: Chinese media "must bear the surname 'party'"

The Chinese government has tightly controlled its domestic media ever since the founding of the People's Republic in 1949. There have been virtually no independent newspapers, media companies, or publishing houses in China. In the 1990s and 2000s, a handful of domestic newspapers and magazines – though still state-controlled – were allowed some space to critically discuss issues related to the government's performance, but such space has significantly diminished in the years since Xi came to power. In early 2016, during a tour of several state media outlets, Xi declared that Chinese media "must bear the surname 'party'" – meaning the Chinese Communist Party – and demanded their absolute loyalty.

Southern Weekend, a newspaper based in Guangdong province, was for many years well-regarded for its investigative stories and editorials critical of government policies, and was widely popular among liberal intellectuals. But in the past several years, the government has exerted more control over the paper, appointed managers who are Xi loyalists, and forced out outspoken journalists.

In early 2013, *Southern Weekend*'s journalists and supporters staged a protest against the Guangdong government's decision to censor a New Year's editorial calling for constitutionalism. Three activists – Guo Feixiong, Liu Yuandong, and Sun Desheng – who joined the peaceful protest outside the newspaper's headquarters were later sentenced to six, three, and two and a half years in prison respectively for "assembling a crowd to disrupt public order." In March 2015, without giving prior notice to most of the staff at *Beijing News*, the Beijing propaganda department suddenly appointed two of its officials to lead the influential Beijing-based liberal daily. And in 2016, Beijing authorities sacked or demoted several top editors of *Yanhuang Chunqiu*, a liberal-minded history magazine with the backing of relatively liberal Party elders, leading to its closure. As a result of this heavy-handed censorship, the space for pro-reform voices in domestic media is now almost nonexistent.

Crumbling Hong Kong publishing industry

Because of the Chinese government's stringent control over domestic publishing, Hong Kong had become a place where mainland Chinese could purchase politically sensitive books and magazines. However, a series of jailings and alarmingly, cross-border abductions, have seriously undermined the industry and represent a blatant violation of free expression, the likes of which have never been seen in Hong Kong.

In October 2013, a Shenzhen court sentenced Hong Kong-based publisher Yiu Mantin to 10 years in prison on politically motivated charges of smuggling. Prior to his arrest, Yiu planned to publish a biography called "Godfather of China Xi Jinping," which was authored by a well-known Chinese dissident. In 2014, a Chinese court sentenced publisher James Wang, a US citizen, and his Chinese colleagues, for selling magazines about Chinese politics to mainlanders. Wang was sentenced to over five years in prison.

In 2015, in a case that attracted global attention, the Chinese government forcibly disappeared five Hong Kong-based booksellers. Among them, Lee Bo, a British citizen, was abducted in Hong Kong, likely by Chinese security agents. Gui Minhai, a Swedish citizen who was abducted from Thailand, remains in detention. Before their forced disappearances, the booksellers planned to publish a book on Xi Jinping's love life, though the two had also published many other titles.

The abductions were felt deeply by all actors in the Hong Kong publishing industry. It created such fear that, as *the Guardian* put it, "bookshops have closed. Publishers have left. Authors have stopped writing. Books have been pulped. Printers are refusing political works. Translators have grown weary of being associated with certain topics." It is estimated that over 80 percent of

Hong Kong bookstores – and almost all the ones occupying store-front properties – are run by three major chains controlled by the Chinese government. The assault on Hong Kong's small minority of independent publishers and booksellers further deepens China's grip on the entire industry in Hong Kong.

Intensified crackdown on bloggers and further criminalization of online speech

With the advent of the internet, there was once hope that it would bring increased freedom of expression to China, as anyone could publish instantly and with anonymity. As imprisoned Nobel Peace Prize Laureate Liu Xiaobo put it, the internet is "God's gift to China." Unfortunately, Beijing quickly caught up, created one of the world's most sophisticated internet censorship and surveillance systems – colloquially known as the Great Firewall – and has been refining the system ever since. During the Hu Jintao administration from 2002 to 2012, there appeared to be some online space – especially on the microblogging platform Weibo – in which people could discuss certain social and political issues critically. For example, netizens' heated online debates and fierce opposition contributed to the government's decision to drop Green Dam, a web filtering system the government proposed to install on computers in 2009. However, such space has narrowed significantly since Xi came to power.

Forty years into the reform era, and at a time when other kinds of information can move freely and instantaneously, people continue to land in jail for peaceful criticism of the Chinese government, including a slew of influential online activists. Among them, Charles Xue, a businessman who had over 12 million followers on Weibo and was known for his commentaries on social issues such as the rights of children and migrant workers, was detained in September 2013 for "soliciting a prostitute." In January 2014, Uyghur scholar Ilham Tohti was arrested and later sentenced to life in prison on charges on "separatism" in relation to a website he founded that discussed China's policies on ethnic minorities. Pu Zhiqiang, a prominent human rights lawyer, was detained in May 2014 for over a year on charges of "inciting ethnic hatred" and "disturbing public order" for his online posts.

In 2013, the Chinese government issued a judicial interpretation that expanded existing laws to punish "online rumors." Social media users who post libelous information viewed more than 5,000 times or forwarded more than 500 times can be charged with defamation and jailed for up to three years. Anyone sharing false information deemed to cause "serious social disorder" can be charged with "picking quarrels and provoking troubles," which carries a maximum five-year prison term. In 2015, the government revised the criminal law to impose a punishment of up to seven years in prison for "spreading rumors" about disasters or diseases. The vagueness of the provision means that individuals doing nothing more than asking questions or reposting information online about reported local disasters could be subject to prosecution.

The crackdown on influential bloggers and the criminalization of social media activity has greatly chilled political discourse on Weibo. Many prominent bloggers became less active and some withdrew from social media altogether. For example, Wang Xiaoshan, an actor who had over one million Weibo followers told AFP, "I feel the pressure, I am more careful about posting

about any kind of topic." He Weifang, a well-known law professor and public intellectual, closed his Weibo account by posting a classical painting of a poet who retired from government service in protest against corruption.

The rise of WeChat, a less open social media platform

During the Xi era, many social media users have shifted away from Weibo to WeChat as a result of heavy censorship on Weibo. WeChat, launched by Chinese tech giant Tencent in 2011, is a mixture of social media and messaging services. Its users can only see posts by individuals who have friended them, and none of these posts are directly sharable or searchable. Because of these unique designs, information cannot be circulated as widely and quickly on WeChat as it is on Weibo, which is a more open platform. The shift creates a situation in which users may feel less constrained, but their messages have a much more limited audience.

Furthermore, WeChat is still subject to significant censorship. Technical research conducted by Toronto-based Citizen Lab has found both keyword and image filtering on the platform, particularly with group chats, with no transparency for users when information is restricted. WeChat's censorship raises concerns about surveillance, too. Previous investigations into TOM-Skype, Microsoft's former mainland Skype product, found that chat messages containing sensitive terms were logged and sent to a remote server, raising questions around whether WeChat messages are subject to similar surveillance. In September 2016, the Chinese government issued a new notice explicitly allowing collection of social media messages and contact lists for use as evidence in investigations.

Enhanced enforcement in real-name registration and surveillance

The Xi administration has continued to push for real name registration. The policy has been most successful with mobile phone users, such that it is nearly impossible to purchase SIM cards that are not tied to any ID number. In September 2013, the Ministry of Industry and Information Technology (MITT) imposed regulations that require all phone users to be registered with their real names, and in August 2016, the MIIT issued a notice ordering China's telecom companies to disable services to any accounts that are not real-name registered by June 2017. After the notice was published, users across the country started to receive text messages asking them to bring their ID cards to service centers to register their cell phones. At the same time, the government has also pushed social media and messaging apps to require users to tie an ID card or mobile phone number to their accounts; although it is possible to use these without registering one's ID, many functions increasingly important for daily life in China, such as those involving online payments, require such registration.

Real-name registration is an effective mechanism to surveil and censor users. As now-prosecuted human rights lawyer Li Heping said to Radio Free Asia in 2011, "The reality [in China] is that for any message you post on Weibo, your real identity can be found. But ordinary citizens might not know this. They think if they use a pen name, police would not be able to find them. They have a sense of [false] security, thus they dare to speak up… If using real names, some people likely will not dare to speak."

In late 2016, China passed the Cybersecurity Law, which further strengthened surveillance. The law requires companies to restrict online anonymity, to store users' "personal information and other important business data" in China, and to monitor and report to the government undefined "network security incidents." While there are no truly enforceable privacy rights in China and internet companies are already expected to do all these, enforcement has been uneven. Requiring companies to do so in a specific national law may reduce the leeway and differing level of implementation among companies, which has been exploited by internet users to get their message out despite censorship.

The Cybersecurity Law is part of a raft of security laws passed by the Chinese government, along with the National Security Law and the Counterterrorism Law, that are aimed at ensuring all information technologies are "secure and controllable." The Counterterrorism Law is also particularly worrisome as it requires companies to help decrypt information per requests by law enforcement, and its vague and broad provisions, including the definition of terrorism, allow police to request such information in a wide variety of situations.

Foreign websites blocked, Virtual Private Networks (VPNs) increasingly disrupted

While the government has increased its control on the flow of domestic information, it also enhanced its ability to fend off information coming from outside of China. During the Xi era, the Great Firewall has blocked an increasing number of news and social media websites, such as the *Economist*, the *Wall Street Journal*, and Instagram. In January 2017, American tech giant Apple removed the *New York Times* app from its digital store in China, acting on orders from the Chinese government. Apple had previously removed other apps associated with media organizations and a bookstore that distributed works about Tibet and Xinjiang.

In order to get around the Great Firewall to access prohibited information, Chinese netizens have to use software such as Virtual Private Networks (VPNs). However, VPNs have increasingly become unreliable as the Chinese government has stepped up efforts to block or disrupt VPN services. And this year, the government issued new rules to increase its legal controls over the use of VPNs.

In January 2017, the MIIT issued regulations that require all providers of circumvention tools in China to be pre-approved by the ministry, which effectively puts most of the country's providers of VPNs in violation of the law. By only allowing government-approved VPN providers – in other words, providers that are compliant with censorship and surveillance orders from the government – the Chinese government will certainly be in a better position to monitor VPN traffic and control VPN users.

In March, the government of Chongqing, a city of about 50 million in southwest China, made public a regulation that bans unauthorized use of internet circumvention tools in the city. Anyone – from individuals to companies – who skirts the Great Firewall will be ordered to disconnect and receive a warning. Those who make a profit while using circumvention tools will be fined.

The Chongqing regulation is unprecedented as it places a blanket ban on the use of VPNs and other circumvention methods used to connect to the global internet. Previous regulatory efforts to rein in the use of such tools have focused on providers and left individual users alone. It is unclear whether other local governments will follow suit.

The mere use of VPNs is already the basis of prosecutions in Xinjiang. In October, a man in Changji city was reportedly detained for “downloading violent and terrorist circumvention software,” which turned out to be a VPN. In February, a man in the capital Urumqi was detained for 15 days for using a VPN to visit websites perceived by the authorities as hostile. The restive northwestern region leads the country with respect to tech-based controls on the freedom of expression. In July 2009, the internet in Xinjiang was cut off entirely for several months in the wake of ethnic rioting in Urumqi.

What the Xi administration has done to control information is not necessarily unprecedented, but by heavy-handedly patching the cracks in China’s censorship apparatus, the Xi government has effectively eliminated the pockets of free speech that had emerged during China’s three decades of reform era.

Citizens’ continuing fight for freedom of expression

While facing a myriad of difficulties and risks in obtaining and sharing information, many Chinese citizens nevertheless persisted, “reincarnating” themselves on Chinese social media every time their account were censored. Wang Wusi, who is known on WeChat for his satirical commentaries on Chinese politics and society, has had more than 20 accounts removed due to his unremitting criticisms of the Chinese government. Police have gone so far as to harass his wife, his parents, and his wife’s parents. But Wang is still publishing, and said, “I had been worried [about being jailed], and tried to avoid sensitive topics, but it has become useless because the government just has so many sensitive spots. Then I decided not to think about whether and when I will get jailed, because it is not like if you think about it, you will be able to avoid it. What ought to come will come.”

Despite the looming danger of using VPNs, many China-based activists are still active on Twitter, speaking critically or making fun of Xi Jinping and voicing their support to fellow activists. Among them is Murong Xuecun, a Beijing-based writer. Murong, in an interview with the Committee to Protect Journalists, said, "In the past several years, I have often envisioned such a scene: a group of police officers break into my home, handcuff me, and take me away. After living under the shadow of such a scenario for years, now I feel I can handle it. I will not give up on my writing. I will not self-censor. I think I am ready for whatever is going to happen to me."

The spread of “internet sovereignty”

Under President Xi, China has expanded its efforts to assert influence over the development of the internet beyond its borders. The government continues to promote “internet sovereignty” at

the United Nations and in other international forums as an alternative to the open, global vision of the internet that the US and other governments promote. In the Chinese government's view, the concept of internet sovereignty validates its legal and technical efforts to control access to independent information and spy on its citizens on a mass scale. Under this approach, cybersecurity threats can be defined broadly enough to include sharing information that diverges from official narratives.

The notion of internet sovereignty is also code for a multilateral approach to global governance of the internet, where states are the primary actors in determining the rules of the internet and civil society can be excluded from policy discussions. This approach contrasts with the "multi-stakeholder" model supported by the US, European Union, Brazil, India, and others, where civil society and industry can participate on an equal footing. Since 2014, the Chinese government has held its annual World Internet Conference in Wuzhen to promote its vision of the Internet, inviting like-minded governments while excluding civil society groups.

Russia is clearly also championing this idea, and its recently passed counterterrorism legislation reflects many elements of China's approach to internet regulation, including increased nationwide blocking, control over physical infrastructure, and pervasive surveillance. Recent media reports have described a series of high-level meetings between Russian officials and the architects of China's censorship and surveillance regimes, including Lu Wei, the former head of China's state internet information office, and Fang Binxing, the "father" of the Great Firewall. The reports suggest that Russia is seeking best practices and technology from Chinese companies that have built China's systems of control.

These reports are consistent with our research on surveillance in Ethiopia, where for many years, the Chinese company ZTE provided technology, training, and consulting services to Ethiopian authorities. The Ethiopian government has used this expertise to censor information critical of the government, spy on activists, and target vulnerable groups for repression.

Human Rights Watch is concerned about the further spread of the Chinese government's approach to internet controls beyond its borders, including the transfer of technology and know-how to other governments.

Building up the Orwellian Social Credit System

In June 2014, China's State Council issued a lengthy planning document, outlining the construction of a "Social Credit System." The goal of the system is to collect and integrate a wide range of personal information on all citizens and organizations, and use that information to score them. The system will score citizens not only based on their financial creditworthiness, such as mortgage or credit card payments, but also based on their social and possibly political behavior, including but not limited to purchasing preferences, adherence to traffic rules, and online posts. In the future, a person's social credit score may have an all-encompassing impact on a person's daily life, such as loan interest rates, school admissions and scholarships, access to public parks and tourist sites, and travel on planes and high-speed trains.

After the promulgation of the 2014 State Council document, various local and provincial governments – from local residential committees to the central government – across the country have issued policy documents to begin implementing the system, but so far, the scheme remains largely experimental and the actual impact has been limited. For example, the Guangdong provincial government has set up a website called Guangdong Credit where people can search for "credit information" of companies, organizations, and "key individuals," such as notary publics, licensed lawyers, and registered accountants. Human Rights Watch's test of the system on April 29 shows the current data set primarily involves business records, such as registration information and tax payment history. Data on individuals are still lacking. Human Rights Watch entered several common Chinese names, as well as the names of Guangdong-based human rights lawyers and activists in the "key individuals" search; no results were shown.

Another example is the website maintained by China's judiciary system. On the home page of the website, a list of names of people that the courts have determined as having lost their creditworthiness is constantly shown. One can also search for specific names in the system. Human Rights Watch tested this on May 1, by entering several common Chinese names into the search bar. Each entry yielded hundreds of results. By clicking on "details," a court record appears, showing why the person has been deemed to have lost their creditworthiness. However, cases of dissidents and activists seem to be not included. The name "Liu Xiaobo" resulted in 41 entries, but none of them refers to the imprisoned Nobel laureate. The same situation applied to the names of several other prominent dissidents Human Rights Watch tested.

So far, the consequences of appearing on a court-ordered blacklist appear to be largely restricted to being unable to buy tickets for planes or high-speed trains. By the end of 2015, over three million people in China had been blacklisted.

One major difficulty facing the government is the enormous task of integrating data, but it is apparently addressing the issue. A central data platform called Credit China has been established to encourage information sharing. An official at the central planning agency told the *Wall Street Journal* in late 2016 that the platform had collected 640 million pieces of credit information from 37 central-government departments and various local governments. And in April, Wuhan, Changsha, Hefei, and Nanchang – four major cities in different provinces – signed an agreement to share and integrate social credit data, state media reported.

The social credit scoring system has also enlisted the participation of major internet and e-commerce companies in China. In January 2015, the People's Bank of China issued a notice giving eight companies a six-month period to "prepare well the work of scoring individuals' credits" as "an important measure of the State Council to promote the social credit system." These eight companies include Tencent, one of China's biggest tech companies, which provides a range of services in social media, news media, online gaming; and Sesame Credits, a company under e-commerce giant Alibaba that also runs the e-money platform Zhifubao. Instead of just being rated on their financial history, as the estimated 300 million People's Bank of China users

are currently rated by the PBC's financial database, people using these companies' services could now be rated for their online behavior, too.

All kinds of details could be collected by these companies in forming credit ratings. The vast amount of data held by these companies include utilities payments, information from social media, and shopping records. Precisely what kind of information would be part of a person's credit report has not been made public, but state media has speculated that anything from "not showing up after calling Didi Taxi [an online ride-hailing service], being rated poorly [by users] on Taobao [an e-commerce platform], falsifying personal information to defraud insurance premiums" could negatively impact one's credit score. It is unclear how, or if, the government's social credit scores would be connected to the companies' scores and ratings. The State Council encourages these companies to "integrate the credit information disclosed by the government and the credit information not collected by the government."

Part of the impetus to set up such a system appears to be the authorities' concerns with a decline in "social morality" and desire to stamp out unscrupulous and illegal practices that undermine public confidence in the government. However, the system raises serious privacy concerns and has great potential for abuse given the lack of effective privacy protections in China. One of the most ominous aspects of the system is the ability to link an individual's speech to their social credit score. At least one human rights lawyer from Beijing, Li Xiaolin, was put on such a social credit blacklist in 2016 by a Beijing court after he posted his defense statement in a politically sensitive case. It is unclear what dispute resolution mechanisms are available to individuals to contest the ratings imposed on them.

The system, which is expected to be implemented by 2020, could have a serious chilling effect on internet speech. According to journalist Zhao Sile: "You already see how people can withdraw from expressing critical opinions online because they are afraid that their accounts can be shut down. If the government can enforce real-name registration and closely link people's speech to their daily life and economic opportunities, it will be an extremely powerful tool to force people into self-censorship."

Recommendations

- The US should provide support for programs that enhance access to information, freedom of expression and privacy in China, ranging from circumvention technology and digital security tools to broadcasting by the Broadcasting Board of Governors.
- The US Congress should call on US technology companies that do business in China to answer questions on how they respond to Chinese government's censorship and surveillance requests.
- Members of Congress should try to raise the profile of detained American publisher James Wang, and continue to call for the release of all those detained in China for exercising their right to free expression.

- The US should continue to call for the repeal or revision of laws in China that restrict peaceful expression, enable censorship, and oblige companies to participate in that censorship.

CHAIRMAN BARTHOLOMEW: All right. Senator7.

COMMISSIONER DORGAN: Thank you very much.

First of all, the testimony is excellent. We really appreciate you taking the time to be here.

A couple of years ago I was in Nanjing, and I was invited--actually I invited myself or I guess requested to speak to a group of students at a university there, and spoke to a group of 30, I think 30 to 50 graduate students, and there was a minder from the government with me, of course, but I asked the students, I said, you know, kids your age in the United States are using the Internet, just as you are, except they're able to access things on the Internet that you can't see because your government has decided what you can and cannot access.

And I said to some of them, you've talked about freedom, as they did, about they are free in China, et cetera, but you are not free to make your own decision about what you wish to access on the Internet. Your government does that for you. How do you feel about that? So that's the question I--and the question was not actually treated very seriously by the students, and one of them said immediately, with a smile, we have our ways around the Wall. And then smiled. And there was this murmur of assent by most of the other students in the room.

And as I indicated to you, there was a person from the Chinese government there, and I didn't pursue it further except they had treated it as an inconvenience perhaps, but one that they easily got around.

Now I'm wondering if you sense that's the case with most educated young people? These are people about to get their master's degrees. And the millennials who are using the Internet, if they have their ways around the Wall, will not those ways allow them to access information and perhaps also allow them to use social media to organize, and that's exactly what the government is afraid of, of course?

But tell me about this response I received. Would that be a response I would receive in most universities with most educated young people--oh, we have our ways around the Wall? What's your sense of that?

CHAIRMAN BARTHOLOMEW: You're the expert here.

MR. XIAO: I'm interacting with a lot of students from China studying at UC-Berkeley and some of them in my classroom. Yeah. I also keep very close contact with the people inside of China who actively circumvent the Wall. My sense is that if it's honest conversation, that they're really honest with you, then you're probably right, that among a group of master students, at least there may be one or two of them curious enough to do that.

It's not secret knowledge. It's commonly known. Yeah. But then they may not necessarily tell someone in some kind of semi-public places. Yeah. But that being said, there's a big issue of motivation to do that. For many Chinese Internet users, including the educated ones, it is inconvenient, that people rather don't want to bother. They're not motivated enough. They say, okay, so I know there's articles criticizing the Chinese government. Matter of fact, I know that too. I don't need to go around the Wall to know that, and then they still go on their daily

business because they feel it's like bad weather or it's like the smog. We don't like it, but we can't do anything about it.

COMMISSIONER DORGAN: But let me just further, I mean I was, I really challenged them with that question, thinking I would--I thought I would get one answer, and I got kind of an amused revelation on the Wall. And it seemed, as I left, and incidentally the government minder was not happy at all with that kind of approach challenging those students, but it seems to me as I left, it occurred to me that the issue of freedom, which I talked about a lot with them, the issue of freedom was interpreted by them in a slightly different way. Their pact with their government was I get a good education here, I've got a job when I get out of here, and so my travel along this opportunity is educate, job, and as long as the Chinese government continues to provide jobs and progress for them, they'll be fine.

But once, once that kind of opportunity doesn't exist, there's going to be lots of trouble. I sort of got the feeling they weren't interested in confronting this basic issue of freedom, particularly talking about the Internet, largely because that wasn't part of their thinking. They're thinking they're going to graduate and get a job, and they're able to access plenty.

DR. ROBERTS: I think this is part of the design of the Great Firewall, which is really smart on the part of the Chinese government, is that it makes it seem like it's not an imposition on freedom because it's possible to circumvent. So if it were not possible to circumvent, it would be much, much more difficult, you know, much more difficult for them to frame it that way.

And we see in the surveys that it is true that young people are much, much more likely to jump the Wall. So overall we see about five percent of urban residents are jumping the Wall.

For people where the Internet was available in China when they were in high school, it's about 25 percent. So it's much much higher; right. And I think that that is something that is an indication for the future.

But I also agree with what Professor Xiao was saying, is that even if people do know how to circumvent the Wall, there's an issue of motivation. So one of the recent studies I've done on the Internet in China has looked at the Instagram block during the Hong Kong protests in 2014, and during this time because Instagram was suddenly blocked by the Great Firewall, millions of people downloaded a VPN to jump the Wall because they wanted--the Instagram is a form of entertainment and they wanted to continue to access it.

And so this was all of a sudden a motivation to jump the Wall, and we see this effect all over data on the Internet. So there are hourly counts of the number of Wikipedia page views. On the day of Instagram block, there were twice as many Wikipedia page views of Chinese language blocked Wikipedia pages on that day.

So there is this issue of motivation that if something is blocked that you really want to access, like Instagram, which may be because you want to follow a celebrity, there are more reasons to jump the Wall. So I think that thinking about the pole across the Wall is as important as the cost of going across the Wall.

PANEL I QUESTION AND ANSWER

CHAIRMAN BARTHOLOMEW: Anybody else? Sophie? No. Okay.

Dr. Wortzel.

HEARING CO-CHAIR WORTZEL: First of all, Dr. Roberts, I said adjunct professor, and you're an assistant professor.

[Laughter.]

HEARING CO-CHAIR WORTZEL: I apologize for that.

DR. ROBERTS: No worry.

HEARING CO-CHAIR WORTZEL: I really have two questions of you. Dr. Richardson, I want to thank you for mentioning the social credit system. I think it's really important, and the influence of it, the potential influence, underappreciated, certainly here. But if you know, what ministries or organizations in the Party manage those social ratings? And what penalties are there for low ratings?

And then for all of you, one of the things that American businesses have complained bitterly about is the new set of regulations on data transfer and the ability to actually protect proprietary information moving among companies or between corporate offices in different countries because, as I understand the regulation, they have to really allow some element of the Chinese government to get a look at not only proprietary data but maybe design and pricing and things like that.

Do you want to start?

DR. RICHARDSON: Sure. I'll start by making you this promise, which is that as we come to understand more about the social credit system, I'm happy to keep you updated. It is very much a work in progress, and when we first sat down to start trying to get our heads around it, about a year ago, it was so fledgling and fragmentary at the time that we couldn't even really we felt write anything about it.

The original document, setting out the aspirations, came out of the State Council Information Office, which that and 50 cents--

[Laughter.]

DR. RICHARDSON: So it's a little hard to see where the actual origins lie, but we've seen reference to probably at least a dozen different government agencies, you know, many of the usual suspects, the PLA, but it's all the way through to the Ministry of Education, which is an opportunity to get information on teachers, I think for reasons that we would necessarily find problematic.

It's a little bit like, it's a little bit like Whack-a-Mole. You know, different government agencies keep sort of sticking their heads up and saying, well, we want this piece of it, and we want to control that piece of it. So we'll have to come back to you, but it certainly has prompted us to dig into various other surveillance related technologies and efforts, including things like the use of DNA, the use of GPSs to track movement, and we're happy to, happy to keep you posted on all of that.

I mean from our perspective, the most serious concern here is that there really are no privacy rights. There's almost no way to challenge these ratings. It's not clear to us yet what the range of punishments might be or even, in fact, what criminal charge could flow from saying

certain things online, or what happens to you if you have a very low score.

HEARING CO-CHAIR WORTZEL: I mean it's very 1984 like.

DR. RICHARDSON: Yeah, the word Orwellian has been used a lot.

CHAIRMAN BARTHOLOMEW: Data transfer.

HEARING CO-CHAIR WORTZEL: Data transfer. Anybody want to pick that ball up and run with it?

MR. XIAO: I don't follow in great detail, but I certainly know that it is part of this whole cyber sovereignty approach. There's a number of offices, and the most important one is this Cyber, CAC, Cyberspace Administration of China, which in China everything is like this. There's a government office, and there's a Party office, but matter of fact, the same group of people. They have two names.

So the CAC is a government office, but it's sitting in the same office of what's called the Central Leading Group for Cyberspace Affairs of the Communist Party. It's just their office, but it has a government title.

They have a number of major pushes, policies, and I know some think tank people that have been focusing on data security and cyber sovereignty, meaning every data coming through the Chinese cyberspace, they want to know, they have a right to know, and the state needs to know, whether you're a foreign company or not. So that's just part of that.

One more thing, if I can add, but that's also their dilemma, which is they want to control and surveil information, but their most difficulty, their concern, is the collateral damage of interacting the business transaction and trade. Yeah. And they know that. And that very often gives them a policy headache, how far they want to go. Yeah.

CHAIRMAN BARTHOLOMEW: Sorry. Sorry. Just a clarification, which is there is that policy dilemma, Xiao, but also are they not able to access the data of American companies that could disadvantage American companies in their efforts to operate in China and compete in China?

MR. XIAO: Well, yes. They, at an end, it's always, for the Chinese government, it's always the security over and the politics over rights of economic interests. Yeah. That's always the end. Even you can tell by the Leading Office name--security first. They talk about security, not talking about economic development.

CHAIRMAN BARTHOLOMEW: Okay.

HEARING CO-CHAIR WORTZEL: What strikes me, the dilemma here is even if the U.S. government or Congress attempted to put in place reciprocal requirements on Chinese companies, it only validates the Chinese concept of cyber sovereignty so I mean we're really between a rock and a hard place on the issue.

CHAIRMAN BARTHOLOMEW: Right.

Vice Chairman Shea.

VICE CHAIRMAN SHEA: Great. Thank you all for being here. Really interesting testimony.

I want to reverse the frame a little bit. Instead of negative, let's go positive. I mean say the Chinese did precisely what we all think they should do: eliminate their domestic censorship controls, allow freedom of expression, knock down the Great Wall, Great Firewall, allow free expression over the Internet, what would the impact be on Chinese society, its political system

and its economy, and what would the implications be for the United States? And just be careful what you say because your social credit score might be affected by your words.

[Laughter.]

MR. XIAO: I will not go further.

[Laughter.]

MR. XIAO: And, honestly, I think if that's the case, there's not going to be People's Republic of China. I think the Chinese leadership knows that. I think that Xi Jinping has many times mentioned that. Of course, I mean it's not instant overnight, but they surely, I think that rightly so, that if you let information flow really freely, the current Chinese Communist Party's monopoly of power doesn't last for too long.

That's how they understand it. That's how I think they're right in terms of estimation consequences. However, as we discussed, this information control, both domestically and in the Great Firewall, it's far from perfect, far from they would like matter of fact. So they, on the one hand, you will see they are quite on top of it in terms of the resources and the efforts and technology they invest.

They actually controlled the Internet over the past two decades, and that will continue to go on probably for a decade or so. The question probably is at what price? And can they continue to pay that?

Let's say the censorship is a tax for the Chinese Internet users, it's also taxing the government, politically and economically, the price that they're paying. That cost is getting higher and higher. Just look at the kind of--the one other thing I mention in my testimony is the public trust of the government. It's getting lower and lower, precisely because the people are more and more transparent. People can see you are hiring Fifty Cent Party. It's not too hard to tell who Fifty Cent and that kind of language. It's not hard to tell these days. Even you cannot directly say it too much, it will be deleted, but the information still goes around.

So there the government has a very insecure position that one, on the one hand, they keep, put a lid on. On the other hand, they know the people know. Yeah. And that is a situation quite different than I would say 20 or 30 years ago.

CHAIRMAN BARTHOLOMEW: Anybody else?

VICE CHAIRMAN SHEA: Dr. Roberts? Dr. Richardson?

DR. ROBERTS: I'm not sure, I'm not sure I can speculate on what would happen. I think, I do think, though, that Professor Xiao is right that there are three sort of dilemmas that the government faces with respect to censorship.

One is this backlash dilemma. The more visible censorship is, the more likely it is to have backlash, and I think that is why we are going to see the development of more and more invisible forms of censorship. So we've even seen this in the last few years. Search filtering instead of putting up an error. It doesn't put up an error anymore. It just sort of refilters your search results.

Even if your post is deleted, if you're signed in, you will see the post, but others won't. So there are more and more sort of ways of them figuring out how to make this invisible.

The second dilemma I think that the government faces is an information collection dilemma. So the problem that a lot of regimes like the Chinese government face is that they don't know what people think, and they're using the online space to collect that information. The

more they censor it, the less information they have.

So there's a problem, a problem there, and I think you will see that they allow certain types of information to flow online because they want to know what local governments are doing wrong.

And then the last is an economic dilemma, and I don't think that anyone knows. I think we need to do a lot more research to understand the actual price of censorship. We do a lot of economics research on the price of taxes, and we don't do a lot of economics research on the price of the taxes of information. And speaking to a lot of computer science students in China, they are constantly frustrated by the inability to access things like Google Code, the inability to access a lot of technology that's coming, the cutting edge technology coming out of the U.S.

And so I think that if we make those economic costs really clear, then sort of the first, the backlash against censorship by the elite, is going to be, is going to be larger.

DR. RICHARDSON: I'll just add a few thoughts in--

VICE CHAIRMAN SHEA: It's a big question.

DR. RICHARDSON: --in a different vein. I think for all the reasons that have been identified, it's not likely to happen anytime soon.

But try to imagine, you know, what else we and people around the world could know about China absent those controls, and how that could really profoundly change everything from bilateral relations to academic exchanges. I mean it would just be an entirely different universe.

But I think it's also incredibly important to contemplate the consequences for accountability, and I mean that on issues ranging from, you know, open access to information about who made decisions about Tiananmen on June 4, 1989 all the way through to things like public health or product safety scandals or the environment, if people could actually access all of the relevant information and act on it in a way presumably to produce public policies that were more consistent with what was deemed to be sort of in the general public good.

VICE CHAIRMAN SHEA: It seems to me what the CCP has going for it very strongly is that there is no obvious alternative to the CCP. I mean maybe the military; right? But if not the CCP, who would step in? And that's largely a result of an inability of alternative voices to express themselves within the societies. Is that fair?

MR. XIAO: Yes. Actually let's look at a very specific example. There's an ongoing drama of a politically connected tycoon in New York right now, Guo Wengui. It's, I have never seen something like this, which is in terms of looking at the Chinese government reaction to him. I have seen the crackdown on Ai Weiwei, for example. That's a big celebrity on the Internet. Yeah. But the other day, they simply shut him down on the Internet and then they arrest him. Yeah. That's physical force.

But this one, of course, he's outside. But the point is look at what the Chinese government is doing. Interpol. Chinese lawsuits, lawsuits against him--is there going to be more coming? The diplomatic, talking to bilaterals of different countries. Domestically, massive articles, media discredit him. They don't do that to Liu Xiaobo. They didn't do that to dissidents because they didn't want everybody to know their names in China, but they do that to him. They had to. Yeah. They had to.

VICE CHAIRMAN SHEA: Interesting.

MR. XIAO: So the amount of resources mobilized currently right at this moment and

overseas, not even mentioning the Fifty Cent Party and technology, everything, everything, the full power on him right now. So it's very simple. If you say this guy--only have a bunch of rumors, make it up, then what's the big deal? What's all this effort about, you know?

Then, of course, the directives that order the website what to do and what not to do. And also another thing about this particular case is on the Chinese social media, on the Chinese Internet, you don't see much information about him. No. Because very plain. But if you talk to the people in the city at least or the people, that's everybody is talking about. Yeah.

And it even goes together with just incidentally, but it's not really incidentally, with another national phenomenon, which is there's a Chinese soap opera called "In the Name of the People." Yeah, it's about anti-corruption. It's a Chinese official propaganda about boosting Xi Jinping's legitimacy, which he's the leader of anti-corruption. It's a well, relatively very well made Chinese soap opera, which because giving a particular room to show some political reality so it looks like a political reality show, and then boost Xi Jinping, how he's on top of it.

So everybody is talking about it. Everyone is reading about it. Everybody is watching about it. This time Guo Wengui, Guo Wengui story came out, it's really on top of that. Now there's another show, real show called "In the Name of Guo Wengui," yeah, which directly discrediting the whole anti-corruption campaign as a political struggle, power struggle, and the people think that's, you know, that is a frame of opposing.

Of course, it's not coincidental because both efforts are targeting to the Communist Party Congress, the Party Congress. And that was why the propaganda for it, that's why Guo Wengui here right now campaign for. So if you look at that, you realize if there is no Great Firewall, say, the Chinese politics would be very different.

Those oppositional political forces will play out their politics in the domestic media space and Internet. They wouldn't do from outside, and then, but from outside, usually you would think the Great Firewall censorship can shut them out so they're irrelevant. No. It's very relevant right now. Yeah. So that censorship is not--they prevent a lot of things, but in this case, it's a test how good that censorship is really, probably not by preventing people to know, but it can prevent people to act.

VICE CHAIRMAN SHEA: Uh-huh. Thank you.

CHAIRMAN BARTHOLOMEW: Thank you. Very interesting.

Commissioner Wessel.

COMMISSIONER WESSEL: Thank you all for being here and thanks to the Chair and Vice Chair for putting this together--and the staff.

HEARING CO-CHAIR WORTZEL: And the staff.

CHAIRMAN BARTHOLOMEW: And the staff.

COMMISSIONER WESSEL: I said "and the staff."

[Laughter.]

COMMISSIONER WESSEL: I hate to say I'm somewhat depressed by all of this. Because it feels to me like here in the U.S., there's somewhat of a human rights fatigue, that human rights is no longer the top values issue, if you will, that I think has driven much of it in the past, and is now being viewed for its economic costs. And I appreciate your analysis.

But I'm very concerned that for U.S. companies operating in China, it's an economic calculation. It's not a question of values. It's can they have access to the information they need?

Can they do what they need to do with their data flows, et cetera, rather than should they be spreading American values as the proponents of China PNTR argued that, you know, engagement would yield results?

I don't see those results, and I think it was you, Dr. Richardson, who talked about some of our companies that, you know, may be enabling in some ways through some of their activities, and for me I see that here now as well. We have a transaction, you may be aware of, where Ant Financial is trying to acquire MoneyGram, and MoneyGram is the number one, as I understand it, remittances vehicle for individuals. So individuals who are engaged in the Falun Gong activities or human dissidents, et cetera, the Chinese, if they're able to acquire this entity will have the financial data, the personal data, on all of those people.

We certainly have to take your recommendations in terms of what we need to do to pressure the Chinese. What do we need to do more to pressure our own people, our own companies? Our media, which has diminished its attention to human rights--there's a lot going on here, as we know, and that's consumed everyone--but how do we reignite attention and not just look at it as a dollar cost-benefit analysis, but, you know, for what this really is? Comments?

And I know each of you spends your lives doing this so that's why I'm--you know, what more would you like to see that's not happening that there are actually some tools that potentially can be used?

DR. RICHARDSON: Right. Well, I'll take a stab at it, and I will start with perhaps a little bit of optimism. This is, as I'm sure some of you know, the third China hearing this week. Governor Branstad's confirmation hearing was Tuesday. Yesterday, the CECC had a hearing about Hong Kong, and I have to say I was very relieved, pleased, encouraged to hear about as diverse a group of members as you could possibly get talk about human rights in China and really talk about it as an economic matter, as a way of creating transparency for everything from security discussions to trade ones, but also to talk about it in terms of values and doing the right thing for fellow human beings.

I have to say that optimism was significantly diminished by Secretary Tillerson's remarks yesterday, which seemed to suggest that he thinks we are in 1817, not 2017, about the role of human rights in U.S. foreign policy, where it seems to have simply been dismissed as a problematic afterthought in frankly language that sounded to me like it was written in Beijing. And that's enormously problematic.

So I think there's a lot of work to be done in Congress. I'm grateful for all of the members who care about these issues and who I think will fight the administration on it.

But I also think there are a lot of questions to be asked of American companies. Just to clarify, the ones I mentioned were Chinese companies.

COMMISSIONER WESSEL: Oh, I'm sorry. Okay.

DR. RICHARDSON: Not U.S. companies.

COMMISSIONER WESSEL: Okay.

DR. RICHARDSON: But I do think there is room for asking big tech firms how they are answering to demands inside China to share information or hand over source code or otherwise share critical technological information. And, you know, I don't say that to be uncharitable. It may be that they need certain kinds of legislation, for example, to be able to say we're prevented

from complying.

But I think there are a lot of questions there that could be surfaced, and that's an important point of leverage for the U.S.

COMMISSIONER WESSEL: Thank you.

Dr. Roberts.

DR. ROBERTS: Yes. Thank you.

Those are really good comments. And I think, I definitely don't want to suggest that the human rights issue is not a problem. I think that the logic, the Chinese government and many people in China don't see that frame as convincing, but they would see it as convincing in economic terms, and I think--but certainly, we care a lot about human rights, and this is one of the biggest issues when it comes to censorship.

I think that one of the things that we should focus on also in addition to sort of keeping American values and being consistent internally with U.S. companies is that when U.S. companies comply with regulations within China that there is the potential for these to leak into the U.S. also; right?

So we know that the Internet, in general, is a very international thing, and some recent work by Citizen Lab has showed that even Chinese social media companies like WeChat are censoring people within the U.S. because of their censorship technology within China. So how do we even--I mean it seems to me very difficult to even create a barrier if you were a company between what happens in China and what happens in the U.S.

And I think that we have to think about those issues and realize that we're in a very international space. The Internet doesn't really have boundaries, and that whatever we do in other spaces then leaks into many other countries and including our own. And so I think that's something that we need to think a little bit more about and to press U.S. companies on for sure.

COMMISSIONER WESSEL: Thank you.

MR. XIAO: I don't have a lot to add. I mean it is a fact that Chinese Internet market is so large, therefore--just by sheer number of Internet users--and therefore one is then China can develop those domestic companies that--domestic products using censorship as a competitive weapon to take over the Chinese market.

But also for any foreign company on the Internet, particularly a U.S. company, even at the beginning, even a startup, let's say Dropbox in the early days, even they were still looking only at the U.S. domestic markets, but on the Internet, inevitably, they know they are a global company, yeah, and they have potential markets of China and everywhere else, which makes them immediately start censoring themselves, thinking about the Chinese access, like I don't want to be blocked by Great Firewall.

So even before they actually do anything with China, yes, there are so many companies, technology companies, like that, because once you put yourself online, you realize they're the potential visitors and all of that and your brand can be affected. So that kind of censorship does project, yeah, because it's backed by the market power. So that is a challenge.

COMMISSIONER WESSEL: Thank you.

CHAIRMAN BARTHOLOMEW: Commissioner Tobin.

COMMISSIONER TOBIN: Thank you. Thank you all for very thought-provoking comments. On this round--I hope we'll have chance for a second round--but on this round I'd

like to direct my questions to you, Dr. Roberts.

As you all know, we are responsible for thinking about public policy and what can be done, and I found it absolutely intriguing to have you present the tax concept. As you say, the conceptualization you have is for most people in China censorship acts like a tax on information, requiring them to spend more money and time.

And then you go on to say in addition to the government, the U.S. government's efforts to shed light on human rights, the government should consider treating censorship as a tax.

So because we can educate through listening to you, can you give several examples, specific examples, because it's an economic concept, and I think the minute you get concrete about it, it will be easier for a congressperson or staff, for them to see what can be done and how important it is? That's part one of my question.

The second thing is you mentioned in your research that you do qualitative research with people. Many Chinese leave the mainland, come here. Have you done either a study where you're looking at what they might have said if you met with them in the PRC and then here and then get a sense of is there any "aha," I feel so much freer, or do they experience the Internet differently?

So those are my questions.

DR. ROBERTS: Those are both great questions. As an academic, I tend to think of things as a tax. A few concrete--a few concrete things that could be done. First is what the USTR is already doing, which is thinking about censorship as a tariff. I think that's certainly--that's the way I think about it also, is that it protects certain companies within China, and there are companies that have an interest in keeping the Firewall because it protects them from U.S. competition.

But it also really hurts a lot of entrepreneurs within China that don't have access or have a taxed access to some of the most cutting-edge Internet technology. So that's the first sort of concrete example.

But the second concrete example is if we frame it more as a tax, as well as a human rights issue, which it's definitely both, I think that people who are using the Internet in China would be able to see it a little bit more clearly. So, for example, from the comments from before that a lot of people in China say, well, my freedom isn't impeded by censorship because I just evade it, but yet it's not impeded by censorship, meaning you can still evade it, but you have to spend money and time in order to do that, and that is an imposition on your time and your money, and it's taxing you, and it's making you spend that time to do it.

And so in framing it that way, I think that that's more understandable sometimes to people, especially even when I talk to my students who are from China. It's more understandable to them about why that's an imposition on them rather than, rather than this is, you know, something that blocks you completely because they don't see it as that.

So in that sense, doing more research, actually being able to communicate the economic cost of censorship to both Chinese students and Chinese businesses I think would be really useful, and I think that's something that I certainly want to do more research on in the future, but I think that if we can sort of make that more clear, it would be helpful.

The second is on--

COMMISSIONER TOBIN: Not just in economics, even underneath the economic

model, concrete experience, the human experience of that tax.

DR. ROBERTS: Exactly, yes. So I talk to a lot of students who get very frustrated when they go back. They study in the U.S., they go back to China, and they have trouble accessing code, they have trouble accessing, you know, shared Dropboxes. They have trouble accessing--and this is a tax on their education; right? This is a tax on human capital and innovation, and I think that that is something that is easier to communicate sometimes because people, you know, students are so excited about learning, and they want to compete in a really competitive international market for computer scientists, for people working in any sort of human capital sector.

And I think that that, that that rings really true to a lot of students who go back and then are frustrated the Firewall and their lack of access to information.

So I think, I'm actually starting some work trying to understand how students who come to the U.S. and then go back and are affected by censorship and how that influences how they view censorship, but I don't have any data on that right now. All I know is that they are much, much more likely to evade censorship when they go back, but I don't know how that changes their views of it.

COMMISSIONER TOBIN: That would be interesting to monitor, and it goes back to Mr. Xiao's concept of collateral damage, and if China's instinct as a country to try to be more innovative, the collateral damage of this oppression and lack of freedom is preventing that.

Thank you.

CHAIRMAN BARTHOLOMEW: All right. Commissioner Stivers.

COMMISSIONER STIVERS: Thank you all for your excellent, excellent testimonies. Mr. Xiao, in particular, your recommendation that we should be boosting U.S. Internet freedom initiatives is well received certainly by me.

Dr. Roberts, I support your recommendation that obviously more research should be done in terms of quantifying the economic impact of censorship and that the U.S. government should continue treating censorship as an tax on information, censorship as a tax and non-tariff barrier.

Sophie, Dr. Richardson, in terms of your recommendation that the U.S. Congress should call U.S. technology companies to testify, kind of following up on Commissioner Wessel's question, can you be a little bit more specific in terms of telling us about U.S. technology companies? Which ones are taking positive steps in terms of their relations with China and supporting censorship activities, and those who maybe are more concerning--I remember it wasn't--I guess it was that long ago when the House Foreign Affairs Committee called the technology companies in that landmark hearing that got so much attention, and there was real policy actions that happened after that.

I don't think we got the legislation over the finish line, but certainly the companies were galvanized to take more action. They had a code of conduct and there was a lot of activity around that for a long time.

Does this need to happen again or are the issues not as important as they were then because, you know, the tech companies, they'll argue that if they're not there in China, that they're a force for a good and they're providing more open information, and if they're not there, they'll cede the market to the Chinese companies that will cooperate with Chinese authorities? So can you kind of give us the state of play and who's up, who's down, who's doing the right

things, and who should we be concerned with?

DR. RICHARDSON: It's not a simple list. I'm going to ask my panelists to help me out here. Let me give you just a sense of some of the companies I would love to put questions to. Probably close to the top of the list, Facebook, which has not yet entered China, but I think needs to answer some fairly significant questions about how they will protect users' privacy if they do enter China, and that's really sort of their bread and butter, so to speak.

I think also there's been quite a bit of reporting about Apple and what access to certain kinds of technology they may have--and I stress the word "may"--have given. It was--Xiao, help me out here--it was Google that moved its servers; correct?

MR. XIAO: Yeah, Google still has some research and mobile--yeah. Yeah, but Google right now is in very bad terms still with Chinese government. My HikingGFW website measuring the top 100, top 1,000 websites, the first, about first hundred websites, Google, Google, Google, Google Friends, Google Belgian, the Google data, Google, pretty much all Google services have been blocked by Great Firewall, and that's the only company that have that kind of treatment. It can tell you, tell you something.

DR. RICHARDSON: Yeah, I think any Internet service provider, any company that's selling technology, and again I want to be careful to stress, these are not necessarily companies we know or are suggesting have done anything wrong. It's about answering certain kinds of questions about what they will do when we think inevitably they are faced with questions about sharing data.

And this extends all the way through companies like Uber, for example, or even Airbnb, that are now providing services in China that are fundamentally about sharing individuals' information or their location, how that information is managed. Is that, does Airbnb hand information over to the Public Security Bureau as any hotel in China is obliged to do?

You know, it's not clear. So I think it's a long and complicated conversation that you might want to imagine breaking down according to sector, essentially, you know, a technology, a company that was, for example, just selling technology as opposed to providing certain kinds of services as opposed to actual ISPs, but I'm sure that Xiao will now tell you everything I just got wrong.

[Laughter.]

MR. XIAO: No, no.

DR. RICHARDSON: He's so diplomatic.

MR. XIAO: From Chinese government point of view, I know that like Uber or Airbnb, if any foreign company has this much information on Chinese individuals, Chinese government will say we want that information. You cannot just keep it. Yeah. And we want that data inside of China. You put your server inside of China. Otherwise, you cannot have China market. That's what their so-called cyber sovereignty is about. Yeah.

CHAIRMAN BARTHOLOMEW: Okay.

COMMISSIONER STIVERS: Thank you.

CHAIRMAN BARTHOLOMEW: Senator Goodwin.

COMMISSIONER GOODWIN: Thank you.

I certainly join my colleagues in expressing my appreciation to the panel for their insight and testimony here today.

And as a follow-up to Commissioner Stivers' question, I'm certainly interested in hearing about how these tech companies respond to requests for censorship for lack of a better description. These are companies that--rightfully so--hold themselves out as paragons of free expression and free thought and human communication and connectivity, and they've certainly been allowed to grow and prosper in societies where those principles form the bedrock of our civil society.

So, again, I'm very interested in how they respond to requests for censorship, but I'm also equally interested in how they're asked. Is it explicit? Do this or we'll do that. In the case of--you mentioned Apple--a recently well-reported instance where an app for The New York Times was removed from the store in China.

What's your sense of how that sort of development occurred? Is it again explicit or is it more subtle? And then what happens if they said no? Do they--and if Apple, a company of that size and with those resources, cannot, would do other companies have the ability to do or not do?

DR. RICHARDSON: Xiao, do you want to take a first stab at that?

MR. XIAO: Well, then, we all remember the last, not too long ago, but actually quite long ago, the hearing about companies doing China--Yahoo and Google. I was sitting there. Right. I was at that hearing too.

It was after that or around that time, there was also momentum that corporate responsibility, that for the companies together to have some code of conduct regarding freedom of expression. So collectively they can sort of holding out government--Chinese state pressure or any government pressure, as matter of fact, better than individual companies. Otherwise, different companies have different interests. For example, Apple. Apple has huge interest of all these China laborers and producing their components; therefore, they are, their position is quite different than some other company that doesn't have the same kind of economic interests like that.

But if you put them together, hopefully, they have a more stronger strengths. Unfortunately, it didn't happen that well. The foreign companies right now, including American companies, as long as you're interested in China's market and going to China's market, you behave just like the Chinese companies or maybe even worse. Yeah. They don't have much things to bargain that they can do a little bit better than the Chinese companies.

I haven't seen the significant difference at all, yeah. And that's partially because the Chinese government put much more pressure now than say even ten years ago or five years ago to all the companies, much stronger demand. If you don't meet their demands, you don't get China. You don't get entrance of the market. And the Chinese market is really big now so that's--the Chinese government knows that using that economic power for their political purpose, and they play that very well.

DR. ROBERTS: Just to add one thing on the leverage of U.S. companies in China. I think they think a lot about access to the Chinese market. I think that's a really important obviously motivation for a lot of these companies. But I also think--I just want to also stress the amount that U.S.--social media companies, in particular, are some of our biggest assets against censorship because so many people want to access them from China.

So I think that sometimes we forget how much the Chinese government would like them in some sense to come in because then there isn't as much motivation for them to go across the

Wall; right? So if you look at the Instagram block in China, that millions of people right when Instagram was blocked decided to evade censorship because they all wanted to get on Instagram.

One of the first things they downloaded was the Facebook app; right. So there's a pull of U.S. social media companies across the Wall. I think we need to encourage U.S. social media companies to realize that they have some leverage, right, because they are a motivation for people to jump the Wall.

I'm not exactly sure how that all plays out in policy, but I do think it's something that we have to sort of remember.

DR. RICHARDSON: I'll just add a couple of dimensions to this. One is that, Commissioner Goodwin, I hope some of these companies feel a bit more compelled to answer the questions coming from you than coming from us. Some of them have been quite obstructionist when we've put precisely these kinds of questions to them.

On the flip side, we have had some companies explain to us in a fair amount of detail what sort of requests have been made of them and how they've responded, and it's gone fine. They've pushed back and in some instances been okay. So it's hard to give you sort of a perfect overview of how this plays out because I think it varies somewhat from company to company.

But I think there may also be success stories or best practices or ways that these companies can choose to respond as a group so that none of them individually suffers any particular disadvantage for having resisted, you know, and hopefully sets a bit of an example; right? That would be--yeah, that would be a nice story, too.

I do also think it's the case that while I do think there's enormous pull towards the international firms, a lot of Chinese companies have been established and grown up to provide some of these services so that it is somewhat less compelling I think for the companies to have to go through, for example, the hassle of talking to you or answering criticisms from us about how they're going to manage these kinds of problems because there's not necessarily that much of a market there for them.

COMMISSIONER GOODWIN: Thank you.

CHAIRMAN BARTHOLOMEW: All right. Commissioner Talent, Senator Talent.

COMMISSIONER TALENT: Two questions. First, for Dr. Roberts, although certainly the other panelists can comment. You've referred to this as a tax, which I think is a useful analytical concept. I'd like to get a better flavor from the standpoint of the average Chinese citizen, whoever that is. How big is the tax for them?

How much do they feel it? I think of my Internet, you know, what I do if I want to surf the net for an hour, you know, do sports. I'll read a lot of a pol--I assume that anybody who is interested in politics feels this. But how much does it affect what the average person can do or read and how aware are they of it? With examples. And if the others want to chime in, please.

And the second question, for all of you, so the repression has been increasing the last four or five years, and I'm interested in your estimates as to why? Okay. Is this personal to Xi Jinping and his leadership? Is the regime more concerned perhaps about dissidents within the Party? Are they feeling less stable in general? Is it because they knew they were going to do this more aggressive foreign policy and they wanted to make--I mean are they concerned about the economy slowing down?

Why? I mean they've always obviously tried to control information. It's the nature of the

regime, but it's gotten worse. So if you have any speculation on that I'd appreciate it.

DR. ROBERTS: Thank you. Those are great comments. So I think it really depends on who you are, how much of a tax it is, and also how much you're aware of it. So I think it's a tax for everyone, but not many people are aware how much they're missing; right?

So it's sort of not knowing what you're missing that makes censorship really difficult for people to evade because they don't even know what's beyond the Wall. So when we ask people why do they not evade censorship, many say that they don't know what we're talking about, and other portions say I have no reason to. And other portions say it's too bothersome; I don't really know how. And then very few say that I do.

For entrepreneurs, especially for people in tech, I think it's a very big tax, and it's something that they're very aware of. For your sort of typical citizen, I think it's a huge tax on what they know, but they're not really aware of what they don't know.

And one sort of specific example of this, I've done a lot of interviews just asking people about pretty well-known and well-covered in the U.S. domestic issues within China that were events like protest events, arrested activists. People just don't know that these even happened. Or maybe they heard of them but they thought maybe they weren't very important because nobody was talking about them; right. So there's this double edge of that.

COMMISSIONER TALENT: Would it intrude on the average person's hobbies? You know, I'm just trying to get a flavor. I'm interested in sports.

DR. ROBERTS: Yeah.

COMMISSIONER TALENT: You know, maybe because of Yao Ming, I've been following the NBA.

DR. ROBERTS: Yeah.

COMMISSIONER TALENT: So can I get access to the websites, inside a website about the NBA? Or discussion forums online? I mean music, that sort of thing.

DR. ROBERTS: Right. Yes, certainly music, TV shows are sometimes blocked within China, and I think those are times where there's more of a pole across the Wall.

Instagram, when that was blocked, that was a huge pole against the Wall. We saw that within the data. Even pornography is something that is blocked within China, and I think that's a pole across the Wall. I also think that the other way that it affects typical individuals within China, is that I think censorship increases the amount that people believe and share misinformation.

Because there's some awareness that there are some things that are censored, then any rumor is sort of like more likely to be true, and there's a huge problem with misinformation--

COMMISSIONER TALENT: Of course, in fairness, we have a little bit of sharing misinformation.

[Laughter.]

COMMISSIONER TALENT: Here in our--

DR. ROBERTS: It's a problem. It's a problem of the Internet, in general, definitely. Certainly it's true. But there's a huge amount of misinformation about health and about the government in China, and I think that it's very confusing to be a consumer of political information in China, and so certainly people are aware of entertainment taxes, and I think they're also just much less informed about politics than they would be otherwise. Whether they

know that or not is a separate issue.

MR. XIAO: Just briefly about why this intensified policy for last four years. Xi Jinping. Yes, it was Xi Jinping. But he's not just one person. There's a whole force behind him that share the same belief, which is Internet is getting out of control, that before the previous one, even they tried everything, it's not enough.

So what I call this phase is Empire Strikes Back. Yeah. And another reason, which is very interesting--now, it's become a bit more clear--it is because of internal politics. It's not just about dissidents and activists and public intellectuals.

It's about their own colleagues, yeah, the internal house struggle. So Xi wants to make sure he controls the Internet. Yeah. And that's why when finally the politics, the backlash shows or pushback shows, it shows up on Twitter here; right--somewhere in New York. You cannot show it in China because they need control of that space. And it's not a smart reason at all to put this much control over the Internet.

COMMISSIONER TALENT: Thank you, Madam Chairman. I suspected that. Commissioner Shea's question about alternative voices, who are they afraid of? And the natural thing would be afraid of rivals within the Party and use the Internet to gain a platform.

Thank you.

CHAIRMAN BARTHOLOMEW: Great. Sophie, quickly.

DR. RICHARDSON: Yeah. Just one quick response to Senator Talent's question on why more repression? I don't think Xi Jinping and his allies in the Chinese government as a whole are being made to pay a price for it. And when you face no unpleasant consequence for carrying on this way, why not?

CHAIRMAN BARTHOLOMEW: Yeah. Thanks.

And I'm going to take the prerogative of the chair, if our witnesses can give us five more minutes, that would be terrific. To just start, though, with a personal statement, which is that it has been one of the great honors of my professional life to work with some of you on all of this. Dr. Roberts, welcome to the community.

Xiao, it's been a long time we've been doing this. Sophie, you also. So thank you for your leadership on this, and it's obviously an interesting time of year. Today is May 4, which we're almost at the 100th anniversary of one of the movements of Chinese citizens speaking out expressing their concerns.

We are, of course, coming up to June 4. Xiao, I know that it changed the path of your life. Tiananmen massacre. That astrophysics is probably weaker because you didn't commit your life to working on astrophysics, but the rest of us and the people in China are certainly stronger and benefiting from the brilliance that you bring to that. So thank you very much.

And, of course, we're coming up to the 20th anniversary of the handover of Hong Kong. All of this, in addition, to the Party Congress that is happening. It was an honor for me the other night be able to eat with Martin Lee and Joshua Wong, and I think that we need to acknowledge the companies that are doing the right thing.

So The New York Times, I want to mention, which is, of course, continuing to do excellent reporting in China at some cost, not just financial costs in terms of what it costs to keep the reporters there, but at some cost to its own revenues, and also I'd like to acknowledge Reed Hastings and Netflix, which are airing on May 26 the documentary about Joshua Wong, and that

is taking some risk for them about blowback, so at the same time that we raise concerns about companies that we think are not carrying forth values of the access to the free flow of information.

So that's my comments aside. But a couple of questions, which you guys have touched on a little bit, but I'm wondering a little bit more, how do people know what they don't know? I know when I get on the Internet, I go down rabbit holes. I think all of us. Hours pass, and we look up and we think, uh-oh, I didn't get this done, but I learned this.

The Chinese are talking about setting up their version of Wikipedia. People are going to be able to spend hours out there. How do they know what they don't know is one?

And then the second one, I'm interested, you know, is the Gini coefficient is changing in China and there's increased economic stratification and the impact of the stratification of access to information. Dr. Roberts, you introduced a concept of a tax of time and a tax of money, but that means that only certain classes of people get access to the kind of information we're talking about, and are we seeing that play out? And what happened? So two broad questions, but I'm interested in your comments.

MR. XIAO: One comment I can say is that Internet, social media, in general, because these days in China, everybody has cell phones and they spend an awful lot of time on WeChat or something in their daily life. Across the different social classes, the behavior is very social, meaning you do what your group does. You do what your friends do, what the other people do.

If you're hanging out with a group of people that do not seek for alternative information, then you do not. Most people do not. It's very collective behavior online. And then, of course, there's always exceptions. Those people also hang out together seeking each other on common networks. And then they polarize.

Internet, in that sense, sometimes we think it's an equalizer, level the playground and information, which in some part is true. But the other part is really not true. Your question is right. The people with different behavior and different interests and different motivations, they have lack of interest across boundaries to do different things.

Even they know they could, maybe take some effort, but I see so many people just familiar with their routines. If that routine doesn't include seeking for alternative views, then they don't because they want to be just like everybody else, and that is a big pattern on online activities.

DR. ROBERTS: I completely agree. I think we worry about the Internet causing polarization in the U.S., and I think that censorship exacerbates that in China by creating barriers that we select. As humans, we select information that confirms our beliefs, and if there are barriers to selecting information that maybe push what you think, then that makes that even worse, and one of the things that I think censorship is doing in China is creating a divide between what we think of in political science as the core and the periphery.

And I think that that makes it more difficult to organize collective action or any type of push for government accountability. So I agree with Professor Xiao that I think this is causing more polarization in China, and it's also contributing to inequality because as censorship influences what people know about the economy, how they invest, how they obtain human capital, people who have more resources are able to do that more easily.

CHAIRMAN BARTHOLOMEW: Sophie, anything?

DR. RICHARDSON: All I can add is a little bit about our own experience where we know that the people who seek and consume our information or try to access our website, it's a very specific group of people, and that to try to get beyond that is extremely difficult. I mean there's almost no discussion that would lead you to our work if you weren't already part of that community.

And we don't get mentioned in the State press. We don't get interviewed or invited to testify and so, yeah, it can be very hard I think to get beyond those boundaries without broader ways of communicating or sharing information.

CHAIRMAN BARTHOLOMEW: Right. One way, of course, is to help support people who are working to bring information to people who are workers in China, and there are some good people working on that.

So we've run over. Thank you all very much for your thoughts and the time that you've given to us. We look forward to continuing to work with you. We're going to take a ten-minute break. So we'll start the next panel five minutes late, but thank you.

[Whereupon, a short recess was taken.]

PANEL II INTRODUCTION BY CHAIRMAN CAROLYN BARTHOLOMEW

CHAIRMAN BARTHOLOMEW: All right. I'm pleased to see that our conversation earlier, our panel earlier, has engendered so much interest in freedom of speech as people have been talking during the break. They are interesting issues, they are timely issues, and they're important issues to the U.S., clearly both in terms of our values and in terms of economic interests and our security issues.

So panel two, I'd like to introduce our first panelist. Dan Southerland has also testified before us before. He, until December 2016, was the Executive Editor of Radio Free Asia, a congressionally-funded service that broadcasts news and analysis via radio, TV and multiple other platforms to Asian countries whose governments restrict the media. I'd note that some of us were there for the birth of RFA. That's how long we've been around, and Vice President Biden was very important in that initiative.

Dan, of course, is also part of the family. And I want to thank him for bringing us the next generation of people who are interested and concerned about these issues. For those of you who don't know, we have a bit of a conflict here: Dan's son, Matt, works on our staff.

Before Dan was at RFA, he was a correspondent in Asia for nearly 20 years, also was a diplomatic correspondent based in D.C. for the Christian Science Monitor, during which time he traveled to more than 40 countries with five U.S. Secretaries of State, was nominated for the Pulitzer Prize in recognition of his coverage of the Tiananmen Square massacre, June 4, 1989, and he was awarded the Edward Weintal Prize for distinguished diplomatic reporting in 1995.

He holds degrees from the University of North Carolina, Harvard and Columbia. Welcome back, Dan, and again thank you. Thank you for giving us your son.

Next we will hear from Shanthi Kalathil--am I pronouncing it correctly--a Director of the National Endowment for Democracy's International Forum for Democratic Studies--again, a very important organization at a very important time.

Ms. Kalathil recently published the report Beyond the Great Firewall: How China Became a Global Information Power, and she is co-author of Open Networks, Closed Regimes: The Impact of the Internet on the Authoritarian Rule, with Rebecca MacKinnon, I believe--did she--

MS. KALATHIL: No.

CHAIRMAN BARTHOLOMEW: No, not. Okay. It's a book that examines the Internet and political transition in eight authoritarian contexts.

She was previously a Senior Democracy Fellow at the U.S. Agency for International Development, an organization I'll put a plug in for here, a non-resident Associate at Georgetown's Institute for the Study of Diplomacy, and a Hong Kong-based staff reporter for the Wall Street Journal Asia.

She holds degrees from Berkeley, U.C. Berkeley, and the London School of Economics and Political Science. Thank you for being here.

For our last witness in the media portion of this hearing, we will hear from Sarah Cook--somebody else we know well--Senior Research Analyst for East Asia at Freedom House--another important organization. She directs the China Media Bulletin, a monthly digest in English and Chinese providing news and analysis on media freedom developments related to

China, and is the author of several Asian country reports for Freedom House's annual publications.

In the last few years, she has also published three special reports about China for Freedom House: The Battle for China's Spirit in 2017; The Politburo's Predicament in 2015; and The Long Shadow of Chinese Censorship in 2013.

Before joining Freedom House, Ms. Cook co-edited the English translation of A China More Just, a memoir by prominent rights attorney Gao Zhisheng, and was twice a delegate to the U.N. Human Rights Commission meeting in Geneva for an NGO working group on religious freedom in China.

She holds degrees from Pomona College and the School of Oriental and African Studies. Welcome back, Sarah. We're always glad to have you testify again.

So, once again, please limit your remarks to seven minutes. I think we've got somebody who will hold the sign up for you. Thanks, Dan. And we'll go ahead and start with you.

OPENING STATEMENT OF DAN SOUTHERLAND, FORMER EXECUTIVE EDITOR, RADIO FREE ASIA

MR. SOUTHERLAND: Thank you. And I'll be sure to make this--

CHAIRMAN BARTHOLOMEW: Do you need some water?

MR. SOUTHERLAND: I've got water. I'm just worried about rushing through this too fast. I have so much to say. Can you hear me all right?

Okay. Thanks for bringing me back for a third time. I've been asked to talk about--oh, thank you so much--I'm just going to try to push through here. I've already had half a bottle.

[Laughter.]

MR. SOUTHERLAND: In fact, they asked me, they said, okay, you can have a bottle because you're on the panel.

[Laughter.]

MR. SOUTHERLAND: I was asked to talk about a lot of things--challenges facing both Chinese and foreign journalists in China as well as about China's growing global media influence.

When I last spoke here in 2008--that was nine years ago--I mentioned that Chinese journalists were doing some outstanding reporting on the Sichuan earthquake that hit Sichuan in March of 2008. The reporting ended once journalists began going deeper into why so many schoolhouses had collapsed in the earthquake. It was a scandal. They called them "tofu" schoolhouses or something like that.

This reporting ended and much of the best investigative reporting in China has been done over the past half a dozen years or so by foreign reporters, several of whom have addressed that most sensitive issue--the wealth of the families, accumulated by the families of leaders, the top leaders of the country.

I emphasize investigative reporting throughout because it's obviously the hardest thing to do, and in many ways, it's getting at things that are hidden so I'll come back to it time and time again.

Getting to the Chinese reporters, many of them have studied journalism, but they don't plan to hang around for long doing it. They work for a few years to get a little experience. They call them "young rice bowl" reporters. And once they've done that, they move on to better jobs, and some of the best and brightest are the ones who move on and don't stay in journalism.

We can discuss later what the reasons for all this are. Their view of investigative journalism can be summed up by a Chinese saying, translated roughly as "hard work for little reward."

[Laughter.]

MR. SOUTHERLAND: And they also tend to say it's dangerous, and it is.

Hu Shuli, the founder and editor-in-chief of Caixin Media, stands out as an exception, and I don't know how she does it, but over the years, she's broken numerous investigative stories on business and financial corruption, and this can be really challenging work. In fact, she's being threatened with a lawsuit as we speak.

When it comes to foreign reporters in China, I think the Foreign Correspondents Club of China's report on--quote--"working conditions"--unquote--for 2016 says everything you need to

know.

Quote: "The reporting environment for foreign journalists working in China is proving hostile for yet another year. Intimidation of sources and local staff, growing harassment and obstruction are major challenges." End of quote.

The good news, if there is good news, is that at least a few of the foreign reporters whose visas were delayed or denied have now obtained new visas.

But I want to stress the risks that some Chinese run in continuing to try to pursue the news. Chinese assistants who work for foreign reporters are particularly vulnerable. They're often invited in for "chats" with the police, so-called "chats," which are basically intimidation sessions, you know, tell us what your boss is up to, that kind of thing. You can help us. Very scary stuff.

When I reported from China for more than five years in the 1980s and then later for some months in 1995, I knew the worst thing that could happen to me was just to be expelled. But the Chinese reporters and foreign reporter assistants can be jailed, and several were, even at that time.

I got used to be constantly followed by unidentified men in cars and motor bikes, on foot, but these days the thugs who assault foreign journalists is something new. Two months ago, some thugs roughed up a BBC crew as they were trying to interview a petitioner in the provinces. They smashed the cameras and forced the BBC guys to write some kind of confession to get released.

Since the massacre in the spring of 1989, China's leaders have been convinced that the country's international image has been damaged by Western reporting.

China has worked hard since then to present itself as a peace-loving nation whose rise threatens no one.

Once he came to power in 2012, President Xi made image building "soft power," including broadcasting, a key part of his vision of China regaining its greatness.

By any calculation--actually I should mention David Shambaugh, whom you probably know, estimated that China now spends $10 billion a year on soft power.

CHAIRMAN BARTHOLOMEW: Ten billion?

MR. SOUTHERLAND: Ten billion. Yeah. Nobody probably has the exact number, but I think he probably has good sources. And by any calculation, China is vastly outspending the U.S. on soft power, including broadcasting, and broadcasting has been tasked with promoting China's desire for peaceful win-win solutions. I don't know how many times I've heard that.

The Broadcasting Board of Governors, the BBG, which oversees U.S. international broadcasting, spent $777 million last year on all of international broadcasts by five entities, including RFA, VOA, and others. Only about 50 million of that, as I understand it, went to broadcasting on multiple platforms to China.

So I guess it's obvious that as one recommendation I would favor increasing the amount of money devoted to broadcasting.

Now I'll turn to China's global media influence. In my written testimony, I talk about the effectiveness of this influence. I've chosen to look at two continents--Africa and Australia--in order to examine what might work for China pretty well, which is Africa, and what might not work so well, which is Australia.

In Africa, CCTV and the official Xinhua news agency have secured partnerships. They've made investments with African media across the continent. Their success stems partly from offering to present African developments in a favorable light, in effect, countering what some Africans regard as mostly negative news reports from the Western reporters--famine, disease, corruption, and so forth.

I chose to focus on Australia partly because that influence on the media has been extensive but also because Australia has an alliance with the United States. China's been trying unsuccessfully so far to win Australia's support for its activities in the South China Sea, which is something that's really got to be watched, and at least Australia's neutrality regarding the South China Sea.

Australians meanwhile are debating every aspect of Chinese involvement in Australia--it's hard to keep up with it--support for Confucius Institutes and, in particular, donations given by a Chinese-Australian to a university, which is now having problems over there, as well as to both major political parties.

The guy, by the way, the Australian-Chinese complained that he wasn't getting his money's worth, which I thought was pretty entertaining.

Finally, I'll make recommendations. First, the U.S. government should raise its concerns at the highest level when American journalists' visas are delayed or denied. Vice President Biden raised the issue with President Xi in 2013. I think it had an impact.

Two, the U.S. government, also at a high level, should raise the issue of China's jamming of RFA and VOA radio broadcasts throughout its territory.

Three, it would be good if members of Congress also raised these concerns when they visit China. I'll give you an example of how different U.S. departments worked together to get a good result on a kind of outrageous case in China. An RFA Uyghur reporter named Shohret Hoshur had three of his brothers jailed in Xinjiang because of the work that he was doing for RFA.

The message we got was get your brother to stop making all these phone calls. The guy works all night sometimes. Talks to police, talks to everybody in Xinjiang. It's amazing what he can get. Just get him to stop this, and we'll let you out of jail. The State Department pursued the case at all levels, helped to secure--push from the State Department but others as well--we finally secured the release of two of the brothers.

I assume the one still being held is kind of a hostage. I don't know. Two U.S. Senators, Marco Rubio and Mark Warner, wrote to John Kerry regarding the case and got his interest. This was an occasion when not all branches, but many branches of the U.S. government worked together to counter some wrongdoing.

After watching this particular issue over the years, I can safely say that Shohret's brothers were just trying to do their jobs. They had nothing to do with the allegation that they, quote, "endangered national security." Not true.

Reciprocity. If China begins denying or delaying visa renewals again, I think the U.S. should consider delaying visas of Chinese media executives, not the journalists, planning to visit the United States. Show that we really care about this, and we don't like the way our journalists have been bullied and so forth.

I'm not advocating a tit-for-tat approach against Chinese journalists. As China expert

Robert Daly once explained, punishing China's journalists for a situation beyond their control might only tell the world that our commitment to free speech is only skin deep. So it's a nuanced thing that has to be debated. I'd like to hear more from foreign correspondents about it.

And that's it. Did I make the seven minutes?

CHAIRMAN BARTHOLOMEW: You went actually a little bit over, but that's okay. We don't have somebody with a sign. We actually have buzzers, the lights here.

PREPARED STATEMENT OF DAN SOUTHERLAND, FORMER EXECUTIVE EDITOR, RADIO FREE

Asia Hearing on "Information Controls, Global Media Influence, and Cyber Warfare Strategy"

Testimony before
The U.S.-China Economic and Security Review Commission

May 04, 2017

I've been asked to comment on China's global media influence as well as on the current challenges facing both foreign and local journalists working in China. I'll focus my written testimony first on the foreign correspondents and Chinese journalists and then on China's global media influence. I'll save many of my recommendations regarding the journalists working in China for my oral presentation.

I'll devote the lengthiest part of my written testimony to China's global media influence and save a number of my comments and recommendations regarding the foreign and domestic media in China for the oral presentation.

At the end of this written testimony I'll describe China's media influence on two continents—Australia and Africa. Australia's experience illustrates the lively debates which China's influence on domestic Chinese-language media can arouse. It also reveals the many factors that can cause resistance to Chinese "soft power" influence in its many forms. Africa's experience illustrates China's ability to invest in local media partnerships and to broadcast Chinese state media content across a continent embracing more than 50 countries.

First, a summary of what I see as the challenges facing local and foreign journalists in China:

When it comes to the challenges facing foreign reporters, the Foreign Correspondents Club of China's "Working Conditions Report" for 2016 says it all:

"The reporting environment for foreign journalists in proving hostile for yet another year in China—a situation that correspondents judge to be distant from basic international standards. Intimidation of sources and local staff, growing harassment and obstruction are major challenges for journalists conducting their work.

"The annual Working Conditions survey …finds an alarming new form of harassment against reporters, some of whom have been called into…meetings with the State Security Bureau. The survey also finds an increase in the use of force and manhandling by authorities against journalists performing their work.

"Vast areas of the country remain inaccessible to foreign reporters. Those who took part in government-sponsored trips to Tibet…expressed mixed satisfaction about the degree of access obtained. It is still largely impossible for foreign journalists to report from Tibet, Tibetan areas or Xinjiang without incurring serious interference."

The good news is that several foreign reporters whose visas were denied have now been able return to China and once again begin reporting there. A notable example is Chris Buckley of *The New York Times*, a fluent Chinese speaker who has spent many years reporting from China. He was forced to leave the country in 2012 after *The Times* reported on the wealth accumulated by the family of former Premier Wen Jiabao.

Expulsions of foreign reporters have been relatively rare in recent years. No reporter whom I know of has been expelled since Ursula Gautier, a French reporter for the *L'Obs*, was forced to leave in 2015.

This was the first expulsion since 2012, when Melissa Chan of Al Jazeera's English Service was forced out, apparently for reporting on China's hidden black jails, or detention centers, and on land grabs by provincial Chinese officials.

Difficult though conditions might be for foreign reporters, conditions for Chinese reporters have been even more challenging in recent years. When I reported from China for five and half years in the 1980s and again for several months in 1995, my colleagues and I knew that the worst that could happen to us was to be expelled, and a few colleagues were expelled.

But Chinese reporters could be jailed, and several were. As recently as 2015, Zhang Miao of the German weekly *Die Zeit* went to prison for nine months. She had accompanied a reporter for *Die Zeit* on a visit to Hong Kong so that she could help cover the pro-demoracy protests occurring there. When she returned, Ms. Zhang shared some photos of Hong Kong demonstrations on the social media service WeChat.

Since China's president, Xi Jinping, took power in 2012, several Chinese journalists who have offended the state or the CCP have been forced to engage in televised confessions regarding their alleged wrongdoing.

Chinese investigative reporting, the most difficult kind of reporting to pursue in China, has been in decline for a number of years, with many top reporters dropping out.

As David Bandurski of the China Media Project (CMP) in Hong Kong explained in a post on April 25, "Over the past few years, it has been increasingly clear that much of the experience that the journalism profession in China has gained since the 1990s is being hollowed out by deeper economic, political, and technical shifts in the media industry."

Many factors, from poor pay to the digital transformation of the industry and the vagaries of

censorship, have driven the exodus of experienced reporters from China's media, according to Bandurski.

A 2016 PR Newswire showed that more than 80 percent of the "front-line journalists" reporting the news in China were 30 years old or younger.

Following the disappearance of Malaysia Airlines Flight 370 in March 2014, many internet users were appalled by the inability of Chinese journalists to get valuable scoops such as those reported by CNN, *The New York Times* and *The Wall Street Journal*, says Bandurski.

He cites columnist Sun Letao who noted evidence of some young journalists' inexperience when covering a National People's Congress meeting at the time. "What audiences witnessed were great numbers of young reporters, looking like they had just stepped out of college…stopping representatives to ask the same stereotyped questions, and writing the same stereotyped reports." Some were pulling aside delegates to pose with them for selfies—not a sign or professional behavior.

By "stereotyped reports" Sun apparently meant, "safe reports" lacking in new or challenging insights and reports that would not offend the censors.

Since 2014, the Chinese media have remained "virtually silent on major stores, says Bandurski. Only the Tianjin explosions of August 2015 have offered "a truly notable exception to the lull in quality reporting by China's domestic media," he says.

"The explosions were a story of such immense scale, unfolding in a highly populated urban area,that coverage was impossible to quell entirely."

All of the reasons cited in a recent WeChat article on journalism becoming a profession dominated by the young and inexperienced "might be resolved if the industry was permitted to develop a sense of professional purpose," says Bandurski.

He cites President Xi Jinping speech on media policy of February 2016, in which Xi stressed that the media must "sing the main theme and transmit positive energy."

Positive stories are the order of the day for the Chinese media at home and abroad as China stresses positive stories and "soft power" image-building.

Given the restrictions faced by the Chinese media, it's no wonder that some prominent Chinese journalists have simply dropped out or gone into business. Following a golden era of investigative reporting in the 1990s, one of the most famous among them, Wang Keqin, began devoting himself to philanthropic efforts on the part of the Chinese coal miners who suffered injuries but received little compensation in the end for their injuries. In some cases, they received no retirement pay or experienced long delays before they could receive it.

One thing that the Party still has difficulty blocking is videos provided by citizen reporters from all over China, whose work reaches the outside world. Foreign reporters can use these videos as tips for stories. The videos sometimes provide information regarding issues on China's taboo list, such as popular protests against provincial officials who grab farmland without providing villages with adequate compensation. The videos are particularly helpful when they come from restricted regions such as Tibet and Xinjiang.

But the citizen journalists who send these videos to the outside world risk imprisonment for doing so. In April 2016, a Tibetan blogger was jailed for sharing "sensitive news" and a video showing police beating people in the streets. In December of last year, a Tibetan monk was sentenced for sharing "information and images."

Finally, I should stress that the Chinese assistants who work for foreign reporters often come under pressure and run the greatest personal risks in pursuing sensitive stories.

News assistants conduct research, translate materials, and arrange interviews. As Yaqiu Wang, correspondent for the Committee to Protect Journalists explained in late 2015, "their role is a precarious one, and they must straddle the expectations of their employers and the pressures of China's security apparatus. They are on occasion invited for intimidating "chats," or tea, and questioned about their employers, and their sources. In some cases, the security police have been known to go to the assistants' families in an attempt to pressure them.

But as a former correspondent for Agence France-Presse told the Asia Society, "Most foreign bureaus would be nothing without their Chinese news assistants."

China's global media influence

Working with a budget many times larger than that which the United States devotes to international broadcasting, China has expanded and transformed its overseas operations with the aim of improving China's image while downplaying outright propaganda.

All of this fits in with China's larger aim of expanding its "soft power" alongside its growing economic and military power.

China is spending billions to improve its image across the world, but the results so far are mixed. The reach of Beijing's overseas media is impressive and should not be underestimated. And, as Shanthi Kalathil has noted, with the help of world-class international journalists, China's CCTV has developed the capability of producing "sophisticated long-form reports on complex international issues such as climate change."

At the same time it might be a mistake to regard such state-media developments as simply part of a Juggernaut, or irresistible force.

While some efforts to diversify and create more engaging websites, such as the new "Sixth

Tone" appear to be smart moves, many people in many countries are still quick to detect hidden propaganda when they see it.

A fairly recent flawed move by China's main overseas television outlet, until recently known as China Central Television, or CCTV, shows how things can go wrong. In December 2016,

Beijng rebranded its main overseas television outlet, until recently known as China Central Television, or CCTV. But the rebranding, or makeover, has several shortcomings, according to media experts.

In an apparent effort to show that it has modernized and gone global, the network needed to stop using the acronym CCTV, which might remind some people of surveillance cameras. So the network came up with a new name: China Global News, or CGN TV.

One problem arose at the outset. CGN is difficult to remember, and it sounds vaguely like CNN.

David Bandurski, the widely respected editor of the China Media Project at Hong Kong University, describes CGN's new website as unattractive and "ill conceived."

In contrast, Beijing's smartest media move over the past year or two might have been the creation of *Sixth Tone*, an English-language site spin-off from *The Paper* in Shanghai.

Sixth Tone is edited by Colum Murphy, an experienced former *Wall Street Journal* business reporter, who is described by one of his former colleagues as "a very capable editor."

While subject to censorship, Sixth Tone enjoys a bit more freedom than most Chinese state media, because it's in English.

Foreign Policy magazine said after *Sixth Tone's* kick-off a little more than a year ago in April, 2016, that if the U.S. media start-up Vox were acquired by the Chinese Communist Party, "it might resemble *Sixth Tone*."

Reasons for focusing on China's Media Influence Africa and Australia

When it came to China's global influence, I decided to focus on Africa, partly because, CCTV, now known as CGN TV and the official Chinese news agency Xinhua have established good relations with governments as well as media partnerships with African media across the continent. This seems partly due to Chinese efforts to present African developments in a favorable light while countering what some African governments regard as mostly negative news reports carried by Western media.

While CGN and Xinhua have made heavy investments in Africa and have secured a number of media partnerships, few quantitative studies are available to precisely measure China's impact in

Africa. And the impact obviously varies from county to country. In a continent with a total of more than 50 nations, research in one of them might not apply to the others. But looking at it from Beijing's point of view, China can boast of some media success stories in Africa.

Meanwhile, a number of African academics and human rights advocates say that China's media links and African government connections are encouraging some African leaders to feel that they can control, harass, and repress African journalists with impunity.

I chose to focus on China's media influence on Chinese-language media in Australia, partly because that influence has been extensive. But I also think Australia is worth looking at because of its alliance with the United States. China has been trying, unsuccessfully and not so subtly so far, to win Australia's support or at least its neutrality regarding China's expansionist activities in the South China Sea. Some say that China might be trying to drive a wedge between Australia and the United States. Australians have been debating every aspect of China's involvement in Australia from Confucius institutes, donations by local Chinese to political parties and universities, and even the smallest matters, such as lift-outs, or inserts, of *The China Daily* in Australian newspapers.

The Australian example is also interesting because similar debates over growing Chinese media influence have also taken place in Canada and the United States. But nowhere, it seems, is there more debate and talk of it than in Australia.

Here are my findings regarding Chinese media influence in Africa and Australia:

China and Africa

China's media outreach in Africa has been part of a worldwide effort aimed at breaking what Beijing regards as a "monopoly" over international media discourse.

This was laid out clearly in late 2013 by the then Chinese ambassador to Kenya, Liu Guangyuan, when he stated at a seminar in Nairobi that Chinese and African media "…must break the monopoly of the current international discourse." (See JHU's 2016 Policy Brief No. 12)

Ambassador Liu described this alleged monopoly as part of a Western "conspiracy." But it's not clear how many Africans believe that Western media narratives are part of a conspiracy.

The ambassador's comments have to be placed in the context of a multi-billion dollar effort that began nearly a decade ago when then President Hu Jintao gave priority to "soft power" at a Communist Party Congress. Once he took power in 2012, President Xi Jinping gave even more attention to making soft power a part of his vision of a rejuvenated China regaining national greatness. Under Xi, this also involves countering Western concepts, such as "universal values," which is now on China's media taboo list.

Africa is the continent where China's efforts to promote its values through media and counter Western narratives appear to be most visible. These efforts include a major expansion of Chinese state media offices and broadcasts throughout the continent; training for African journalists; and perhaps of most long-range significance, Chinese partnerships with and investments in African media organizations.

According to a research report conducted or sponsored by the China Africa Research Initiative at the Johns Hopkins University School of Advanced International Studies (SAIS-CARI), Chinese media outlets are now present across Africa. Among foreign media outlets, Xinhua bureaus "in many cases" have become a primary source of news alongside Western news agencies such as Agence France-Presse, the Associated Press, and Reuters.

The English-language *China Daily* has an office in Kenya and can be obtained for free in several African countries.

China has been training African journalists, some of whom have been offered scholarships. China has also invited African journalists to cover special events in China and to take expenses-paid tours of the country.

In a report prepared with support from SAIS-CARI, researcher Jakup Emil Hansen says that while "the Chinese do not appear to be directly or overtly attempting to influence journalists through their training programs, it is clear that courses are intended to indirectly influence participants by promoting China's view of media's role in society." But he concludes that the extent to which they've succeeded isn't clear.

One area in which the Chinese media might be succeeding is in broadcasting Chinese language lessons. According to Kenneth King, a scholar and author of a book on "China's Aid and Soft Power in Africa," starting in 2008 China Radio International (CRI) began broadcasting short lessons in Chinese. This, King says, is one of the resources that played a part in "encouraging young people to become interested in China and in studying Chinese."

Most significantly perhaps, China has also made gains through media investments and partnerships.
One example of a Chinese media partnership stands out. In early 2015, two South African billionaire entrepreneurs launched the African News Agency (ANA), with the aim of carrying more positive stories than Western news agencies provide. Those stories would portray Africa as a continent of hope and opportunity.

ANA said that it would be using China's Xinhua News Agency for international news as well as photos along with other partners, such as Germany's Deutsche Presse Agentur (DPA).

In South Africa, China now has a 20 percent stake in one of the country's largest media entities, the Independent Newspaper Group, which launched ANA in 2015. As an online report said at the

time, the 20 percent will go to a new entity to be incorporated in tax haven Mauritius called Interacom Investment Holdings. Its shareholders are China International Television Corporation (CITVC) and the China Africa Development Fund (CADF). The ruling African National Congress (ANC) supported the Chinese investment. Some journalists feared that China would now be able to exert undue influence over the English language newspapers in one of Africa's most robust media environments. (See correspondent Geoffrey York of the Toronto *Globe and Mail* for extensive reporting from Johannesburg on Interacom and its shareholders.)

South Africa has Africa's most developed economy, but it has been mired in corruption scandals, which contributes to doubts about the ANC's relations with China.

According to Corruption Watch, the South African chapter of Transparency International, South Africa has consistently ranked among those countries perceived to have a "serious corruption" problem.

Although South Africa's dealings with China may lack full transparency, the country is also the site of ongoing debates over what China's growing influence might mean for press freedom.

Emeka Umejei, a doctoral candidate at the University of Witwaterstrand University in Johannesburg, says that "China's media expansion in Africa has elicited widespread debate among scholars and practitioners on its impact on journalism and democracy on the African continent."

Umejei notes that China media organizations based in Africa make sure that content provided by their African employees doesn't offend Chinese interests on the continent. Story ideas proposed by African journalists have to be approved or rejected by Beijing.

A story on China's controversial activities in the South China Sea is likely to quote high-ranking Chinese officials but fail to quote Southeast Asian officials who protest those activities.

Mohamed Keita, the former advocacy coordinator in Africa for the U.S.-based Committee to Protect Journalists (CPJ) says that China's influence in African affairs has been "very toxic for democracy."

Anne Nelson, an author, lecturer, and international media consultant, warned in a report four years ago on CCTV's international expansion that "China's integrated approach to media investment could provide it with a high level of control. African leaders are assured that they can practice censorship with impunity."

But aside from any Chinese influence, African journalists have long faced difficult challenges in doing their work in a number of African countries.

The CPJ has documented numerous cases of African journalists who have been harassed,

intimidated, jailed, and even killed by repressive governments and their police forces while trying to carry out their media work.

In the CPJ's 2016 prison census, Egypt, Eritrea, and Ethiopia respectively were among the top countries jailing journalists, after Turkey and China. Eritrea is the most censored country in the world, according to the CPJ, with Ethiopia coming in number 4.

The repression of African journalists is a story in itself that could use more coverage but it's not likely to be covered by the Chinese media.

In the meantime, international media organizations with foreign correspondents based in Africa have been cutting back.

It's worth noting, however, that U.S.-funded Voice of America has a strong media presence in Africa alongside the BBC, Al Jazeera, Deutsche Welle, and Radio France International. VOA claims to be reaching more than 60 million people a week online, on shortwave radio, and through television and radio partners across the continent in English, French, Portuguese, and 10 African languages and dialects.

Zimbabwe takes Western broadcasting seriously enough to use radio jamming equipment provided by China in order to block shortwave broadcasts from the VOA, the BBC, Deutsche Welle, and an exile Zimbabwean group based in London. Ethiopia apparently did the same at one point.

VOA has focused heavily on reaching young Africans through radio, television, and social media. Young people, who account for nearly 70 percent of the population, are the most vulnerable to violent extremism.

According to Anna Quintal, Africa program coordinator for the CPJ, while some international media organizations have indeed cut back, local African correspondents, or stringers, have been filling gaps by providing content to foreign news organizations.

Meanwhile, Quintal says, vibrant online media, including Quartz Africa and some African media groups, have online subsidiaries that go beyond a tendency of some African media to focus only on their own countries and not invest in covering other countries on the continent.

New York-based Quartz launched its second international mobile-first design website in Africa in 2015. Its first international launch was in India. Quartz calculated that the high penetration of mobile devices in Africa would allow it to reach a growing population of African entrepreneurs and innovators. Quartz focuses on technology and business news in contrast with more crisis-driven media.

"So the idea that China is helping to feed the void left by Western media who no longer maintain

a network of foreign correspondents in Africa is a bit superficial," says Quintal.

But the staffing cutbacks by some Western media organizations hardly fits with the idea promoted by China—and some Africans—that the West is involved in a conspiracy to perpetuate a monopoly over Africa-related information flows.

China and Australia

Australia would appear to be a country where China would have a good chance of winning hearts and minds, partly through China's strong trade ties with Australia but also through Beijing's media connections there.

But a debate not always favorable to China is underway in Australia at the moment over what is seen by some as Chinese government attempts to promote pro-Beijing views through the country's Chinese-language media and through a local Chinese "patriotic association."

Australia's debate over Chinese influence is worth examining, partly because it shows how Chinese media influence can backfire. It also shows how unforeseen events, such as China's recent detention for more than a week of a Chinese permanent resident of Australia, tend to undermine China's efforts to win potential friends in Australia.

More broadly, signs of China's media influence among Chinese residents are raising questions in Australia over China's "soft power" and whether it is to be feared.

Australian journalists at *The Sydney Morning Herald* have reported on possible Chinese influence on a "patriotic association" called the "Australian Action Committee for Peace and Justice."

The committee, which purports to represent Australia's Chinese community, drew attention a little more than a year ago when it urged the country's "political elite" to avoid criticism of China's controversial claim to most of the South China Sea.

The committee called on Australia's leadership take care when discussing sensitive issues in April of 2016 just as Malcolm Turnbull prepared to make his first trip to China as Australia 's prime minister.

Australia's debate has been partly fueled by a political scandal that erupted in September of last year. Senator Sam Dastyari of the opposition Labor Party resigned on Sept. 7 after acknowledging that he'd received funds from Chinese companies to pay off debt and a legal fee. After having supported the U.S. position on the South China Sea, Dastyari later stated that Australia should take a neutral position on China's claims to most of the sea. Prime Minister Turnbell said that Dastyari's change of position on the issue was a case of receiving "cash for comment."

Dastyari had accepted funds from the Yuhu Group, a property development company headed by Huang Xiangmo, a wealthy Chinese businessman known to be a supporter of China. Huang has contributed funds over the years to both of Australia's major political parties.

Huang was the founding donor of the Australia-China Relations Institute (ACRI) at the University of Technology in Sydney, self described as a think tank whose work is "based on a positive and optimistic view of Australia-China relations."

Huang resigned as the head of ACRI in September 2016, saying that he didn't want "unfair" publicity about his political donations to distract from the "good work" that Institute was doing. Some Australian scholars have called ACRI a "propaganda vehicle" for Beijing.

Chinese Media in Australia

On July 10, 2016, *The Sydney Morning Herald* reported that Beijing had gained control over "messaging and propaganda" appearing in nearly all of the Chinese-language newspapers published in Australia. "Politically sensitive or unfavorable coverage of China and the ruling Communist Party has been effectively stopped outside all but a couple of Chinese language outfits…," said reporters Kelsey Munro and Philip Wen. In addition, they said, the Chinese government had stepped up efforts to filter what Chinese readers in Australia saw online through social media and through WeChat, a popular mobile phone application developed by China's Tencent Inc. which censors sensitive subjects.

Wanning Sun, a professor of media and communication at University of Technology, Sydney, published a 62-page paper last year for ACRI titled "Chinese-Language Media in Australia," which takes a less alarming view of Chinese media influence.

Despite the criticism of ACRI's apparent pro-China leanings, Professor Sun makes some interesting points.

She notes that the Chinese-language media had shifted over the past decade or so from a focus on Cantonese speakers to a focus mainly on a Mandarin-speaking migrant community from the People's Republic of China.

At the same time, Chinese state media's "going global" initiatives have dovetailed with the business acumen of elite Chinese migrants…," Sun says.

"As a result, migrant Chinese media—and for that matter—mainstream Australian media… have been willing to lend their platforms as carriers of China's state media," she says.

"Also, for business reasons, she adds," some Chinese media may from time to time engage in a certain degree of self censorship."

And finally, she says, Chinese-language media have shifted from representations of China that were once mostly critical to representations that are "sympathetic or even supportive."

But Sun argues that the view that much of the Chinese-language media "has now been 'bought off,' 'taken over,' or is owned or directly controlled by China's propaganda authorities is simplistic..."

There is, however, she says, "clear evidence that Chinese propaganda has moved offshore from the mainland and become to some extent integrated with Chinese media in Australia. But this does not necessarily mean that such 'localized' propaganda has a direct impact on Chinese-speaking audiences."

Sun says that better-educated Chinese migrants get their news from a wide range of sources; that the circulation of Chinese newspapers in Australia is "relatively small;" and that they can easily get Chinese propaganda content directly from mainland Chinese media.

The real problem, she says, is that many PRC residents in Australia "mostly side with China if there is a potential clash between the two nations on matters of national pride, sovereignty, and territoriality," presumably a reference to disputes over Taiwan as well as China's activities in the South China Sea.

Driving a Wedge

In his 2007 book "Charm Offensive; How China's Soft Power is Transforming the World," Joshua Kurlantzick wrote that China might drive a wedge between America and its closest allies. He singled out Australia as an example.

Ten years later, China doesn't appear to have succeeded in driving that wedge, but at times statements emanating from China make it seem to be trying to do so. And some such statements aren't taken well by many Australians.

In 2016, China's *Global Times* newspaper, which is part of China's Communist Party mouthpiece, *The People's Daily*, blasted Australia for urging China to abide by an international tribunal in the Hague that disputed China's claims to most of the South China Sea.

Euan Graham, director of the international security program at Australia's prestigious Lowy Institute, said that threats of revenge against Australia and harsh and insulting language used by the *Global Times* amounted to "bullying." In an opinion piece written for *The Australian* newspaper, Graham added that whatever the *Global Time's* intention, "its crassly phrased effort at intimidation should awaken more Australians to China's growing chauvinism and the strategic risks it poses."

China seems to have managed to have alarmed much of Australia's defense and security

establishment. *Time* magazine correspondent Charlie Campbell in Beijing reported on March 29 that "Australia's wariness is partly prompted by China's ham-fisted attempts of gaining domestic political leverage."

In 2013, Campbell says, Chinese hackers stole the blueprints for the Australian Security Intelligence Organization's (ASIO) new $480 million headquarters.

According to Campbell, "the Dastyari case prompted Australian intelligence services to map the flow of Chinese money and businessmen into Australia, augmenting demands for an end to donations to political parties."

There are also calls to ban China-funded Confucius Institutes from Australian universities. Australian critics say that the institutes promote Beijing's political agenda.

So it's clear that despite China's influence among Chinese-language media in Australia, a number of elements make it difficult for China to influence Australia as much as it would like, much less drive a wedge between Australia and its U.S. ally.

Australian attitudes are affected, for example, by Chinese purchases, or "buy-ups," of high-cost housing in the Sydney area. Rich Chinese are seen as driving the costs even higher.
The possible impact of Chinese money going to Australian politicians is obviously another concern.

But interestingly, Huang Xiangmo, sometimes described as China's point man in Australia or the "Reigning Emperor of the Chinese Community," has said that he doesn't think he's getting his money's worth.

In an interview last September with Australia's *Financial Review,* Huang said that he'd received no benefit from his donations and contacts with Australian politicians. He acknowledged paying Senator Sam Dastyari's legal bills but denied getting any benefit from it.

The *Financial Review* cited an editorial written by Huang for *The Global Times that* suggested that the Chinese community would demand "a greater say in Australian public life after being used as a 'cash cow' by both sides of politics, then ignored."

Helen Clark is an Australian journalist and former foreign correspondent who reports on Asia-Australia relations and writes on China and Australia for varied publications.

Clark says that when viewing Chinese influence in Australia or a lack thereof one must take into account much more than expanding Chinese-language media influence.

She concludes that "despite the strong economic relationship, China is unlikely to be able to mount a front-on charm offensive in Aussie media aimed at the general populace as there

remains too much fear and mistrust.”

OPENING STATEMENT OF SHANTHI KALATHIL, DIRECTOR, INTERNATIONAL FORUM FOR DEMOCRATIC STUDIES, NATIONAL ENDOWMENT FOR DEMOCRACY

MS. KALATHIL: Thank you. Chairman Bartholomew, Commissioner Wortzel, distinguished members of the Commission, thank you for inviting me to testify before the Commission on the topic of China's global media influence.

I appreciate the opportunity to discuss China's efforts and impact in this area. I would also like to thank you for drawing attention to this issue of strategic importance to the U.S. and other democracies.

China has long included the cultivation of global influence as part of its overall strategy to position itself as a rising, though non-threatening, global power. In recent years, this has evolved beyond standard propaganda to reflect a much broader understanding of how command of media and communication constitutes power in the modern age.

China, like other authoritarian states, understands that the information space is an area of contestation in which democracies are increasingly vulnerable and that it is in shaping the related norms, standards, and corporate platforms where the long-term opportunities for influence lie.

As a result, China is targeting not simply media-related products but the mechanisms that determine which products are produced in the first place. This sets it apart from other authoritarian governments in no small part due to China's unique market leverage.

Here I'll briefly touch on three media and communication-related mechanisms through which China seeks to exert influence: shaping international news; guiding the evolution of the global Internet; and influencing global culture through Hollywood. It's important to consider them together for they indicate that China has mobilized information resources on a massive scale to project power and maximize desired outcomes.

First, let me address China's influence on the international news environment. This occurs through pressuring reporters and news organizations reporting on China, extending its presence abroad through international broadcasting, publication and social media; and influencing the structure and values of news organizations, primarily in developing countries, through funding, training and cooperation.

Just to give one example of this, China has supported the media and communication sectors of countries in Latin America, Central and Eastern Europe, and particularly Africa, providing financial resources, infrastructure, equipment, study tours in China, and training. But, unlike most donors, China doesn't support the typical goals of this kind of assistance, which include freedom of expression, editorial independence, developing professional capacity.

Rather, the Chinese government is helping to develop China-friendly media sectors around the world that will de-emphasize accountability, portray China as a reliable partner, and support China's foreign policy positions and objectives.

With respect to the global Internet, the Chinese government seeks to shape the institutions that govern the Internet; the norms, standards and protocols conditioning its use; and the corporations powering its platforms.

For instance, as we've heard already today, China has championed the idea of Internet sovereignty, essentially national borders on the Internet and a state-based regulatory approach,

preferably involving the ITU. This would be a stark departure from the current multi-stakeholder approach and would give authoritarian countries much more latitude to censor, surveil and impede the free flow of information worldwide.

But even without traction on this, China can affect the way the Internet develops--the global Internet--at numerous other levels. For instance, Chinese Internet companies are now big enough to go global, and indeed they are, but their corporate policies on digital rights are not encouraging, and the Ranking Digital Rights' 2017 Corporate Accountability Index, which is led by Rebecca MacKinnon, who you mentioned earlier, ranked two Chinese companies among the worst global performers on issues of governance, freedom of expression, and privacy.

It is in the new domain of the so-called "Internet of Things," or the proposed data connectivity of everyday objects, where China's policies on surveillance, security and privacy take on added relevance. China is proposing to become a world market leader in producing IoT-enabled devices, as outlined in its "Internet Plus" initiative.

This is usually framed as a Chinese domestic manufacturing and innovation issue, but there are clear implications for the global information ecosystem. For instance, any Chinese-led IoT would be informed by a government attitude toward consumer and personal privacy that is largely out of step with global democratic norms on these issues. Consider the proposed "social credit" system for Chinese citizens that we heard about today, predicated on collecting personal data.

China's domestic innovation policies, global information ambitions, and attitudes toward surveillance, privacy and expression are thus likely to intersect--largely at an unseen level--in a way that directly affects how communication evolves for the foreseeable future.

Finally, I'll briefly mention the issue of the Chinese government's influence in Hollywood, a subject that has seen considerably more influence over the last year. Due to quotas in the domestic market, and the fact that all films released in China are subject to censorship guidelines on politically and socially sensitive content, U.S. studios are incentivized to favorably alter depictions of China, especially with respect to big-budget tentpole films that rely on success in the Chinese market.

In the past, this was done in post-production specifically for the Chinese market. But now it occurs from the conceptualization stage onward so that the final product released to all markets is tailored to suit Chinese censors' sensibilities. Essentially, the Chinese government has used the carrot of its domestic market to get otherwise independent actors to help, quote, "tell China's story to the world," to use a favorite phrase of Xi Jinping and other Chinese leaders.

Many of these trends may be subject to fluctuations as domestic Chinese policy emphases change. For instance, measures to control the pace and nature of foreign acquisitions have already affected proposed entertainment deals. Yet a few key points are likely to remain salient over the long term.

First, the Chinese government's broad conception of communications-driven influence encompasses sectors outside of what is typically conceptualized as "media." It also includes technology, entertainment, innovation policy, domestic manufacturing, and international norms and diplomacy, in addition to the cyber realm, which we'll hear about in the third panel this afternoon.

Perhaps most importantly, the Chinese government has found that leveraging market

power can have ideological benefits. Rather than focusing exclusively on official propaganda, the CCP has found that it may be easier to simply buy up assets, encourage them to be bought by sympathetic entrepreneurs, or induce self-censorship. If the government can stay one step removed, yet still accomplish its goals, all the better.

It may seem that democracies, whose very openness can make them vulnerable, have little recourse in the rapidly evolving information environment. Perhaps the first most important response by democracies would be to directly acknowledge the rising and fundamental threats to democratic institutions around the world.

It is important to support cross-regional information sharing by civil society around understanding and countering authoritarian influence. Support for independent, credible and financially sustainable media is crucial, as well as the development of deeper expertise in the frameworks and arguments that authoritarian regimes use to advance their own communication agendas.

Civil society would also benefit from efforts by democracies to ensure that China is not able to unilaterally restrict non-government exchanges or access markets in the U.S. and other democracies for the purposes of exerting influence without any scrutiny as to the negative effects of such efforts.

Putting Chinese media and technology companies in comparative international perspective on digital rights-related policies would also help generate international pressure for increased transparency. All these efforts would be reinforced by the active, coordinated participation of democracies in international forums to support fundamental democratic values.

Ultimately, the Chinese government's natural impulse is still to cover up rather than to open up. It sees transparency and democratic decision-making as an element of brittleness rather than resilience. So it is worthwhile to keep in mind that as long as democracies hew to--and actively defend--their core strengths and values, they will always possess this natural soft power advantage that authoritarian countries will be unable to match.

Thank you.

PREPARED STATEMENT OF SHANTHI KALATHIL, DIRECTOR, INTERNATIONAL FORUM FOR DEMOCRATIC STUDIES, NATIONAL ENDOWMENT FOR DEMOCRACY

Hearing on "Information Controls, Global Media Influence, and Cyber Warfare Strategy"

Testimony before
The U.S.-China Economic and Security Review Commission

May 04, 2017

Chairman Bartholomew, Commissioner Wortzel, distinguished members of the Commission: thank you for inviting me to testify before the Commission on the topic of "China's Global Media Influence." I appreciate the opportunity to discuss China's efforts and impact in this area. I would also like to thank you for drawing attention to this issue of strategic importance to the U.S. and other democracies.

China has long included the cultivation of global influence as part of its overall strategy to position itself as a rising, though nonthreatening, global power. Championed by a succession of Chinese leaders, this "soft power" focus has traditionally included media components such as pro-government reporting by Chinese state-run broadcasters and the cultivation of friendly overseas news outlets.

In more recent years, though, the Chinese government's strategy has evolved beyond these standard elements to reflect a much broader understanding of how command of media and communication constitutes power in the modern age. China, like other authoritarian states, grasps that the information space is an arena of contestation in which democracies are increasingly vulnerable. Moreover, China in particular understands that it is in shaping the related norms, standards, and corporate platforms in which the long-term opportunities for influence lie.

Hence, China is also seeking to build out the infrastructure of the evolving global information ecosystem itself, targeting not simply media-related products but the mechanisms that determine what kinds of products are produced in the first place. This sets it apart from other authoritarian governments, in no small part due to China's unique market leverage.

Here, I'd like to present a broad, synthesized overview of China's efforts to harness this evolving global information ecosystem. This overview will touch primarily on three media and communication-related mechanisms through which China seeks to exert influence: shaping international news; guiding the evolution of the Internet and its norms; and influencing global culture through Hollywood.[1] Seen individually, any distinct piece might be glossed over as a discrete, isolated activity. Yet, taken together, they are indicative of an authoritarian government

[1] This analysis draws in part from Shanthi Kalathil, "Beyond the Great Firewall: How China Became a Global Information Power," Center for International Media Assistance, 2017.

that has mobilized global information resources on a massive scale to project power, maximize its desired outcomes and protect its own rule.

International News: Content, Values, and Funding

China has attempted to influence international news in three ways: influencing foreign reporting on China, extending its presence abroad through its international broadcasting and publication arms; and influencing the structure and values of news organizations, primarily in developing countries, through funding, training and cooperation.

While the Chinese government has always monitored foreign reporters operating within China, this practice has expanded and grown more aggressive under current president Xi Jinping, who has instituted a wide and long-lasting crackdown on domestic civil society and media. Recent reports assert that foreign journalists in China now face greater restrictions than at any other time in recent history.[2] The CCP seeks to influence international reporting through a combination of direct action, economic pressure to induce self-censorship by international media owners, indirect pressure applied via proxies such as advertisers, and cyberattacks and physical assaults.[3] Increasingly, these levers are applied beyond China's own borders.

This combination has had a cumulative chilling effect on the diversity of perspectives on China available in the international media. This is particularly true of Chinese language media. In some countries, such as Australia, local analysts report that the formerly lively, independent Chinese language media space now hews largely to the pro-China line, in part because pro-China media groups now control much of the Chinese language media sector.[4] In supposedly autonomous Hong Kong, the local media has developed increasingly close ties to the Chinese government and friendly entrepreneurs; for instance, in 2015 the South China Morning Post was bought by Jack Ma, founder of AliBaba Group, China's largest e-commerce conglomerate, and press watchdogs have raised concerns about that paper's continuing editorial independence.[5]

With respect to international broadcasting and publication, the Chinese government is focused on amplifying China's voice in the global media landscape, a landscape currently undergoing a seismic shift brought on by changes in access, technology, and business models. This period of flux has presented certain opportunities for China's state-run and state-affiliated media, which do not suffer from the same budget pressures as their private sector international competitors. The international arm of China Central Television was rebranded China Global Television Network (CGTN) at the end of 2016, with all new foreign language channels, digital and video content falling under the new group. CGTN has hired away respected journalists from other outlets, and in general enjoys more editorial leeway than its domestic counterpart does (while never reporting on genuinely sensitive topics).

---

[2] *Darkened Screen: Constraints on Foreign Journalists in China*, PEN America, Sept. 22, 2016.
[3] Sarah Cook, "The Long Shadow of Chinese Censorship: How the Communist Party's Media Restrictions Affect News Outlets Around the World," Center for International Media Assistance, 2013.
[4] Paul Monk, "China's propaganda infiltrating our shores," *The Sydney Morning Herald*, July 10, 2014.
[5] Tom Phillips, "Mysterious confession fuels fears of Beijing's influence on Hong Kong's top newspaper," *The Guardian*, July 25, 2016.

Even before this recent rebranding, CGTN had significantly expanded its broadcasting footprint, opening major global offices in Washington, D.C. and Nairobi, and pouring financial resources into international news bureaus during a time when other major media outlets worldwide were forced to scale back their international coverage due to declining budgets. It is important to note that while CGTN may lack presence and authority in the U.S., it is increasingly viewed in many countries as simply another credible outlet that adds to the plurality of voices.

New ventures may look more like overseas-targeted, English-language publication *Sixth Tone*, which is backed by state-owned Shanghai United Media Group, the same company that publishes the relatively lively domestic paper *Pengpai*. *Sixth Tone* features compelling human interest and trend stories with a local focus, skirting close to charged social and political issues without crossing the line into highly politically sensitive territory. Indeed, the tone, structure and social media adeptness of *Sixth Tone* may indicate the future of at least some Chinese state-affiliated media. (*Foreign Policy* magazine has described *Sixth Ton*e as if "Vox were acquired by the Chinese Communist Party."[6]) As scholars of Chinese soft power note, Chinese media executives are well aware that market-driven, audience-savvy products can be far more effective in swaying perception than state-owned organs issuing stiff proclamations, and are more in line with what young, global digital natives desire.

Finally, China has been involved in supporting the media and communication sectors of many countries in Latin America, Central and Eastern Europe, and Africa.[7] It has done so through providing financial resources, infrastructure and equipment, study tours in China, and training. Unlike most international independent media donors, though, China does not support the typical normative goals of this kind of assistance: freedom of expression, editorial independence, technologically neutral protocols, and developing the professional and investigatory capacity of local journalists.

Rather, the Chinese government's primary purpose in providing this type of assistance is to counter what Chinese officials see as the unfavorable narrative about China in Western media, by developing a China-friendly media sector that will both portray China as a reliable partner and support China's foreign policy positions and objectives. Moreover, the model of journalism presented in training and study tours emphasizes a cooperative approach that de-emphasizes the accountability aspect of journalism. Ugandan participants in Chinese media training and study tours, for instance, have said that classroom lectures did not focus on practical skills, emphasizing instead China's history and politics, as well as the importance of the China-Africa relationship.[8]

The Global Internet: Norms, Standards, and the Future

---

[6] Bethany Allen-Ebrahimian, "China, Explained," *Foreign Policy*, June 3, 2016.
[7] See, for instance, Douglas Farah and Andy Mosher, "Winds From the East: How the People's Republic of China Seeks to Influence the Media in Africa, Latin America, and Southeast Asia," Center for International Media Assistance, 2010.
[8] Jakup Emil Hansen, "Media Training for Africa: Is China Exporting its Journalism?" *China-Africa Research Initiative Policy Brief No. 12*, 2016.

China has long engaged in domestic censorship and shaping of the Internet, utilizing a variety of techniques ranging from co-optation of the private sector to multilayered levels of technological and public opinion management. What has been less well understood is the extent to which the Chinese government has turned its attention outward, seeking an instrumental role in developing not only the current iteration of the global Internet, but future versions as well. Here, the CCP is directing its attention to the institutions that govern the Internet; the norms, standards and protocols conditioning its use; and the corporations powering its platforms. Once again, China is in the unique position of using its market power, including its protected domestic Internet industries, to influence the future of the global communications landscape.

At the broad level of advocating for global norms and governance, China has championed its conception of "Internet sovereignty," which promotes the idea of distinct national borders on the Internet and a state-based regulatory approach, preferably involving the International Telecommunication Union (ITU). While the U.S. and other democracies have typically supported the multistakeholder model of governance because it involves a bottom-up and decentralized process that incorporates civil society, government, and the private sector, China has advocated for a multilateral process because it inherently privileges the role of states.

This approach finds some supporters within developing countries (including democracies) who lack capacity to influence the multistakeholder process and thus are drawn to a state-based model of governance. However, a multilateral model would be a stark departure from the way the Internet is currently governed, and would give authoritarian countries much more latitude to censor, surveil, and impede the free flow of information worldwide. Moreover, the Internet sovereignty framework would also allow the Chinese and other authoritarian governments to justify internal crackdowns on dissent and political activity within the broad rubric of cybersecurity.

Even if China does not succeed at normalizing the concept of Internet sovereignty, it can practically affect the way the Internet develops at numerous other levels. Because China has effectively excluded foreign competition from its domestic Internet sector, its homegrown Internet companies are now large enough to be testing international waters. China now leads the world in e-commerce, accounting for 40 percent of global sales, and by some estimates has four of the top 10 Internet companies in the world by market capitalization.[9] Those Internet companies are being encouraged to go global, as part of China's broader emphasis (within the 13th Five-Year Plan and elsewhere) on supporting its Internet-based industries.

As these companies spread overseas and diversify, they may bring features of the Chinese Internet with them. For instance, WeChat, a Chinese messaging service, is now expanding beyond China; its centralized China-based servers are subject to Chinese law and regulations on surveillance and censorship.[10] While it is unlikely that Chinese Internet companies have

[9] Simon Denyer, "China's scary lesson to the world: Censoring the Internet works," *The Washington Post,* May 23, 2016.
[10] Lotus Ruan, Jeffrey Knockel, and Masashi Crete-Nishihata, "We (can't) Chat: "709 Crackdown" Discussions Blocked on Weibo and WeChat," Citizen Lab, April 13, 2017. https://citizenlab.org/2017/04/we-cant-chat-709-crackdown-discussions-blocked-on-weibo-and-wechat/

inherently malicious intent toward their potential global customers, they understand that state and corporate interests are intertwined, and that the government is free to impose fines and revoke operating licenses at will. Emerging signs regarding the rights-related corporate policies of Chinese Internet firms are not encouraging: Ranking Digital Rights' 2017 Corporate Accountability Index ranked two Chinese companies, Baidu and Tencent (which operates WeChat), as among the worst performers on issues of governance, freedom of expression and privacy, out of 22 of the world's most powerful telecommunications, Internet and mobile companies.[11]

It is in the new domain of the so-called "Internet of things (IoT)," or the proposed data connectivity of everyday objects, where China's policies on surveillance, security, and privacy take on added relevance. As the Internet Society points out, "IoT amplifies concerns about the potential for increased surveillance and tracking, difficulty in being able to opt out of certain data collection, and the strength of aggregating IoT data streams to paint detailed digital portraits of users."[12] Not coincidentally, China is also proposing to become a world market leader in producing IoT-enabled devices. The "Internet Plus" initiative outlined in the 13th Five Year plan heavily emphasizes government-prioritized domestic innovation in this area in a bid to enhance the value-added component of Chinese manufacturing, as well as to help set standards for the global market in IoT-enabled devices. The incentives are clear: according to the Economist, embracing IoT-enabled manufacturing could add up to $736 billion to China's GDP over the next fifteen or so years.[13]

While production of data-enabled devices is frequently framed as a Chinese domestic manufacturing and innovation issue, there are clear implications for the global information ecosystem. For instance, any Chinese-led IoT would be informed by a government attitude toward consumer and personal privacy that is largely out of step with global democratic norms on such issues; this attitude is embodied most strikingly in the government's widely publicized plan to aggregate personal data to create a "social credit" system for Chinese citizens. China's domestic innovation policies, global information ambitions and attitudes toward surveillance, privacy and expression are thus likely to intersect – largely at an unseen level – in a way that directly affects how communication evolves for the foreseeable future.

Hollywood: The Big Chill

Past discussions of China's soft power emphasized the transmission of Chinese culture to the outside world. This priority – part of "telling China's story to the world," in the words of Xi Jinping and other leaders – is manifested in numerous ways, including the expansion of Confucius Institutes in U.S. universities and the cultivation of think tank and media experts in countries across Eastern Europe, Latin America and Africa. In the past few years, however, China has made its presence felt in global culture most strongly through another avenue: Hollywood. The Chinese government has leveraged the increasing importance of the Chinese

[11] Ranking Digital Rights Corporate Accountability Index, https://rankingdigitalrights.org/index2017
[12] Karen Rose, Scott Eldridge, Lyman Chapin, "The Internet of Things: An Overview," Internet Society, October 2015, p. 6.
[13] "The Great Convergence," *The Economist,* July 21, 2016.

filmgoing audience to U.S.-based entertainment companies, encouraging self-censorship by major studios who wish to gain a foothold in the limited domestic release market. Essentially, the Chinese government has realized a powerful truth: that through Hollywood, in a form of market-based judo, it can use the soft power strength of the United States for its own purposes.

Currently, U.S. film studios can access the Chinese market in three ways: through revenue-sharing films, flat-fee movies, and co-productions with a Chinese company. While the first two categories are subject to a restrictive quota system to be re-negotiated in 2017, co-productions do not count as foreign films, and allow foreign studios to receive a greater percentage of total box office receipts. All films, of course, are subject to approval by the State Administration of Press, Publication, Radio, Film and Television, which reports directly to the State Council and enforces censorship guidelines on politically and socially sensitive content. On top of official regulations, unofficial measures designed to boost domestic films can also negatively affect foreign films' reception within China.

This limited potential for domestic Chinese release creates an incentive system for U.S. entertainment companies that encourages maximum cooperation with the Chinese censorship apparatus, to ensure widespread, favorably timed release within China. It has also accelerated the formation of joint ventures and other tie-ups, as well as talent acquisition, between Chinese and U.S. entertainment conglomerates, particularly within the last few years. In particular, it has encouraged U.S. studios to alter depictions of China, especially with respect to big-budget tentpole films that rely on success in Chinese and other overseas markets to be profitable. Generally, studios alter content to please China in four key ways, listed here from least obtrusive to most: Chinese product placement; casting decisions (including Chinese stars to qualify as co-productions); excising sensitive material (in, as in one example, taking out references to destruction of the Great Wall); and proactively including positive story elements featuring China (such as favorably depicting Chinese achievements in science and technology).

Whereas a few years ago only a handful of films per year might feature one or more of these elements, now it is almost a truism that blockbusters destined for global rollout will do so; they include productions or co-productions from many major U.S. studios. Moreover, in the past, these types of content alterations were made in post-production specifically for the Chinese market. Now, they take place from the conceptualization stage onward, such that the final product released to all markets is tailored to suit Chinese censors' sensibilities. Essentially, the Chinese government has used the carrot of its domestic market to get otherwise independent actors to "tell China's story to the world." This has also led to a global chilling of expression with respect to China, leading some media scholars to characterize China as the "world film police."[14]

A Long-Term Influence Strategy, and Potential Democratic Responses

It should be noted that many of these trends are still evolving, and may be subject to fluctuations as domestic Chinese policy emphases change. For instance, while Chinese outbound investment

[14] Frank Langfitt, "How China's Censors Influence Hollywood," NPR, May 18, 2015.

reached record levels in 2016, Chinese authorities have recently become more concerned over capital outflows and excess corporate diversification, and have introduced measures to control the pace and nature of foreign acquisitions, which have already affected proposed entertainment acquisitions such as Dalian Wanda's $1 billion bid for Dick Clark Productions.[15]

This, in addition to a recent Chinese box office slowdown (and a lukewarm global reception for widely touted co-production *The Great Wall*), has served to temper enthusiasm for U.S.-Chinese entertainment tie-ups. The difficulties experienced by Chinese technology and entertainment company LeEco in the U.S. have also demonstrated that conquering the global market will not necessarily be easy for Chinese firms.[16] As more and more Chinese companies compete globally, there may be increasing tension between the demands of the market and Beijing's ideological directives.

That said, an overview of these issues surfaces a few key points that are likely to remain salient over the long term. First, the Chinese government's broad conception of communications-driven influence encompasses sectors outside of what is typically conceptualized as "media." It also includes, inter alia, technology, entertainment, innovation policy, domestic manufacturing, and international diplomacy (in addition to the military "cyber" realm, which is covered in another panel today). In essence, China's unitary approach increasingly targets the information ecosystem at its source: the entertainment powerhouses that shape global culture, the media that informs international opinion or policy, and the norms, standards, technological and corporate platforms powering the Internet and its future.

Perhaps most importantly, the Chinese government has found that leveraging market power can have ideological benefits. Rather than focusing exclusively on official propaganda, which is growing more sophisticated but remains out-of-step, the CCP has found that it may be easier to simply buy up assets (or encourage them to be bought by sympathetic entrepreneurs). The Chinese government has learned important lessons about soft power: that credibility, authenticity, and the identity of the messenger matter. If the government can stay one step removed yet still accomplish its goals, even better. As the global media landscape continues to evolve and traditional values of editorial independence give way to blurred lines between advertising, opinion and news, greater openings for influence may emerge. Certainly, China is watching with interest the successful efforts by Russia and others to tactically exploit opportunities for disseminating disinformation.

It may seem that democracies, whose very openness can make them vulnerable, have little recourse in the rapidly evolving, chaotic and poorly comprehended information environment. Perhaps the first, most important, response by democracies is simply to directly acknowledge the rising and fundamental threats to democratic institutions around the world. With democratic reversals and so-called democratic deconsolidation underway in a number of established democracies, it could be argued that democracies have finally become aware of the dangers to

---

[15] *Economics and Trade Bulletin*, U.S.-China Economic and Security Review Commission, April 4, 2017.
[16] Christina Warren, "'It's All Over Now But The Screaming': Inside The Unraveling of LeEco in America," *Gizmodo*, April 18, 2017.

established liberal norms, as well as of the information-savvy efforts by authoritarian regimes to subvert core democratic values.

Yet more comprehensive and sustained understanding is still sorely needed. In this regard, it is important to support researchers, activists, journalists and others who are seeking to shine a light on the Chinese government's influence activities in their various forms around the world – especially in environments where deep or technical knowledge about such activities is lacking. In particular, civil society efforts across the globe would benefit from better cross-regional information sharing, and more coordinated awareness-raising efforts, around understanding and countering authoritarian influence. In this complex information environment, support for independent, credible and financially sustainable media is crucial, as well as the development of deeper expertise in the frameworks and arguments authoritarian regimes use to advance their own media agendas (such as the assertion that authoritarian state-owned media only seek to broaden media pluralism).

Civil society would also benefit from efforts by democracies to ensure that China is not able to unilaterally enact laws and regulations that directly restrict non-governmental exchanges, or access markets in the U.S. and other democracies for the purposes of exerting influence, without any scrutiny as to the negative effects of such efforts. Because the Chinese strategy is multifaceted and likely to rely increasingly on Chinese companies, continuing to put these companies in comparative international perspective on digital rights-related policies would help generate international pressure for increased transparency. These efforts would be complemented if U.S. media, technology and entertainment companies spoke with one voice to the Chinese government and Chinese companies on issues relating to freedom of expression, privacy, and other key matters. The entire spectrum of activity on these fronts would also be reinforced by the active, coordinated participation of democracies in international forums on issues ranging from Internet governance to market access to fundamental democratic values.

Ultimately, China cannot singlehandedly decide to accrue soft power; its inherent "attractiveness" is still generated organically by its culture, businesses, system of government, and most importantly, its people. Ironically, the Chinese government suppresses this potentially vital source of its soft power: the unbounded, uncensored opinions of its citizens, participating freely in national conversations about their future. [17] The Chinese government's natural impulse is still to cover up rather than open up; it sees transparency and democratic decision-making as an element of brittleness rather than resilience. It is worthwhile to keep in mind that as long as democracies hew to – and actively defend – their core strengths and values, they will always possess this natural soft power advantage that authoritarian countries will be unable to match.

[17] Shanthi Kalathil, "China's Soft Power in the Information Age: Think Again," *ISD Working Papers in New Diplomacy*, Institute for the Study of Diplomacy, Georgetown University, May 2011.

OPENING STATEMENT OF SARAH COOK, SENIOR RESEARCH ANALYST FOR EAST ASIA, FREEDOM HOUSE

MS. COOK: Thank you for the opportunity to address the Commission again, this time on China's influence over the media landscape here in the United States.

The Chinese Communist Party has long sought to influence media coverage of China here in the U.S. But over the past decade, these efforts have expanded and intensified. They're increasingly targeting English media alongside their Chinese counterparts. As a result, the "China factor" is palpably present, be it at the Wall Street Journal, a cable TV provider here in Washington, or a Chinese radio talk show in Los Angeles.

After briefly addressing the goals of CCP media influence campaigns in the United States, I will focus my remarks on recent trends and their impact, and then brief recommendations.

So what are the goals? CCP influence campaigns mostly target two audiences--overseas Chinese and non-Chinese foreigners--with three primary aims:

First, to promote a positive view of China and the CCP regime; second, to encourage U.S.-China investment; and third, to suppress voices that present the Chinese government negatively.

The Party's obstructions have traditionally prioritized a certain set of topics: Tibetans, Uighurs, Falun Gong, democracy activists, and proponents of Taiwanese independence.

But now we're seeing the mechanisms being applied to new topics. Since 2012, Chinese authorities have obstructed or punished major U.S. outlets for coverage of the Chinese economy, looking into the assets of top leaders' families, or portraying Xi Jinping in an unfavorable light.

Recent trends. The CCP uses various strategies--from direct action to economic "carrots and sticks"--to promote state propaganda and suppress criticism of the regime.

As current Chinese President Xi Jinping has tightened ideological controls at home, according to scholar Anne-Marie Brady, "China's foreign propaganda efforts have taken on a new level of assertiveness, confidence, and ambition."

Chen Pokong, a democracy advocate in New York and an observer of Chinese media here in the U.S., has also noticed Chinese government influence increasing. He reports that China's diplomats in the United States are more arrogant and, quote, "more actively interfering" in the editorial decisions of American Chinese media, including potentially a recent incident at Voice of America.

These attempts to influence U.S. media are evolving in three ways:

One, expansion of previous tactics. State-run media outlets like China Daily and CCTV continue to expand in the U.S. Radio stations in 15 U.S. cities are broadcasting content provided by Chinese state-run media. By contrast, since June 2014, the English and/or Chinese websites of the Wall Street Journal, Reuters, and Time magazine have all been blocked in China.

In December, Apple removed The New York Times application from its store in China. This was the first known instance of the firm censoring a major U.S. outlet rather than a Chinese dissident one.

In another first, in January, a particularly polemic negative article appeared in Chinese paid supplements in the Washington Post and Wall Street Journal. It targeted the New York-

based Shen Yun Performing Arts Company and Falun Gong, practiced by many of its performers, thereby bringing hate speech against a minority persecuted in China here to the United States.

Two, adaptation to changing technology. A new cyber attack tool researchers have called the "Great Cannon" emerged in March 2015. It hit a U.S.-based website, which, among other pages accessible in China, hosted a copy of The New York Times's blocked Chinese website.

Meanwhile, pro-government Internet trolls, often referred to as the "50 Cent Party," have begun verbally abusing U.S.-based commentators critical of the government.

Three, fine-tuning media expansion tactics. In December 2016, the Party-State rebranded CCTV America as CGTN. More significantly, Anne-Marie Brady notes that, "foreign propaganda activities are also increasingly conducted as business transactions." And that there may be an attempt to shift from what the Chinese call "borrowing the boat" via supplements like China Watch to "buying the boat" by acquiring all or part of U.S.-based media or cultural enterprises.

The impact and limits of Beijing's influence. The Chinese Party-State invests billions of dollars a year in foreign propaganda and media censorship. So how effective are these tactics in the United States?

The answer is mixed. There are three ways in which the CCP's efforts have been effective:

One, establishing dominance over Chinese- language media in the United States, especially television. Based on August 2016 data, CCTV News is available in 90 million cable-viewing households in the United States. Now this figure far exceeds the four to five million Chinese Americans, but it indicates that Chinese-speaking households almost anywhere in the U.S. can watch CCTV.

The next most widely available stations are the Hong Kong-based pro-Beijing Phoenix TV and a pro-China Taiwanese station, each reaching over 70 million households.

By contrast, a pro-independence Taiwanese station is available in just 12 million households, and the New York-based New Tang Dynasty TV, founded by Falun Gong practitioners and known for its reporting on human rights, is available in about six million households.

This imbalance does not appear to be accidental. In a January 2017 submission to the FCC, NTDTV notes that some U.S. cable companies will not meet their representatives. And in 2009, Chinese embassy officials threatened an RCN cable executive who was arranging with NTDTV for the channel to be aired in Washington, D.C.

An estimated 78 percent of Chinese American homes speak a language other than English, rendering CCTV's television dominance especially significant.

Two, provoking self-censorship and editorial shifts. In 2013, Bloomberg executives reportedly killed an investigative story after suffering reprisals over a 2012 piece about Xi Jinping's family wealth.

A 2016 PEN America report found that Chinese government pressure has also led to new vetting of human rights stories at Reuters, with the result that, quote, "the story gets softened," end quote, spiked or published with a delay.

Imposing financial difficulties on disfavored media. In October 2012, within 24 hours of

China blocking The New York Times English and new Chinese websites, the entire media company's stock fell by 20 percent within 24 hours. The incident and related advertising difficulties highlight how censorship in China can negatively impact the financial viability of a major U.S. paper.

Manipulated competition for advertising also exists among Chinese media. The above-mentioned imbalance in stations' access to cable viewers renders CCTV more attractive to advertisers than its competitors critical of the CCP. Because of consular pressure, many businesses in the Chinese community are more inclined to advertise in pro-Beijing papers than with outlets critical of the Chinese government.

And some good news. There are clear limits to Beijing's influence. Media outlets in the United States daily publish news the CCP wants hidden. Targeted outlets still disseminate their content to millions in China and the U.S. And in the relatively competitive online market, compared to cable TV, Alexa's website rankings reveal that NTDTV's Chinese website significantly outranks CCTV within the U.S. in terms of popularity.

Moreover, recent public opinion poll surveys indicate that more Americans have an overall unfavorable view of China today compared to ten years ago, including over China's human rights policies.

Many English-speaking Americans are not attracted to or convinced by Chinese government propaganda, particularly when its state-run origins are known. CGTN America's accounts on YouTube and Facebook show very few viewers, paling in comparison to major U.S. networks. Similarly, despite the China Watch insert calling for a boycott of Shen Yun, many of its performances throughout the United States were sold out.

Still, the current and potential future impact of the CCP's tactics should not be underestimated, be it in terms of press freedom, economics, or national security.

As the U.S. government seeks an effective response, it is critical that policymakers uphold democratic principles like free expression rather than constraining access to certain sources of information.

Thus, Freedom House recommends focusing on enforcing existing legislation, taking action against diplomats who pressure journalists or advertisers, increasing transparency about media ownership, and trying to level the playing field between U.S. outlets and Chinese state-supported competitors.

My written testimony includes more details on the recommendations, and I'm also happy to expand on them in the questions and answers. Thank you.

PREPARED STATEMENT OF SARAH COOK, SENIOR RESEARCH ANALYST FOR EAST ASIA, FREEDOM HOUSE

Asia Hearing on "Information Controls, Global Media Influence, and Cyber Warfare Strategy"

Testimony before
The U.S.-China Economic and Security Review Commission

May 04, 2017

Introduction

Reuters establishes a new round of internal vetting on stories about human rights in China after its English and Chinese websites are blocked.[1] Radio stations in fifteen U.S. cities broadcast content provided by Chinese state-run media.[2] Tech giant Apple removes the *New York Times'* mobile-phone applications from its download store in China with little explanation.[3] And several rounds of crippling cyberattacks hit the New York-based servers of *New Tang Dynasty Television* and *The Epoch Times* newspaper's websites.[4]

These are a small sample of incidents that have occurred over the past three years. Collectively, they illustrate various ways in which Chinese Communist Party (CCP) information controls—in terms of both censorship and propaganda—extend beyond mainland China's borders and influence the media landscape in the United States.

This testimony summarizes and supplements a 2013 study I authored of this phenomenon globally—*The Long Shadow of Chinese Censorship*,[5] while attempting to offer updates on its recent evolution as it pertains to the American news media sector.

The CCP and various Chinese government entities, have long sought to influence public debate and media coverage about China in the United States, particularly among Chinese language communities. However, over the past decade, these efforts have expanded and intensified.

---

[1] PEN America, *Darkened Screen: Constraints on Foreign Journalists in China*, September 22, 2016, https://pen.org/sites/default/files/PEN_foreign_journalists_report_FINAL_online%5B1%5D.pdf
[2] Koh Gui Qing and John Shiffman, "Beijing's covert radio network airs China-friendly news across Washington, and the world," Reuters, November 2, 2015, http://www.reuters.com/investigates/special-report/china-radio/.
[3] Katie Benner and Sui-Lee Wee, "Apple Removes New York Times Apps From Its Stores in China," January 4, 2017, https://www.nytimes.com/2017/01/04/business/media/new-york-times-apps-apple-china.html.
[4] Larry Ong, "Epoch Times Inundated with Cyberattacks Believed to be from China," *The Epoch Times*, March 1, 2017, http://www.theepochtimes.com/n3/2229427-epoch-times-inundated-with-cyberattacks-believed-to-be-from-china.
[5] Sarah Cook, *The Long Shadow of Chinese Censorship: How the Communist Party's Media Restrictions Affect News Outlets Around the World*, October 22, 2013, The Center for International Media Assistance, National Endowment for Democracy, http://www.cima.ned.org/wp-content/uploads/2015/02/CIMA-China_Sarah%20Cook.pdf.

Moreover, they are increasingly targeting English-language media companies and news consumers alongside their Chinese-speaking counterparts. As a result, the "China Factor" is palpably present, be it at the internationally renowned *Wall Street Journal,* a cable TV provider in Washington DC, or a Chinese radio talk show in Los Angeles.

I have divided this testimony into five parts and ask that this full written testimony be admitted into the record:

I. Goals of CCP media influence campaigns in the United States

Similar to CCP outreach and propaganda efforts in other parts of the world, influence campaigns in the United States target two primary audiences: overseas Chinese and non-Chinese foreigners. In both cases, the narratives and actions encompassed by these initiatives reveal three primary aims[6]:

1) To promote a positive view of China and benign perspective of the CCP's authoritarian regime
2) To encourage foreign investment in China and openness to Chinese investment abroad
3) To marginalize, demonize, or entirely suppress anti-CCP voices, incisive political commentary, and exposés that present the Chinese government and its leaders in a negative light.

For overseas Chinese, two additional goals of promoting nationalistic sentiment vis-à-vis China and reunification with Taiwan are evident in programming and news coverage as well.[7] Some Chinese-language state-media content can also be quite anti-American, particularly in how it frames key events in U.S.-China relations.[8]

Research by scholars like Anne-Marie Brady[9] and James To[10] provide detailed examples and analysis of these narratives and their application to various target audiences outside China. In

[6] James Jiann Hua To, *Qiaowu: Extra-Territorial Policies for the Overseas Chinese* (Brill Academic Publishers: 2014); Anne-Marie Brady, "China's Foreign Propaganda Machine," *Journal of Democracy,* Vol. 26(4), October 2015: 51-59.
[7] James To, *Qiaowu.*
[8] Interview with Chen Pokong, April 24, 2017.
[9] Anne-Marie Brady, *Making the Foreign Serve China: Managing Foreigners in the People's Republic* (Rowman & Littlefield: 2016).
[10] James To, *Qiaowu.*

considering the close intersection between the CCP's overseas propaganda and censorship efforts, Ashley Esarey, a scholar of Chinese media, noted in his own 2011 testimony before this commission:

> The objective of CCP leaders is to utilize propaganda to retain high levels of popular support domestically and to improve the regime's international influence. When propaganda messages are disconnected from actions that speak otherwise or challenged by rival perspectives, the effectiveness of propaganda falters and sows doubt among both foreigners and Chinese alike.[11]

Esarey's observation helps make sense of why the party's recent multi-billion dollar effort to expand the reach of state-run media has been coupled with increased instances of extraterritorial censorship. For the party's narrative to be convincing to audiences inside and outside China, reporting—especially investigative reporting and critical commentary—about the darker sides of CCP rule at home and Chinese activities abroad must be suppressed.

In seeking to accomplish this aim, the party's transnational obstructions appear to prioritize a set of targets that one former Chinese diplomat said were internally called "the five poisonous groups."[12] These are Tibetans, Uighurs, practitioners of the Falun Gong spiritual group, Chinese democracy activists, and proponents of Taiwanese independence.[13] In many instances, these groups and related causes have been explicitly mentioned as the focus of direct or self-motivated censorship, or of vilifying propaganda, highlighting the special importance the CCP attributes to

---

[11] Ashley Esarey, "Testimony before the U.S.-China Economic and Security Review Commission Hearing on 'China's Narratives regarding National Security Policy," March 10, 2011, https://www.uscc.gov/sites/default/files/3.10.11Esarey.pdf.

[12] Statement of Mr. Yonglin Chen, First Secretary and Consul for Political Affairs, Former Chinese Consulate, Sydney, Australia, Appendix 2, "Falun Gong and China's Continuing War on Human Rights," Joint Hearing Before the Subcommittee on Africa, Global Human Rights and International Operations and the Subcommittee on Oversight and Investigations of the House Committee on International Relations, 109th Cong. 49–50, July 21, 2005, http://www.gpo.gov/fdsys/pkg/CHRG-109hhrg22579/pdf/CHRG-109hhrg22579.pdf.

[13] These groups and related topics combine perceived threats to both CCP rule and China's territorial integrity, as well as past and present human rights violations whose widespread discussion in China could severely damage the party's legitimacy. Sensitivities regarding Tibet and Xinjiang typically involve challenges to official narratives about the regions' history, advocacy of their independence, independent investigations of recent unrest, and sympathetic coverage of leading figures like the Dalai Lama or Rebiya Kadeer. The party's hostility towards Falun Gong, a spiritual and meditation practice that became popular during the 1990s, dates to 1999 when then CCP head Jiang Zemin and other hardliners viewed its informal nationwide network and spiritual worldview as a threat to party rule and launched a campaign to eradicate it. Since then, sympathetic portrayals of the practice, independent investigations of human rights abuses, and Falun Gong practitioners' nonviolent activism have become among the most censored topics in China. The CCP also remains highly sensitive to discussion of the 1989 Beijing Massacre, in which the military opened fire on unarmed prodemocracy demonstrators, killing between several hundred and several thousand. Movement leaders from the period who continued their activism in exile remain sensitive figures, while new generations of activists and commentators periodically run afoul of party censors, particularly when they proactively challenge one-party rule or advocate for a democratic system in China. Lastly, the Chinese government's position is that Taiwan is a province of China despite its de facto features of sovereignty. Recognition of Taiwan as an independent state internationally or calls for independence by Taiwanese politicians typically draws a strong response. The CCP often conditions foreign aid and other cooperation on counterparts' affirmation of a "One China" position.

them. The transnational activism of Tibetans and Falun Gong practitioners—including the latter's efforts to build their own U.S.-based media entities free of CCP controls—render them even more frequent targets of restrictions. These issues touch on some of the most egregious and systematic abuses taking place in China today,[14] pointing to the CCP's nervousness of regime violence being exposed.

But the mechanisms used to marginalize discussion of these subjects are now also being applied to new topics deemed politically sensitive. Since 2012, the Chinese authorities have meted out multi-faceted reprisals and obstructions against American news outlets for investigative reports detailing the assets of party leaders' relatives, critical coverage of the Chinese economy, or unfavorable reporting about Xi Jinping.[15] Foreign correspondents' attempts to report on issues such as human rights lawyers' trials, land disputes, and environmental pollution have also encountered interference and in some cases, physical attacks. These topics collectively affect the lives of tens of millions of people in China and may have global implications.

II. Propaganda and censorship tactics: two sides of the same coin

The CCP uses a variety of strategies in its efforts to achieve its goals of influencing media narratives in the United States in the directions described above. These typically take the form of propaganda tactics that actively promote Chinese government content and pro-Beijing media outlets or censorial ones that suppress information and obstruct media outlets critical of the regime.

Propaganda efforts have taken three primary forms:

1) **Aggressive attempts to expand state-run media outlets' reach and influence inside the United States.** These efforts have included high-profile initiatives like Xinhua news agency's advertisement in Time Square,[16] the appearance of *China Daily* newspaper boxes on streets in major U.S. cities, and the launch of China Central Television (CCTV) America—recently rebranded as China Global Television Network (CGTN) America.[17] In the Chinese-language media sphere, this effort has been going on for over 20 years, resulting in CCTV being accessible to over 90 million households in the United States[18] and a series of free pro-Beijing newspapers displacing the earlier dominance of Taiwan and Hong Kong-affiliated papers.[19]

---

[14] Sarah Cook, *The Battle for China's Spirit: Religious Revival, Repression, and Resistance under Xi Jinping*, Freedom House, February 2017, https://freedomhouse.org/sites/default/files/FH_ChinasSprit2016_FULL_FINAL_140pages_compressed.pdf.
[15] PEN America, *Darkened Screen.*
[16] Stuart Elliott, "Sign of Arrival, for Xinhua, is 60 Feet Tall," *New York Times*, July 25, 2011, http://www.nytimes.com/2011/07/26/business/media/xinhuas-giant-sign-to-blink-on-in-times-square.html.
[17] "China's state broadcaster CCTV rebrands international networks as CGTN in global push," Associated Press, December 31, 2016, http://www.scmp.com/news/china/policies-politics/article/2058429/chinas-state-broadcaster-cctv-rebrands-international.
[18] This sum was calculated from data in a network carriage report provided by SNL Kagan, August 2016. Detailed data on file with the author.
[19] James To, *Qiawu.*

2) **Insinuating state-media content into mainstream media or other existing dissemination channels.** Chinese officials and state-media reports have referred to this strategy as "borrowing the boat to reach the sea" (借船出海).[20] This phrase refers to disseminating Chinese state-media content via the pages, frequencies, or screen-time of privately owned media outlets that have developed their own local audiences. This strategy has a long history of use in the Chinese-language environment, such as via the provision of Xinhua newswire content for free.[21] In recent years, its robust expansion to English-language media has garnered much attention and public debate. One of the most prominent examples has been the emergence of China Watch—a paid insert sponsored by the state-run *China Daily*—that has appeared both in print and online in prominent U.S. papers like the *New York Times*, *Washington Post*, and *Wall Street Journal*. In November 2015, a Reuters investigation revealed that programming from the state-funded China Radio International (CRI) was appearing on stations in 15 U.S. cities, including Washington DC, via intermediaries of a privately owned media group.[22]

3) **Co-opting or partnering with privately owned media to produce and publish content that serves Beijing's aims:** Not all pro-CCP propaganda appearing in U.S. media necessarily originates from writers and editors at Chinese-state run media outlets. Rather, Chinese diplomats and other officials have gone to great lengths to develop "friendly" relations with private media owners and reporters, encouraging them to produce their own content that promotes key narratives favored by Beijing. Outlets and diaspora media owners whose reporting portrays Beijing positively are frequently rewarded with advertising, lucrative contracts for non-media enterprises, joint ventures, and even political appointments. In several instances, Chinese state-media have also purchased small financial stakes in overseas media to solidify such a relationship. Examples of these dynamics are evident in two media entities whose content is disseminated in many parts of the United States. First, the above-mentioned Reuters investigation revealed that only part of the content aired on radio stations owned or leased by CRI's U.S.-based partner G&E Studio originates from CRI. Other segments are produced by G&E Studio itself in California.[23] Nevertheless, their messaging matches that of Chinese state propaganda. A second example is that of Phoenix TV, the second most widely available Chinese-language television station on cable in the United States.[24] Owned by a former military officer with close ties to Beijing officials, Phoenix TV's coverage is typically

[20] For example, one official report in 2013 noted that "in 2012 the Xi'an Newspaper Media Group and the municipal publicity department collaborated with Los Angeles-based *America Commercial News* to create a special report about Xi'an as part of Xi'an Newspaper Media Group's 'highly effective' boat borrowing strategy." http://news.gmw.cn/newspaper/2013-06/27/content_1664012.htm (accessed August 2013)
[21] James To, *Qiaowu.*
[22] Koh Gui Qing and John Shiffman, "Beijing's covert radio network.".
[23] Reuters, "Covert radio network."
[24] See page 9 of this testimony and footnote 55 for data that served the basis for this assertion.

favorable to the CCP.[25] Moreover, over the past two years, it has been used as an outlet for airing televised confessions by various detained CCP critics, most notably all five Hong Kong booksellers abducted by Chinese security forces in late 2015.[26] Such coverage is perhaps not coincidental, considering that CCTV reportedly holds a 10 percent stake in Phoenix.[27]

Censorship and other attempts to suppress the spread of information deemed undesirable by the regime have taken a variety of other, often more subtle forms. The above-mentioned 2013 study described these dynamics in detail, finding that they manifest in four key ways both in the United States and other parts of the world:

- **Direct action** by Chinese diplomats, local officials, security forces, and regulators both inside and outside China. These measures obstruct newsgathering, prevent the publication of undesirable content, and punish overseas media outlets that fail to heed restrictions.
- **Economic "carrots" and "sticks"** to induce self-censorship among media owners and their outlets headquartered outside mainland China.
- **Indirect pressure** applied via proxies—including advertisers, satellite firms, and foreign governments—who take action to prevent or punish the publication of content critical of Beijing.
- Incidents such as **cyberattacks** and **physical assaults** that are not conclusively traceable to the central Chinese authorities but serve the party's aims and result from an atmosphere of impunity for those attacking independent media.

In practice, different tactics are adopted for varied media and information environments. For **international media**, local officials and unidentified thugs in China obstruct foreign correspondents, the Ministry of Foreign Affairs delays visa renewals, and central authorities arbitrarily block websites. Outside China, diplomats have been known to apply pressure on senior editors and executives to alter coverage, while cyberattacks have infiltrated the global servers of leading outlets such as the *New York Times* and the *Wall Street Journal*.[28]

The CCP's efforts to expand control over Chinese-language media based outside the mainland are more systematic, reflecting how the party's domestic political concerns often drive foreign policy

---

[25] Philip Pan, "Making Waves, Carefully, on the Air in China," *Washington Post*, September 19, 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/09/18/AR2005091801597_4.html.
[26] All of the broadcasts occurred during February 2016. Guo Minhai: http://news.ifeng.com/a/20160228/47620482_0.shtml; Liu Bo: http://news.ifeng.com/a/20160228/47620482_0.shtml; Lam Wing-kee: http://news.ifeng.com/a/20160228/47620482_0.shtml; Cheung Jiping: http://news.ifeng.com/a/20160228/47620482_0.shtml; Lee Bo: Karen Cheung and Tom Grundy, "Detained bookseller Lee Bo says he will 'give up' UK residency in Chinese TV 'interview,' *Hong Kong Free Press*, February 29, 2016, https://www.hongkongfp.com/2016/02/29/breaking-detained-bookseller-lee-bo-says-he-will-give-up-uk-citizenship-in-chinese-tv-interview/.
[27] Philip Pan, "Making Waves."
[28] See the International Media chapter in *The Long Shadow of Chinese Censorship* for details and references.

priorities.

Co-opting owners of media outlets in **Hong Kong, Taiwan**, and the **Chinese diaspora—**whose subsidiary publications and broadcasts are disseminated in the United States—has been a successful strategy for advancing CCP efforts to marginalize dissenting reporting and commentary. When positive incentives have failed to reach their objectives, more heavy-handed approaches have been used, such as Chinese officials' calling editors directly to castigate them for their coverage. For individual journalists, fear of an inability to return to China or of reprisals against family members in the mainland encourage cautious writing and compliance with consular demands here in the United States.[29]

More forceful measures have been taken to obstruct the operations of independent-minded **offshore Chinese media**. These include several initiatives based in the United States, like the California-based *China Digital Times* website, the citizen journalism site *Boxun*, and the Epoch Media Group headquartered in New York, which includes *New Tang Dynasty Television (NTDTV), The Epoch Times/Dajiyuan* newspaper, and *Sound of Hope* radio. Particular efforts have been made to undermine these entities' financial viability and block mainland audiences' access to their content. They have suffered advertising boycotts, debilitating cyberattacks, and harassment of contacts in China. In several cases, foreign companies and event organizers—including Apple and NASDAQ in the United States—have barred their access to newsworthy events outside China or assisted in Chinese government efforts to prevent their content from reaching mainland audiences.[30]

The spectrum of **Chinese government and party entitie**s involved in these attempts to promote state media propaganda and thwart reporting by foreign and overseas Chinese media is as broad as the tactics applied. Not surprisingly perhaps, many of the same bodies that supervise censorship and surveillance within China are also involved in applying media controls with transnational implications. These include the Communist Party's Central Propaganda Department at the pinnacle of the control apparatus, as well the State Council Information Office (whose office of Overseas Foreign Propaganda is central to the day-to-day efforts to influence news coverage abroad), and of course flagship CCP mouthpieces like *The People's Daily, China Daily*, Xinhua News Agency, and state broadcaster CCTV.

The Ministry of Foreign Affairs and Chinese diplomats based in the United States also feature regularly in accounts of obstructions ranging from visa denials to demands for content alterations to pressure on businesses not to advertise with a disfavored outlet. Meanwhile, the State

[29] See the "Hong Kong and Taiwan" and "Chinese Diaspora Media" chapters in *The Long Shadow of Chinese Censorship* for details.
[30] See the "Offshore Chinese Media" chapter in *The Long Shadow of Chinese Censorship* for details.

Administration of Press, Publication, Radio, Film, and Television and the Ministry of Industry and Information Technology are involved in censorship decisions in China that have ramifications for U.S.-based companies, and when interrogation is called for—the Public and State Security Bureaus.

III. Recent trends: Expansion and innovation

Some of the above dynamics date back to the 1990s. Nonetheless, **over the past decade, certain features have intensified, expanded, and deepened**. The paradoxical combination of the CCP feeling emboldened internationally and insecure domestically has contributed to this trend.

This trend began emerging during the tenure of former CCP leader Hu Jintao. Nonetheless, as current Chinese president Xi Jinping has tightened ideological controls at home and prioritized propaganda efforts abroad, content restrictions and manipulation are also affecting an ever-broadening array of institutions and economic sectors overseas.

In an October 2015 article in the *Journal of Democracy* on China's foreign propaganda efforts, media studies professor Anne-Marie Brady, who testified before this commission in 2009, found that Xi has used his highly concentrated political power to personally induce ramped up efforts to influence foreign audiences.[31] For example, in an August 2013 speech at the National Meeting on Propaganda and Thought Work, Xi stressed the need for China "to strengthen media coverage… and promote China's views internationally."[32] In a February 2016 visit to core state-media outlets, Xi also spoke to CCTV America journalists in the United States via a live video conference.[33]

A key focus of Xi's instructions regarding foreign propaganda has been to "tell a good Chinese story" in order to expand China's soft power. In a January 2014 speech, he explained to CCP Politburo members his vision for what this entails:

> China should be portrayed as a civilized country featuring a rich history, ethnic unity, and cultural diversity, and as an Eastern power with good government, a developed economy, cultural prosperity, national unity, and beautiful scenery. China should also be known as a responsible country that advocates peace and development, safeguards international fairness and justice, [and] makes a positive contribution to humanity.[34]

According to Brady, under Xi "China's foreign propaganda efforts have taken on a new level of assertiveness, confidence, and ambition."[35] Overseas Chinese observers have described

---

[31] Anne-Marie Brady, "China's Foreign Propaganda Machine."
[32] Ibid.
[33] "Chinese President Xi Jinping visits with CCTV America via video call," CGTN, February 19, 2016, https://america.cgtn.com/2016/02/19/chinese-president-xi-jinping-visits-with-cctv-america-via-video-call.
[34] Anne-Marie Brady, "China's Foreign Propaganda Machine."
[35] Anne-Marie Brady, "China's Foreign Propaganda Machine."

developments in the United States in similar terms. Chen Pokong, a democracy advocate and political analyst in New York, closely follows the Chinese language media market in the United States as he regularly publishes commentary or hosts talk shows on developments in China or U.S.-China relations across a variety of news outlets. According to Chen, in recent years, Chinese government influence in this sphere has increased rather than weakened. He attributes the changes he has noticed to Chinese diplomats in the United States "more actively interfering" in the editorial decisions of certain American Chinese media. "The diplomats don't hide their efforts or aims and are not hesitant. Rather, they are more arrogant, more aggressive," says Chen.[36]

Alongside such general observations, over the past few years, the Chinese government's evolving attempts to influence the U.S. media market have manifested in three key ways:

1) **Continued—and expanded—application of previous tactics:** The CCP and state entities continue to deploy the above-mentioned toolbox to influence and constrain media outlets in the United States. Incidents of one kind or another are reported on a regular basis. State-run media outlets like *China Daily* and CCTV have continued to expand in the United States and are increasingly hiring foreign media professionals while retaining editorial control.[37] Meanwhile, people in China are facing greater restrictions on their ability to read news published by U.S. outlets. Since June 2014, the English and/or Chinese-language websites of the *Wall Street Journal*, Reuters, and *Time* magazine have been blocked in China. The apparent triggers for the blocks include coverage of the 25th anniversary of the Tiananmen Square massacre, the jailing of a dissident who had criticized propaganda chief Liu Yunshan, and a magazine cover featuring a comparison between Xi Jinping and Mao Zedong.[38]

   Just two weeks ago, controversy emerged surrounding the unexpected interruption of a *Voice of America* interview with Chinese wanted tycoon Guo Wengui part way through a three-hour live broadcast.[39] According to media reports and to Chen Pokong, who hosts a political talk show for VOA, there were intense internal debates among staff about airing the show, reports of Chinese officials applying pressure to prevent it, and suspicion that a senior executive in the

[36] Interview with Chen Pokong, April 24, 2017.
[37] Photos from CCTV America's February 2016 video conference with Xi Jinping, for example, show relatively few Chinese among the staff. The article also notes: "Ninety percent of CCTV America's staff members are from countries other than China." CGTN, "Xi visits with CCTV America."
[38] PEN America, *Darkened Screen;* Emily Feng, "China Blocks Economist and Time Websites, Apparently over Xi Jinping Articles," *New York Times,* April 8, 2016, https://www.nytimes.com/2016/04/09/world/asia/china-blocks-economist-time.html.
[39] Robert Delaney, "Plug pulled on US interview with wanted Chinese tycoon Guo Wengui," *South China Morning Post,* April 20, 2017, http://www.scmp.com/news/china/policies-politics/article/2089000/plug-pulled-us-interview-wanted-chinese-tycoon-guo.

Mandarin service intervened to trigger the last-minute disruption. A VOA spokeswoman attributed the cut-off to miscommunication.[40]

The trend of tactics that were previously reserved for dissident Chinese-language media being expanded to mainstream U.S. outlets also appears to be continuing in disconcerting ways. Thus, in December 2016, Apple removed *The New York Times'* applications for English and Chinese content from its store accessible in China.[41] This is the first known instance of Apple doing this to a major U.S. outlet rather than an overseas Chinese dissident initiative. Second, in January 2017, a particularly negative article appeared in the China Watch supplement in the print editions of the *Washington Post* and the *Wall Street Journal*.[42] The commentary targeted the New York-based Shen Yun Performing Arts company and Falun Gong, practiced by many of its performers. The article used terms that demonize Shen Yun and Falun Gong, mimicking language in state run propaganda inside China, while encouraging readers to boycott the classical Chinese dance show scheduled to perform in New York and Washington that month. While past editions of China Watch have mostly portrayed the advantages of investing in China or occasionally taken a strongly nationalistic tone regarding the South China Sea, this is the first known case of potential hate speech against a U.S.-based Chinese dissident group, arts company, or religious minority being highlighted on its pages.[43]

In a more positive development, the use of certain tactics has been somewhat mitigated—partly due to the U.S. government consistently voicing concerns with Chinese officials. Thus, although American journalist Paul Mooney, whose visa renewal was denied in November 2013, remains outside China[44], several *New York Times* reporters have been able to return to the country or take up new posts since 2014.[45]

2) **Adaptation to changing technology environment:** As the internet and social media have increased in their importance as a source of information and media companies have explored their own tactics for overcoming websites blocked in China, the CCP's propaganda and

---

[40] "Prominent Communist Party Critic Guo Speaks with VOA China Service," VOA News, April 201, 2017, https://www.voanews.com/a/prominent-communist-party-critic-guo-speaks-with-voa-china-service/3818031.html.
[41] Katie Benner and Sui-Lee Wee, "Apple removes New York Times Apps."
[42] Leeshai Lemish, "China Daily Insert Disguised as News in WaPo, WSJ, Others," *Who's Afraid of Shen Yun? (blog)*, February 15, 2017; Larry Ong, "Paid Insert in Wall Street Journal Carries Chinese Propaganda," *The Epoch Times*, January 18, 2017. http://www.theepochtimes.com/n3/2211937-paid-insert-in-wall-street-journal-carries-chinese-propaganda/; A copy of the insert is on file with the author.
[43] Terri Marsh, "Advertising that's not worth the human cost," *Washington Post*, March 10, 2017, https://www.washingtonpost.com/opinions/advertising-thats-not-worth-the-human-cost/2017/03/09/e0652998-0352-11e7-9d14-9724d48f5666_story.html?utm_term=.e1bc1d80820e.
[44] Harrison Jacobs, "Journalist Paul Mooney on Why He Was Blocked From China And How Things Could Get 'Much, Much Worse," *Business Insider*, November 21, 2013, http://www.businessinsider.com/paul-mooney-on-being-denied-chinese-visa-2013-11.
[45] Freedom House, "China," *Freedom of the Press 2016,* April 2016, https://freedomhouse.org/report/freedom-press/2016/china.

censorship tactics have correspondingly adapted. For example, in March 2015, a U.S.-based international code-sharing site Github that also hosts websites blocked in China, was hit by a massive denial-of-service attack later traced to Chinese government servers and attributed to a new cyberattack tool researchers called the "Great Cannon."[46] Among the Github pages apparently targeted in the attack was one featuring a copy of *The New York Times* Chinese-language website.[47] In another example, the Toronto-based Citizen Lab reported in November 2016 that at least some censorship on Tencent's popular instant messaging application WeChat extends beyond China's borders.[48] Notably, users who first create accounts inside China are still subject to Chinese censorship standards like keyword filtering even after they leave the country and link their account to a new international phone number. This also affects users in the United States. WeChat is fairly popular among Chinese Americans, as evidenced by its use to organize protests in several U.S. cities in February 2016 over the conviction of a Chinese American New York City police officer for manslaughter.[49]

Lastly, pro-government internet trolls often referred to as the "50 cent party" have become more active in the overseas Chinese internet environment. Chen Pokong remarked that videos on YouTube of a popular political talk show he hosts are now frequently targeted with similarly worded comments accusing him of being a traitor or insulting his personal appearance.[50]

3) **Fine-tuning media expansion tactics:** As Chinese state media have encountered challenges gaining a foothold in the non-Chinese language market in the United States, the party-state appears to be trying to refine its approach. Some of these changes are semantic, such as rebranding CCTV America as CGTN in December 2016. Others are more operational and may include trying to better implement Xi's instructions to use multimedia content and a variety of platforms to reach target audiences.

In her article, Brady also notes that "foreign-propaganda activities are increasingly conducted as business transactions," and that there may be an attempt to shift from "borrowing the boat" to "buying the boat" by purchasing stakes in or acquiring U.S.-based media or cultural enterprises.[51] This strategy is partly evident in the failed 2010 bid by The Southern Daily Group

---

[46] Citizen Lab, "China's Great Cannon," April 10, 2015, https://citizenlab.org/2015/04/chinas-great-cannon/.
[47] Eva Dou, "U.S. Coding Website GitHub Hit with Cyberattack," *Wall Street Journal*, March 29, 2015, https://www.wsj.com/articles/u-s-coding-website-github-hit-with-cyberattack-1427638940.
[48] Citizen Lab, "One App, Two Systems: How WeChat uses one censorship policy in China and another internationally," November 30, 2016, https://citizenlab.org/2016/11/wechat-china-censorship-one-app-two-systems/.
[49] Julie Makinen, "Chinese social media platform plays a role in U.S. rallies for NYPD officer," February 24, 2016. https://www.wsj.com/articles/u-s-coding-website-github-hit-with-cyberattack-1427638940
[50] Interview with Chen Pokong, April 24, 2017.
[51] Anne-Marie Brady, "China's Foreign Propaganda Machine."

to purchase *Newsweek*[52] and in the CRI example in the Reuters investigation, where a company partly owned by a Chinese-state media outlet purchased some radio stations in addition to leasing airtime.

These adjustments match calls by Xi Jinping in his August 2013 and February 2016 speeches to propaganda cadres and state media to "use innovative outreach methods" and that "Wherever the readers are, wherever the viewers are, that is where propaganda reports must extend their tentacles."[53]

IV. **The Impact and Limits of Beijing's Influence**

As the Chinese party-state invests billions of dollars a year into its foreign propaganda and media censorship efforts, one of the most important questions that emerges is: how effective are these tactics at achieving their aims in the United States?

The answer is mixed. Some aspects of these initiatives have been remarkably effective in ways that raise serious concerns about their political and economic implications. Other elements have been much less effective, triggering some of the adjustments outlined above.

Three ways in which the CCP's efforts have evidently been effective in enhancing the prominence of state-run media outlets or narratives, while negatively impacting media freedom and access to information in the United States are:

1) **Establishing dominance over Chinese-language media—especially television:** Chinese state media or pro-Beijing private outlets are more influential today than they were twenty years ago when many Chinese Americans got their news from relatively independent papers or radio/television stations based out of Hong Kong or Taiwan.[54] The CCP's ability to influence the media consumed by Chinese Americans is especially evident from available data regarding cable television. Based on August 2016 data, CCTV News is available in 90.7 million cable-viewing households in the United States. Although this figure far exceeds the number of Chinese Americans (estimated at 4-5 million in the recent census), it does indicate that Chinese speaking households pretty much anywhere in the United States are able to watch CCTV. The next most widely available station is the Hong Kong-based pro-Beijing Phoenix TV (79.5 million households) and the pro-China Taiwanese station CTI (71.6 million households). By contrast, the pro-independence Taiwanese station ETTV is available in just

[52] Bill Bishop, "Chinese Investors Tried to Buy Newsweek," June 17, 2010, https://www.forbes.com/sites/china/2010/06/17/chinese-investors-tried-to-buy-newsweek/#45e0da492c27.
[53] David Bandurski, "How Xi Jinping Views the News," *Medium (blog)*, March 2, 2016, https://medium.com/china-media-project/how-the-president-views-the-news-2bee482e1d48.
[54] James To

12.3 million households and the New York-based New Tang Dynasty TV, founded by Falun Gong practitioners, is available in only 5.9 million households.[55] This imbalance does not appear to be accidental. In a January 2017 submission to the Federal Communications Commission, NTDTV notes that some U.S. cable companies have not even been willing to meet with their representatives. And in at least one incident in 2009, Chinese embassy officials threatened an RCN executive who was arranging with NTDTV for the channel to be aired in the Washington DC area.[56] CCTV's dominance over the cable TV market in the United States is especially significant because of the importance of television as a source of information among Chinese American households. According to a 2015 Nielsen report, 78 percent of Chinese Americans speak a language other than English at home and at least half of Asian American watch television in a language other than English (this is likely more for Chinese speakers but data on that subpopulation was not available).[57]

2) **Provoking self-censorship and editorial shifts:** Perhaps the most high-profile example of this in recent years was when, in November 2013, Bloomberg executives reportedly killed a story about wealthy entrepreneur Wang Jianlin and his ties to the Chinese leadership. The company's chairman hinted in subsequent remarks that the firm would not be pursuing similar investigations in the future after it suffered reprisals over a 2012 story about Xi Jinping's family wealth.[58] The ramifications for U.S. readers of such self-censorship surrounding reporting on a businessman like Wang have become more significant as he has personally begun investing in the film and entertainment industry in the United States.[59] In October 2016, it was discovered that Bloomberg's website had placed its June 2012 story about Xi behind a paywall, even as another award-winning 2012 article about poverty in India remained accessible to all visitors.[60]

---

[55] These sums are calculated from data in a network carriage report provided by SNL Kagan, August 2016. Detailed data on file with the author.

[56] New Tang Dynasty Television, "Promoting the Availability of Diverse and Independent Sources of Video Programming," submission to the Federal Communications Commission [MB Docket no. 16-41; FCC 16-129], January 26, 2017, https://www.fcc.gov/ecfs/filing/1012763254871.

[57] Nielsen, "Asian Americans: Culturally Connected and Forging the Future: The Asian-American Consumer 2015 Report," June 2015, http://nielsencommunity.com/report_files/Asian_Consumer_Report_2016_Final.pdf.

[58] Howard French, "Bloomberg's Folly," *Columbia Journalism Review*, May/June 2014, http://archives.cjr.org/feature/bloombergs_folly.php; Barbara Demick, "The Times, Bloomberg News, and the Richest Man in China," *The New Yorker*, May 5, 2015..

[59] Patrick Brzeski, "Wanda Chairman Reveals Ambitious Plan to Invest Billions in 'All Six' Hollywood Studios," *Hollywood Reporter*, November 2, 2016, http://www.hollywoodreporter.com/features/wanda-chairman-wang-jianlin-plans-invest-billions-hollywood-942854.

[60] Mike Forsythe reported the discovery on his Twitter account. As of the time of writing, the June 2012 article remained accessible only to Bloomberg Professional Service Subscribers, while the September 2012 piece about India was freely available. https://twitter.com/PekingMike/status/789374785901826048; https://www.bloomberg.com/news/articles/2012-06-29/xi-jinping-millionaire-relations-reveal-fortunes-of-elite https://www.bloomberg.com/news/articles/2012-09-06/indias-poor-starve-as-politicians-steal-their-food (Accessed April 27, 2017).

A detailed 2016 PEN America report about foreign news organizations operating in China found that Chinese government pressure had led to an increase in internal vetting of stories that could be politically sensitive, with the result that "the story gets softened," spiked, or published with a delay. The study also found that news organizations were often more proactive in self-censoring coverage on Chinese-language websites compared to English ones. Chinese-language editions tended to be more focused on economics, business, and lifestyle stories than politics. In some cases, articles only appeared on the English websites of outlets but not on their Chinese version—such as reporting by outlets like Reuters and *Fortune* with regards to Chinese leaders named in the leaked Panama Papers published in April 2016.[61] Such omissions affect not only readers in China but also Chinese speakers in the United States and elsewhere.

Chen Pokong has relayed less well-known incidents in the Chinese-language sphere. In 2010, access to his blog on a New York based news website was blocked after it opened an office in Beijing. Since 2009, the hostess of a political talk radio show in Los Angeles has suspiciously redirected the discussion when he raised points related to incidents of abuse or corruption in China. More recently, he reports observing a shift in the tone of editorials in a prominent Taiwanese-owned Chinese newspaper in the United States, resulting in commentaries that tend to be more supportive of the Chinese government's position on issues like the South China Sea or North Korea and more critical of the U.S. government than in the past.[62]

3) **Imposing financial difficulties on disfavored media:** By the evening of October 25, 2012, after China blocked the *New York Times'* English and new Chinese-language websites in retribution for a story about then-Premier Wen Jiabao's family wealth,[63] the entire media company's stock had fallen by 20 percent compared to 24 hours earlier.[64] Over the following months it returned to its previous levels but the example highlights how censorship in China can negatively impact the financial viability of a major U.S. paper. Since then, the repeated obstructions the *Times* has faced regarding its Chinese-language content—including Apple's recent removal of its app from stores accessible in China—have likely had other economic ramifications. In particular, circulation and readership figures suffer as each new round of obstacles is imposed, making finding and retaining advertisers more difficult.

---

[61] PEN America, *Darkened Screen*.
[62] Interview with Chen Pokong, April 24, 2017.
[63] Keith Bradsher, "China Blocks Web Access to Times After Article," October 25, 2012, http://www.nytimes.com/2012/10/26/world/asia/china-blocks-web-access-to-new-york-times.html.
[64] "The New York Times Company", Yahoo Finance, historical data for October 1-31, 2012, http://finance.yahoo.com/quote/NYT/history?period1=1349064000&period2=1351656000&interval=1d&filter=history&frequency=1d.

> Such manipulated competition for advertising is evident among Chinese diaspora media in the United States as well. Certainly the imbalanced reach of television stations to cable viewers as described above renders CCTV or Phoenix TV a more attractive avenue for advertisers wishing to reach the Chinese American consumer market than their competitors who are more critical of the CCP. More broadly, many businesses in the Chinese community are reticent to advertise with outlets that take a more critical stance towards the Chinese government, and more inclined to advertise in strongly pro-Beijing papers like *China Press*, either because of direct or indirect pressure from consular officials.

In spite of these and other examples, **there are clear limits to Beijing's influence**. Media outlets in the United States daily put out news that the CCP would likely prefer hidden, and the plight of prominent Chinese activists has received much American media and policymaker attention.

Various factors—from market pressures to journalistic integrity to independent courts—serve as countervailing forces to CCP influence. Media executives and advertisers in North America have boldly refused Chinese pressures despite potential reprisals. Targeted media have developed creative ways to disseminate their content to millions in China and within the United States. For instance, following Bloomberg's killing of the story about Wang Jianlin, the *New York Times* hired the key reporter and subsequently published its own exposé in April 2015.[65] Even after the *Times'* application on Apple was blocked, a different application available to Android users via a less easily censored avenue is still reaching readers in China.

Other CCP initiatives have not entirely achieved their objectives, particularly in parts of the market that remain more evenly competitive. Notably, several media outlets founded by American Falun Gong adherents have professionalized and expanded their programming over the past decade, which appears to have yielded fruit in terms of listeners and viewers. Thus, one of the most popular Chinese-language radio stations in the San Francisco Bay Area is the non-profit *Sound of Hope*, owned by local Falun Gong practitioners and known for broadcasting news about human rights abuses in China, hosting political talk shows critical of the CCP, and providing information that can help new immigrants learn about American values and assimilate to life in the United States.[66] Similarly, an examination of website ranking on Alexa reveals that *New Tang Dynasty TV*'s Chinese-language website significantly outranks Xinhua News Agency and CCTV within the United States (ranked 947th, 2,103rd, and 2,475th respectively).[67] *Voice of America*'s online

---

[65] Michael Forsythe, "Wang Jianlin, a Billionaire at the Intersection of Business and Power in China," *The New York Times*, April 28, 2015, https://www.nytimes.com/2015/04/29/world/asia/wang-jianlin-abillionaire-at-the-intersection-of-business-and-power-in-china.html; Barbara Demick, "The Times, Bloomberg News, and the Richest Man in China."

[66] "Sound of Hope Radio," Member Directory, Silicon Valley Chamber of Commerce (accessed April 27, 2017) http://www.svcoc.org/cgi-bin/DJmbr_showmbr.cgi?T=mbr-webcard.html&MBR=00543.

[67] NTDTV.com, Alexa rankings, http://www.alexa.com/siteinfo/ntdtv.com (accessed April 25, 2017); Xinhuanet.com, Alexa rankings, http://www.alexa.com/siteinfo/xinhuanet.com (accessed April 25, 2017); CCTV.com, Alexa rankings,

political discussion shows in Chinese have also gained a following of tens of thousands of regular viewers.[68]

In the English-language sphere, it would appear that for the most part, many Americans are not attracted to or convinced by Chinese government propaganda, particularly when its state-run origins are evident. An examination of CGTN America's presence on social media websites like YouTube and Facebook reveals relatively low numbers of followers and viewers, ones that pale in comparison to major U.S. television networks or initiatives like NTDTV's English-language programming. Most CGTN America videos on YouTube and posts on Facebook garner just a few dozen views or comments, sometimes reaching several hundred viewers. One of the channel's most popular YouTube videos—which garnered 896,947 views over the past year—is about the happy experience of being a panda nanny, an example of content that provokes a "feel good" reaction to China but is not necessarily incisive political propaganda.[69] By comparison, CNN videos about China on YouTube[70] and *China Uncensored*, an English-language parody news show about China by NTDTV (whose application was also recently blocked by Apple in China, Hong Kong and Taiwan)[71], routinely gain tens of thousands of views, with the most popular items reaching several million hits.[72] Similarly, despite the China Watch insert calling for a boycott of Shen Yun, many of its performances throughout the United States were sold out.

More broadly, recent public opinion surveys indicate that more Americans have an unfavorable view of China today compared to ten years ago. This negativity covers topics like China's human rights policies, cyberattacks, and impact on global pollution, alongside economic concerns.[73]

Despite these limits on the Chinese government's media influence efforts in the United States, the current and potential future impact of the tactics deployed should not be underestimated. As noted above, they impose a significant and potentially debilitating economic burden for targeted U.S. media outlets. Meanwhile, the heavy influence of Chinese state media on Chinese-language speakers, particularly via the television market, could have significant political implications, as millions of Chinese voters might be influenced by biased state media coverage of the United States.

---

http://www.alexa.com/siteinfo/cctv.com (accessed April 25, 2017).

[68] https://www.youtube.com/results?search_query=voachinese+%E7%84%A6%E7%82%B9%E5%AF%B9%E8%AF%9D

[69] https://www.youtube.com/c/cgtnamerica

[70] https://www.youtube.com/user/CNN/search?query=china

[71] Reporters Without Borders, "Apple TV censors 'China Uncensored' show," April 18, 2017, https://rsf.org/en/news/apple-tv-censors-china-uncensored-show.

[72] https://www.youtube.com/user/NTDChinaUncensored

[73] Richard Wike, "Americans' Views of China Improve as Economic Concerns Ease," Pew Research Center, April 4, 2017, http://www.pewglobal.org/2017/04/04/americans-views-of-china-improve-as-economic-concerns-ease/; Dorothy Manevich, "Americans have grown more negative toward China over the past decade," Pew Research Center, February 10, 2017, http://www.pewresearch.org/fact-tank/2017/02/10/americans-have-grown-more-negative-toward-china-over-past-decade/.

In the medium to long term, as relationships of economic dependence between the Chinese government and U.S. media outlets increase, this opens the door that pressure to self-censor on certain topics will be more effective. Lastly, should some kind of military confrontation erupt between the United States and China in the future, the avenues of dissemination and control over key nodes in the information flow that the Chinese government has developed inside the United States could be deployed in ways that more directly undermine U.S. national security.

Future outlook

As the above analysis suggests, the Chinese party-state has thus far displayed an ability to adapt to changing conditions in order to increase the effectiveness of its influence over the U.S. media landscape in both English and Chinese. From this perspective, if certain efforts do not yield the desired results while others do, it is likely that at least some resources will be re-oriented in the latter direction. This could manifest in a number of ways.

- First, new methods for insinuating state media content via existing outlets may appear. This could encompass a progression to content-sharing agreements between certain English-language outlets and Chinese state media, as has occurred in the United Kingdom.[74]
- Second, Chinese state media and other content providers may try to identify new and subtle ways to incorporate their content into mainstream information flows via more sophisticated online and social media strategies. This could prove effective at a time when many Americans get their news from social media and may not pay attention to its original source.
- Third, the CCP may try to more aggressively transition—within the constraints of U.S. law—from "borrowing the boat" to "buying the boat," particularly via individual entrepreneurs either in the United States (as the example of James Su and CRI demonstrates) or in China (as Jack Ma's purchase of Hong Kong's *South China Morning Post* typifies). If successful, this could be very effective, as Brady notes:

    > In the long run, the new strategy of "buying the boat"—taking over Western cultural and media outlets—may turn out to be the most effective way of improving China's "international face" and constraining international debate about China-related issues.[75]

Such adjustments are likely to occur alongside continued efforts to stifle the dissemination channels and reporting of U.S.-based media deemed critical of the CCP. In addition, the trend of content that appears more aggressively pro-China, anti-American, or inflammatory vis-à-vis CCP critics may continue. Within China, several harshly anti-Western propaganda videos have been produced in recent years, while forced confessions by detained lawyers and Hong Kong bookseller

[74] David Bond, "Mail Online to share content with People's Daily," *Financial Times*, August 12, 2016, https://www.ft.com/content/c38c33b4-6089-11e6-ae3f-77baadeb1c93.
[75] Anne-Marie Brady, "China's Foreign Propaganda Machine."

have appeared not only on CCTV but also on Phoenix, likely viewable from within the United States.

V. Recommendations for U.S. government and Congressional responses

Much is at stake as this transnational contestation unfolds. Independent media outlets facing Chinese reprisals experience rising costs and loss of advertising revenue in an already competitive and financially challenging industry. Individual reporters encounter restrictive editorial policies, threats to their livelihood, and even physical injury. News consumers in the United States are deprived of information for assessing the political stability of a major trading partner, responding to health and environmental crises, or taking action to support Chinese people's quest for a freer and more just society. As China's international role expands alongside a deep sense of CCP insecurity at home, these transnational confrontations will grow in importance, presenting both challenges and opportunities for those who wish to see the emergence of a freer and fairer market for China-related news in the United States.

As the United States government seeks to identify an effective response to the above developments, it faces several challenges. These include the subtle nature of Chinese government media influences and a lack of awareness among many policymakers to their prevalence, as well as the deliberate secrecy attempted by entities involved and the presence of some American entities who stand to gain financially from certain tactics.

In practical terms, policy areas such as this tend to fall between the cracks of the U.S. government bureaucracy. Thus, an entity like the State Department, which might best understand the dangers and actors involved, is not able to address events that occur within the United States. Meanwhile, other government agencies that may be relevant to these issues—like the FCC or the Department of Justice—may lack the relevant expertise to identify and address threats.

Lastly, in seeking solutions to the challenges presented by expanding Chinese government propaganda and censorship in the United States, **it is critical that U.S. policymakers uphold democratic principles like freedom of expression**, rather than themselves arbitrarily constraining Americans' access to certain sources of information.

As policymakers chart a way forward in the face of this complex and multi-faceted environment, Freedom House recommends focusing on enforcement of existing legislation, initiatives to increase transparency about media ownership, and efforts to balance the playing field between indigenous U.S. outlets and Chinese state-supported competitors. A number of steps that the Trump Administration and Congress can take in these regards include:

- **Take diplomatic action:** The U.S. government should thoroughly investigate reports of Chinese diplomats pressuring editors, journalists, or advertisers in ways that constrain media

freedom in the United States. The U.S. government should respond forcefully to confirmed cases of obstruction with diplomatic demarches and even expulsion of relevant personnel. This would send a strong signal that such behavior contravenes the norms of the Vienna Convention on Diplomatic Relations and will not be tolerated.

- **Implement counter-propaganda act**: In December 2016, President Obama signed into law the *Countering Disinformation and Propaganda Act* as part of the FY 2017 National Defense Authorization Act (NDAA). Among other provisions, the act calls for expansion of the Global Engagement Center at the State Department to enable greater interagency cooperation on this issue. It also includes a funding mechanism for civil society organizations, think tanks, and other experts to help identify and analyze new trends in foreign government propaganda and disinformation techniques related to China. The State Department should act quickly to implement the legislation, particularly its monitoring mechanisms. It should disburse relevant funds in a timely manner and include closer monitoring of the situation in the United States, including potential purchases of American media outlets by companies or entrepreneurs with close ties to Chinese government entities.

- **Hold a Congressional hearing:** Congressional committees should hold their own hearing or investigation into the Chinese government's influence on media in the United States, including apparently anti-competitive actions taken by CCTV or Chinese government representatives that have resulted in their dominance over the Chinese-language cable television market or reduced advertising for competing U.S.-based news outlets.

- **Re-examine regulatory framework:** FCC regulations should be reassessed and possibly adjusted so that the United States' regulatory framework is better equipped to constrain some of the loopholes related to ownership stakes or unequal access opportunities that have enabled developments like CRI's broadcasts or CCTV's disproportionate dominance in cable household reach.

- **Enhance transparency:** In reviewing FCC rules, consideration should also be given to implementing requirements for greater transparency regarding foreign government ownership of media outlets or the labeling of paid content sponsored by foreign governments. This could result, for example, in China Watch supplements having to indicate that the original source of information—*China Daily*—is a Chinese state-owned media outlet.

- **Improve FARA enforcement:** At present, it would appear that the *Foreign Agents Registration Act* can encompass foreign state-owned media operating in the United States. A number of Chinese entities—like China Daily's distribution company—are indeed registered. But the number of people and entities registered from China seems to be remarkably few

considering what we know about Chinese intelligence gathering and information warfare efforts. In practice, there appear to be loopholes in enforcement or definitions. These should be closed so that more publications transmitting Chinese-government propaganda and individuals working for agencies like Xinhua and *People's Daily* who are likely collecting intelligence on Chinese dissidents in the United States are encompassed.

- **Respond promptly to findings of CFIUS review:** In September 2016, the Government Accountability Office (GAO) sent a letter to members of Congress agreeing to examine whether the Committee on Foreign Investment in the United States (CFIUS) has sufficient legal powers to keep up with efforts of state-owned firms from China and elsewhere to buy strategic assets in the United States. The GAO said it would begin its review in four months, meaning that the assessment should currently be underway.[76] Per the letter from members of Congress that prompted the review, the GAO should be including potential U.S. media acquisitions in its examination. Freedom House supports this review, particularly in light of the above discussion of a potential Chinese government transition to "buying the boat" in the form of acquiring U.S. media assets in order to conduct its foreign propaganda efforts. When the findings of the review are made public, Congress should rapidly take action on any legislative amendments that may be necessary to ensure that CFIUS has the power to review acquisitions of U.S. media companies by Chinese state-owned or affiliated firms.

[76] David Alexander, "GAO to examine panel on foreign investment in U.S. strategic firms," Reuters, October 3, 2016, http://www.reuters.com/article/us-deals-cfius-congress-idUSKCN1231YA.

PANEL II QUESTION AND ANSWER

COMMISSIONER WESSEL: Thank you all for being here or being here again, and these issues I think have reached critical importance so it's very timely as we assess China's activities here and in global markets.

My first question relates to the question of Hollywood and censorship, self-censorship, propaganda value, et cetera. This year marks the renewal opportunity for the U.S.-China MOU on how many U.S. films get access to the Chinese market. And over the last two or three years, we've seen a substantial increase in the acquisition of U.S. media properties by Chinese companies--AMC, the attempted acquisition of Dick Clark Media Productions, and a number of others.

I've been looking at the question of whether we should demand that as part of our renegotiation this year that at least half of the allocation of the films that get into China--right now I think it's 34--that at least half of them have to be reserved for domestically or non-Chinese-owned companies.

I'd love to get your views, each of your views, on whether that has value, whether that will promote greater freedom of content expression within those films, et cetera? Ms. Kalathil, you want to start?

MS. KALATHIL: Thank you.

I probably can't speak specifically to the exact number of films.

COMMISSIONER WESSEL: Understand.

MS. KALATHIL: I do think that one of the things that is contributing significantly to what is happening with the film industry is this bottleneck within China and the fact that so many international and particularly U.S. companies need to rely on the Chinese market for their big-budget films to be a success.

In the past, this was not the case. However, now, because the Chinese market and the rising Chinese middle class, they go to the movies all the time, and who can blame them? And so increasingly that market is crucial to not just the movies themselves but the studios that are backing them their success.

And so you can see how then because all these movies are trying to fit through this artificial bottleneck, these 34 that have been selected, that is really, I feel, one of these rate-determining factors that then induces so much of the follow-on effects with respect to content.

So any efforts that might be able to address that particular bottleneck I think would be welcome, and I think, as you've said, this is the year where this will be renegotiated, and I think that is where there's already an existing opportunity to look at some of these issues.

COMMISSIONER WESSEL: But the underlying issue, as well--and thank you for that--there's the bottleneck there, but there's also the acquisition issue here. What are your views on the acquisition? You know, again, the AMC acquisition gave me even greater pause because not only do they have the bottleneck in China, but now potentially there's a bottleneck here because there could be subtle pressure by AMC on the studios to make sure that it is China-friendly content so we're reducing the number of eyes globally that can view these films.

Are you bothered by the acquisition trend here or is it not an issue? And both for you to continue and Ms. Cook as well.

MS. COOK: I think the acquisition, and going to Shanthi's points about the different nodes in the information flow that the Chinese government is very strategic at capturing, I think that is what's disconcerting.

Part of the reason for the acquisitions, and also for Hollywood, is because they want to get around the 34 quota because co-productions don't necessarily count among the 34.

COMMISSIONER WESSEL: Right.

MS. COOK: So from that perspective, to me, it would seem like half the allocation seems small if you're retaining it.

COMMISSIONER WESSEL: I'm happy to go higher.

MS. COOK: I mean one question would be whether there would be an option to increase the bottleneck and push for 50 films instead of 34. That would be perhaps the first thing, and then if within that, perhaps to have something like that, within the allocation.

I guess what I don't know is whether even from a U.S. perspective that could be considered discriminatory in any way. That you would have to look at if there is any discrimination against studios that are still U.S. studios even if they're partially owned by the Chinese government in terms of their opportunity to be part of this set of movies that get into China.

So I think I would prefer trying to push initially to just increase the number. There has been discussion of that. There has definitely been floating around the Chinese side about this and having U.S. policymakers push to make it 50 or 70 is worth a try.

COMMISSIONER WESSEL: Okay. Mr. Southerland, any comment?

MR. SOUTHERLAND: I would like to see more reporting on the self-censorship that's going on. This is not just a business story, and I think a lot of the reporting so far has been about will they get the deal, will they get this or that?. Hollywood is trying as hard as it can. The fact is this is really dangerous stuff they're engaging in, and I think they should be shamed. I think the Hollywood story made it to the front page of the Wall Street Journal the other day. So people are paying attention to a certain extent.

But let's hear more from these reporters about what's been censored. It was interesting to see that the Matt Damon movie completely bombed, and there were fascinating reviews of it, but nobody liked it. I mean I assume they can do better, but that was just kind of fun to observe. But more reporting, more attention, more talking about it, I think, not just whether it's going to be 34 or whatever.

COMMISSIONER WESSEL: Thank you.

HEARING CO-CHAIR WORTZEL: I have two sets of questions. I'll try and move through them quickly. I want to follow up on Commissioner Wessel's points about global media influence. If you went to the National Defense University or one of our war colleges, they would teach that there are four elements of United States' national power. Broadly, those are diplomatic, economic, military, and cultural or informational.

So, at least for me, an element of our national security is the cultural and informational element. You can call it soft power. If we are seeing this activity inside America's media, should CFIUS, the Committee on Foreign Investment in the United States, or the FCC be empowered to do something about that to preserve this cultural element of the national security?

The second one I talked to you about, Ms. Cook. Your testimony cited the Countering

Foreign Propaganda and Disinformation Act of 2016, which directs Department of State to establish a center for information analysis and a response to broadly information warfare, propaganda in the U.S.

That was in the National Defense Authorization Act. So I'm not sure that the appropriations committees, which would be State and Foreign Ops, even appropriated money for that, but even if they did, what can Congress do to force State Department to follow that "shall" because sometimes they ignore it?

MS. COOK: So I'll address the second one. I think letters, phone calls, raising this in interactions between both the members of Congress that introduced that piece of legislation and others who might have an interest in it.

Second, another one of our recommendations would be to hold congressional hearings, and from what I have understood, again, there hasn't been action on it. I think having the State Department, and a lot of things are in flux in the State Department at the moment, but, at least getting the ball moving on that because as we've heard, the Chinese government is moving.

So if we take three years, and it's amazing because when I wrote the report on The Long Shadow of Chinese Censorship in 2013, a lot hasn't changed, but it's also disappointing to go back now and reexamine this, and see the things that have changed. So if we wait three years until the money gets allocated, until there's actually any action, that would really be a missed opportunity.

And then regarding your first question, I think overall this question of having CFIUS review these kinds of acquisitions would be probably a bit more appropriate initially than the FCC. I think with the FCC, perhaps some of these issues related to the imbalance among the Chinese language media and things like that, where there are potentially anti-competitive actions going on, would be more important, more relevant.

And also the question of transparency. I mean it's very clear from the CGTN America example, when Americans know this is Chinese government propaganda, they're not going to watch it. But you start having things like the Reuters report about China Radio International where it's not so clear, or China Watch, where a lot of people do know, but if you actually look, especially online when they describe China Daily, it just says this is the leading English-language newspaper in China, and having some kind of requirement that would have to say "owned by the Chinese government," at least for anyone who's looking a little bit more deeply, you know, besides “paid supplement” by the Chinese government or something might at least flag for Americans and make them less vulnerable to believe in the Chinese government's propaganda.

HEARING CO-CHAIR WORTZEL: Thank you.

MS. KALATHIL: I would just echo Sarah's comments about transparency. You know, I think what we have right now is an environment where sometimes we are not always fully aware of which Chinese government entities may be backing or affiliated with companies that are making purchases. So any effort that can shine more light on who's behind certain acquisitions, whether that is through official mechanisms, such as CFIUS, or through civil society and reportorial efforts that really create that increased transparency I think that would be helpful.

HEARING CO-CHAIR WORTZEL: Any?

MR. SOUTHERLAND: No. I defer.

HEARING CO-CHAIR WORTZEL: Commissioner Bartholomew.

CHAIRMAN BARTHOLOMEW: Thank you and thank you for all of the work that you all do.

Commissioner Wessel said in the last panel he was discouraged. I actually found some hope in the last panel and have to say that I'm a little discouraged not by what any of you said but I'm discouraged by what the U.S. government has said over the course of the past couple of months and even over the course of the past couple days.

So the work that you do, the work that you do as civil society in our country, which is always important, is taking on even more importance. So thank you. Thank you for all of that.

When we first started talking about the acquisition of the AMC theater chain, people looked at us like we were crazy. What is this? This is "Reds under the bed." Here we go. Here we go. And yet when you look at it in the context of acquisitions of companies that make films, do we have any evidence yet that AMC has blocked--I'll put it differently--has chosen not to show films on issues that might be sensitive?

For example, I don't know that anything has been made about Tibet lately, but I'm having a tough time thinking that AMC would allow a movie about Tibet to be shown. Is there any evidence yet? Do any of you know? Have you heard anything?

MS. COOK: I haven't. I mean I think the issue of not having a big movie on Tibet is more related to the other side of the self-censorship. I haven't heard. I think what we saw was one example of the opposite where there was this Chinese propaganda film where they had someone playing Chiang Kai-shek that showed at my local AMC in New Jersey.

And I don't know that many people went there.

CHAIRMAN BARTHOLOMEW: Yeah.

MS. COOK: One of my colleagues went to watch it out of curiosity and said the theater was empty. But I don't know if that would have appeared if the AMC had been under other ownership. If there were to be anything clear like AMC refusing to show a film on Tibet, I would hope in the United States, there would be protections.

Again, the Chinese are always very careful not to be so direct about this. They just won't answer the calls or something like that by whoever the director was of a film that found itself not being put on screens in AMC, that they would have legal recourses in the United States. But I haven't heard any cases or complaints yet.

CHAIRMAN BARTHOLOMEW: Mr. Southerland, you mentioned the issue of reciprocity on the visa issue for journalists, and I commend you for the nuance on that because in previous years when people have raised that issue, there has always been concern about the free speech here in the United States, and we don't want to punish journalists from other countries because we believe in free speech here. So I think it's interesting to explore this idea of reciprocity with some nuance.

Some of us met yesterday with people from the AmCham in China, and they are actually talking about reciprocity in a different context but also more nuanced, that if there's a restriction on corn, we don't necessarily restrict corn, but we look at other sectors.

So could you expand a little bit on sort of how you would structure something like making sure that U.S. journalists can get the visas to work in China?

MR. SOUTHERLAND: Well, we'd have to get some U.S. agencies on board on this

agreement. I mean it's the kind of thing they might not enjoy doing. Diplomats tend to want to kind of stay with the established procedures so I think some work has to be done educating people.

But just mentioning the Chinese journalists, I think many of them would like to do better work, and there's no way we can directly encourage that, but they'd like to do better, and some of these people are the ones who are here. So we have to make that very strictly clear.

I think we need more input from the foreign correspondents themselves, and I of course hoped to do a ten-person survey, but I did a three-person survey, and I got one guy who wants to be very tough, and another one that says that's ridiculous, we shouldn't do it, but it would be helpful if the Foreign Correspondents Club could weigh in on this. They should take the lead, and they should say what they think would help.

It's about all I can say about it at the moment. I put it out there as my last point up for discussion kind of thing. But this kind of discussion would be useful, but it has to be carefully nuanced.

CHAIRMAN BARTHOLOMEW: So we're also seeing restrictions in the United States, on consolidation of media, potentially being lifted here in the United States, and I wondered if anybody has given any thought yet to what is the impact here when we know that some of the companies that are interested in the acquisition, in the consolidation, are actually also trying to do business in the China market? Any concerns about that?

MS. COOK: I would say it's disconcerting whenever there is any company that has large interests in China, the reality is the Chinese government is very good at using such investments as “sticks”. I think the suspicion with regard to this imbalance in the cable industry is that there's been some kind of wink-wink because they can't put this in paper that CCTV doesn't want to be in the same package on cable with a pro-Taiwan or a Falun Gong-owned television station.

There was an incident in France, it was much more explicit, where Eutelsat, a French satellite company, was airing NTDTV, and the Chinese government almost did this kind of bait and switch. Basically Xinhua or some other state-run television broadcasts, they made a deal with them so that they would get this big Chinese state-run deal, and then they essentially shut off New Tang Dynasty beaming into China. But this was a French company.

And Reporters Without Borders got this undercover Chinese person pretending to be a Chinese government official to call Eutelsat, and there's this incredible transcript where the Eutelsat VP, or the person, whoever it was, maybe in China, was very explicit about the fact that they had shut down NTDTV's broadcast as this quid pro quo to get this deal.

And so it's very unusual to be able to catch that, but those are exactly the kinds of things that happen behind the scenes. And even for advertising companies, an advertising company or an advertising firm that has a large business interest in China, we've had cases both in the United States but also for some of the Hong Kong papers where they withdraw advertising because of pressure from China.

And that's where it really gets to this whole ecosystem that can threaten the financial viability of publications. As you get larger companies with more interests in China, they become more and more susceptible to that kind of pressure from the Chinese government.

CHAIRMAN BARTHOLOMEW: Anything to add?

MS. KALATHIL: Yeah. I'd just add that, you know, this has been the system that has

been at play within China for many years, and I think what we've seen recently is that as these Chinese companies have gotten bigger and they're now starting to go global and go overseas, we're starting to see this inducement towards self-censorship using the market as a tactic that's seen much more widely. And so we're already familiar with it. We can expect to see it overseas as well.

CHAIRMAN BARTHOLOMEW: Thank you.

HEARING CO-CHAIR WORTZEL: Commissioner Shea.

VICE CHAIRMAN SHEA: Well, thank you very much for being here and for your testimony.

When you get to ask questions this late in the game, you realize that your questions have been taken, but I was going to ask you about whether media and Hollywood acquisitions should be covered by CFIUS, and whether Hollywood would ever make a movie that is sympathetic towards Tibet or Taiwan?

So those are my questions, but I'm going to just read something out of Ms. Kalathil's testimony, which she mentioned a little bit, glossed over in her oral testimony, but I think it's really powerful and kind of summarizes what's at stake here.

You say China seeks to exert global influence, shape international news, guide the evolution of the Internet and its norms, and influence global culture through Hollywood. Seen individually, any distinct piece might be glossed over as a discrete, isolated activity. Yet, taken together, they are indicative of an authoritarian government that has mobilized global information resources on a massive scale to project power, maximize its desired outcomes and protect its own rule.

Now when I read that, I did a double take on that. And so if you believe that, shouldn't we be viewing these acquisitions in Hollywood through a national security lens?

MS. KALATHIL: I think that that trend is already occurring, as many have mentioned. The CFIUS reform has now been high on the agenda for a while, and so as I said, I think from the standpoint of civil society and supporting democracy, any efforts to shed light on the details of these transactions to perhaps if I had the resources to go through and catalog, as you say, how movies were made about Tibet or Taiwan or issues that were sensitive to China within, let's say, the years--

VICE CHAIRMAN SHEA: Hong Kong.

MS. KALATHIL: --you know, exactly--the years before the last five years and within the last five years, it would be very interesting to have more research and information around that so we can make better decisions based on that.

MS. COOK: I'll just add on the CFIUS issue. There was a letter from members of Congress to the GAO to do this kind of review, and the GAO's response in September 2016 said they'd be starting it in about four months. So I think they are. I think then it's really going to be kind of similar to the Counter-Propaganda Act, up to Congress when they come back to really act quickly on this because, again, these things are in motion. These deals are being made.

So the sooner that the mechanisms of the U.S. government bureaucracy can get these considered under CFIUS more closely and tweak anything that would be necessary if they are, I think the better, and it would give an opportunity to see whehter certain acquisitions are approved under certain conditions.

That's what you see happening in some cases with the National Communications Commission in Taiwan, where some of the acquisitions from China, they'll approve or they'll partially approve. There are discussions about, well, you could have it, but you have to remove your stake in this or that company that probably could potentially be used as the leverage from the Chinese government, if you want to acquire this or that other business. So there might be those kinds of provisions that could be considered.

VICE CHAIRMAN SHEA: I don't see the blue thing waving at me.

CHAIRMAN BARTHOLOMEW: No, actually you've got lights there.

VICE CHAIRMAN SHEA: Oh. I still have time.

This is for Mr. Southerland. I mean you talked about reciprocity and Chinese journalists and U.S. journalists, and you mentioned Robert Daly's quote, but are they equivalent--Chinese journalists operating in the United States and other Western nations and U.S. and Western journalists operating in China? Do they have the same--

MR. SOUTHERLAND: Code of ethics?

VICE CHAIRMAN SHEA: Yeah. I mean same business model, same--

CHAIRMAN BARTHOLOMEW: Independence.

MR. SOUTHERLAND: No. But the game now is to tell--

VICE CHAIRMAN SHEA: Job description? Same job description?

MR. SOUTHERLAND: --tell some truth but also don't tell the whole truth, and it's become much more clever. There's this new operation called Sixth Tone, which allows a more edgy, almost a jazzy kind of approach, run by a very good editor who's experienced, a foreign editor. So we're going to see more of that.

The message, though, underlying message, is to get across Xi Jinping's aim of, regime aim of everything is peaceful, every deal is win-win, and tell China's good narrative, or whatever it is, China's good stories. So you see attempts in some cases, for example, to do more human stories.

Newspapers and digital outfits in China now if they get a big story, they tell a good human story, but there's all kinds of stuff that's hidden like hidden mystery. Nobody dares to talk about the Cultural Revolution in any realistic terms. Nobody will talk about the Great Leap Forward. These are all buried. Tiananmen is buried pretty effectively although I've learned since in recent years that some Chinese students do know what happened. They just don't talk about it.

They're the three Ts--Tiananmen, Tibet, and Taiwan. So they're not going to do anything that brings out developments in those three areas. And they're under a lot of censorship. It's not that obvious because it looks pretty good now. They've had very good foreign advisors, expert advisors, help them make it look better. But I don't think those advisors have been able to do much to make the content more reliable and balanced and fair and so forth.

There's an attempt to appear to do that, on a discussion group or whatever. Bring in some different views, but the underlying message is you got to make Mr. Xi and China look good. That's it. That's a little more than you wanted, but--

VICE CHAIRMAN SHEA: Thank you.

HEARING CO-CHAIR WORTZEL: Commissioner Stivers.

COMMISSIONER STIVERS: Thank you. Thank you. Thank you all for your excellent

testimonies and your concern about China's export of propaganda and censorship. These efforts are certainly counter to our values of having a free and open society, and it also has negative consequences to our economy and perhaps our national security.

I tend to put this issue into two, to separate it between the impact on U.S. domestically and then the impact more broadly internationally or in third countries. In particular, pressure on U.S. academics, business executives, analysts, artists, journalists is a major, major concern, either in terms of negative pressure or incentives to gain more access to China to do their job, and you certainly see this, and how this can affect policy and decisions and different specific goals that the Chinese government may want to pursue in terms of to study or promote certain viewpoints or not other viewpoints.

And so I see this on the micro level as being very effective. But as Ms. Cook stated in her testimony, broadly, in terms of an impact on the American people, it doesn't seem to, whether these inserts in the Washington Post or other more broad messages about China, seems to be a real drop in the bucket compared to the wealth of information that we have from all sources in the palm of our hands.

And so I kind of separate that into kind of the micro and macro views. And so moving to third countries, especially developing countries, in Asia, in particular, my thought would be that this would have the same impact--I'm looking for your views on this--that micro wise, it can achieve certain goals through influence, but--and I want you to tell me if you think this is wrong--but in terms of a macro, you still see very negative views of China, in particular, in the international community, even those who lack a lot of the same access that Americans do.

And so I guess my question here is what do you think about that? But also how do we measure how effective they are? Is it through public opinion surveys? I can't think of a way to kind of measure the micro in any real way that we can tell how effective they've been. So how do we measure that, and then, of course, how do we counter that in third countries, in particular?

So I don't know who wants to take a stab at that? Mr. Southerland.

MR. SOUTHERLAND: Yeah. There are limits to what the influence can do, and I think, I picked Australia where we just had an incident that so undercuts China's soft power it's unbelievable. I haven't evaluated it yet, but a Chinese delegate to an international conference on illegal diamond mining, in the presence of a lot of very smart people and executives, suddenly explodes and starts demanding that the Taiwan observer, who is there under a precedent--this has been established Taiwan can show up at certain international meetings--he's almost screaming--I haven't been able to read the Australian press coverage yet, but I'm talking to a journalist there who considers it a very big story.

So sometimes their actions alone like this outburst or just the hard power of China sometimes intervenes with the soft power.

In Africa, by contrast, they have obviously made some gains and, interestingly, at this Australian outburst, African delegates got up and screamed in support of the Chinese or voiced their support. So what do they get out of Africa? They get some votes at the U.N. They do get some friendly gestures. But at the same time, off the coast of Africa, Chinese huge industrialized fishing boats are scooping up all the fish and driving African fishermen out of business.

I've been following this for years, and Andrew Jacobs did a great piece just recently--incredible piece. Those people are not pro-China at the moment. I mean they're losing their

jobs. There are other things happening in Africa that just don't go right like small Chinese traders coming in and taking over business in a town. There was a demonstration in Kampala in April where people were marching against these people. We thought they were going to sell the goods, the Chinese goods, which we like, the cheap goods, but not bring in their own business people.

Another incident in Ghana where illegal miners have been handcuffed and threatened with expulsion and so forth brought outbursts from the local Chinese mission saying you do illegal mining, too, you Africans. It was kind of a strange exchange, one of the rare times that diplomats would speak up. You do illegal mining too, and you better treat these Chinese miners right and stop those cartoons about our leaders. I didn't know that Africans were drawing cartoons about the leaders, but I learned from the Chinese mission that, in fact, once you get cartoonists going somewhere, that you can't stop them. I mean I tell you.

There's some cartoonists in jail for that, but--so I'm going on and on too long, but I think there are limits everywhere you go. I started looking at Latin America, and I'm not sure that that's successful there. I just didn't have time to kind of work it out. So I'm sorry to take everything over, but I guess I feel strongly about this.

COMMISSIONER STIVERS: Ms. Kalathil.

MS. KALATHIL: Sure. You know I was struck in what you said by the distinction that you, that you created, and I also was thinking back to a conversation that happened in the first panel where people were talking about the tax and whether or not the Chinese Internet users know about the tax, and I wonder if globally, the global media consumer knows about the global tax that's now happening?

So I would draw a distinction between sort of the more overt propaganda and sort of trying to achieve specific kinds of influence using specific communication versus this lack of critical information on China, which I think is much more insidious and perhaps harder to notice. And do we notice that tax as it occurs through a variety of products, through news, through movies, through all sorts of different channels of information?

And that's where I think we're in a very chaotic information environment right now as we all know. Nobody knows what to trust. Nobody knows what's real news versus fake news. I think it creates a real environment of opportunity for authoritarian regimes, like China, who I don't know that has been that active as compared to others in this space, but certainly it's looking to exploit that more.

I don't know how to answer that measurement question really well. That's something that we talk about in my own class when we teach these issues. Certainly opinion polls is one way to get at it, and I think perhaps trying to measure against specific desired policy outcomes could be another way.

But in terms of what to do, what did strike me is that as China's companies move into the global market, that actually creates a situation where the market may not work for them, and I think China has long used its domestic market as both the carrot and the stick to influence global behavior.

But the truth is that these Chinese companies, if they are to be successful at a global scale, they will need to attract global consumers. Global consumers, as you point out, have wealth to a variety of apps and a variety of options, and they will not take kindly to having their

personal privacy violated in ways that they're not used to. They may not take kindly to being surveilled or not being told about it.

So there are practices that may work better domestically for these Chinese companies that will not work in the global space, and I think that that is actually a window of opportunity, and for me I would say better education of the global consumer, efforts like ranking digital rights, which place these companies in comparative perspective, that is actually an opening when we think about what to do.

HEARING CO-CHAIR WORTZEL: Commissioner Slane.

COMMISSIONER SLANE: Thank you. Are you aware that the Chinese are trying to start a film school in Indio, California? And that they have arranged to have the University of California issue the degree? And that they're budgeting about $500 million for this project, which sort of goes to your point about how much more sophisticated they're getting in this medium?

MS. COOK: I wasn't aware of that, but I will give a plug for another organization's report that came out last week on Confucius Institutes--the National Association of Scholars--and I think it's very relevant to this example because this is kind of a branching off of that.

And it looked at 12 schools in New York and New Jersey, real in-depth case studies. It's both fascinating and disturbing. In terms of even things like the classes being taught. They've already started to--you know, Confucius Institutes are sold as being places for teaching Chinese language. At Rutgers, they're teaching a class on Chinese social, economic and cultural development in the 21st century. American students are studying that taught by the Confucius Institute.

And I don't know--are they going to read a Freedom House report in that class? I doubt it, right? And again, that's where these voices that are being suppressed, expanding beyond just the three Ts and the one F, and the Uyghurs--the Falun Gong and Tibet--to much more even mainstream sources information. Are they reading The New York Times' Wen Jiabao article--things like that? They're not going to be reading that. It's going to look very different than what would be taught by an American professor.

And I think that's where this adaptation, too, related to your question as well. I mean now we see this at the micro level, the inference maybe, but not at the macro level, but they're constantly adapting. And so realizing that if it says this is China's CCTV television, people aren't going to watch it, but if it's insinuated over radio stations, inserted in this way, maybe shared on social media so it's not clear. You know, people don't really quite know what it is, and I'm sure they're developing new tactics so they see what works and what doesn't in terms of making that change.

So I wouldn't underestimate the CCP's capacity for adapting, and I guess that just strikes me as an example that fits with other broader trends and an example of, again, taking the Confucius Institute model, maybe using it in other ways to influence the teaching of film, who the actors are going to be, and things like that in these films as well as at the studio level.

So I'll have to look into that. I don't know that example.

COMMISSIONER SLANE: Thank you.

HEARING CO-CHAIR WORTZEL: Senator Dorgan.

COMMISSIONER DORGAN: Thank you very much.

Well, this is such an interesting subject. I was thinking about the old saying, "If I owe you $1,000, I don't sleep; if I owe you a million dollars, you don't sleep." And today is Thursday. Our trade imbalance with China today will be about $1 billion. So at the end of the year this year, likely we will have a trade deficit of about 350, $360 billion with China.

The fact is we should have with that some substantial leverage in trade negotiations. It's not about who's sleeping in the leverage, but I've always been interested in this concept of difficulty getting movies into China. And I understand that censorship is unbelievably powerful. Propaganda can be very powerful. I understand why, why China is using both, but we should not necessarily accept that in our trade negotiations, particularly with respect to this issue of entertainment.

I found all over the world where I have traveled young people especially are profoundly influenced by the export of pop culture and entertainment, including movies and television from the United States. It's a very powerful influence. China wants to keep it out. I mean wouldn't it be nice to have "Hidden Figures" and "La La Land" in every Chinese theater so that if they want access to American entertainment, and "Hidden Figures" is an example in this country of us being very critical of what has happened in our country. A great history lesson for us; right?

So I just say all that because let me just say I don't agree with very much of what is happening in this country with respect to policy choices by this administration, but I do agree with this. The President has said that the current trade situation with China is not mutually beneficial. It is out of balance. He's right about that.

And I hope that our trade negotiators, whether it's on other issues or coming back to this issue with respect to our ability to get American movies into China, and hope we don't go there hat in hand and say, well, can we please go from 24 to 36 or 36 to 48? That's the wrong way to approach this.

I mean, we have certain abilities given the leverage that exists for us to demand much greater from China in these trade negotiations. I don't want a trade war, but I do want our country to insist on mutually beneficial trade relationships, and that is not currently the case with China, and we just put a highlight on part of one of it, and that deals with this issue of influence and censorship and propaganda, and so on, and I was especially interested in some of the comments with respect to how movies can propagandize by product placement and various things and the Chinese becoming more effective at the use of that.

So I just wanted to just say that. I think your testimony has really been interesting, and it's really important because these things happen, and they just wave over us, and we don't even understand the influence of it, even while it's happening perhaps. So I thank you very much for taking the time to come and share your thoughts with us.

CHAIRMAN BARTHOLOMEW: Commissioner Tobin.

COMMISSIONER TOBIN: Great. I thank you, too. And to follow up on what you've just said, Senator, we were preparing for today, reading your testimony over the weekend, and I happened to catch up on Friday's Washington Post story in the Style section. I don't know if any of you saw it. But from Beijing to D.C., the National Arboretum, our U.S. National Arboretum, the Chinese are investing $100 million in this garden to do much as the Japanese did at the turn of the last century, where the beautiful cherry trees have come, and it's a landmark throughout the year really, but in the springtime in particular.

So this is already set up. The plans are made, and I wonder, Senator Dorgan, if they will have any of the garden of the landscape, the Desert Garden of the Uyghur, or the Tibetan landscape, and so one question for you is to what extent is there a role for us to say we want to have something else included in this garden? The various ethnic groups, 50 or so, have gardens other than what at least I saw outlined here? So that's one question.

And then, Mr. Southerland--and any of you can take that--Mr. Southerland, you spoke about vast areas of the People's Republic of China it's hard to get access to.

So two questions. How do you advise American journalists to try to get access to those remote areas? And, secondly, have you thought about how journalism schools in this country, to what extent is there leverage for us to help open up either our better access to China or their journalists' broader freedoms? So I'll let you take that first, perhaps.

MR. SOUTHERLAND: Okay. Yes, yes. It's not easy because even if you're on a guided tour, it's very hard. I used to be able to break away from that kind of thing. When I went into Tibet, I was chased by people, and it was kind of fun, and I outran the police one time at a monastery. I was just so happy.

[Laughter.]

MR. SOUTHERLAND: I climbed over a monastery wall and got into Drepung Monastery, and I said where are the secret police, and the guy said they're all having tea. You got 40 minutes. I talked to a bunch of monks, and climbed back over the wall, got on my bicycle and got away. You can't have that kind of fun anymore. I mean they're really watched.

[Laughter.]

MR. SOUTHERLAND: And that's very disturbing to a journalist.

COMMISSIONER TOBIN: Too bad.

MR. SOUTHERLAND: Yeah, that's too bad. But I recently saw a Washington Post guy on a guided tour giving some hints of the controls, no matter what the guides were saying, you know, by just telling you what he couldn't see, what was off limits, was worth reporting that.

On the garden, by the way, I'm sure it would be easy to do a Uyghur garden and a Tibetan garden, and they can probably produce some happy-seeming Uyghurs to dance there. They like to see Uyghurs dancing and don't like to talk about the other stuff. So that's not probably going to be a big problem for them.

COMMISSIONER TOBIN: But it seems to me we have a role in speaking up to ask for that. Otherwise, it will not happen.

MR. SOUTHERLAND: Oh, sure. I think, I think that would show we care about the ethnic minority, so-called ethnic minorities.

On the access, there are many--there's one journalist who went into the back, the trunk of a car, and popped out at a particularly conflict-ridden area, took a couple of photographs, and got back in the trunk of the car. That's not the best way to do reporting, but, boy, did I admire that person. That was a couple of years ago.

Journalism school leverage. Our universities want Chinese students, partly because, you know, they pay their bills and this is a huge issue. It's a very broad issue. But you can't get--I don't quite understand how journalism schools would use their leverage. I mean they're on the receiving end of this incoming money. The best thing they can do is try to help people understand how to do good journalism, and eventually some of those students who would want

to do that, who stay in the business, will do it, I hope.

But, unfortunately, journalism in China right now is, because of market economics and various things, people aren't paid as well as I think they should be, and so that's one of the reasons they're dropping out of it.

Journalism schools have, are going to have some very bright Chinese students come in, and they'll understand what they're being taught, and I'd say keep that up, but I'm not sure what could be done about that effort because the Chinese, there's a big move now to denigrate Western ideas, and I'm afraid there might be a point at which some of the students who want to come to the United States to study that kind of sensitive thing might suddenly be blocked.

I mean there's a whole denigration of Western culture, universal ideas. I used to keep a taboo list of off-limits things. Universal values is now on that list. There is no such thing as universal values according to China. And so the worrisome thing here is, is the ability of China-- I'm trying to take a look at textbooks. How do they portray the West? How do they look at the West? It's kind of a struggle for me because this stuff is in Chinese, but it's something that I'm going to struggle along with and I'm going to get some help with.

The bombing in Belgrade, that was intentional. That's in the textbook as far as I can tell. Got to go deeper in. But that's not true. I mean I've checked with some U.S. diplomats who convinced me it was an accident, you know. They've tried to convince the Chinese, and the Chinese don't want to hear it or perhaps don't--

So there's a huge problem with the denigration of the West or demonization of the West that I think you need to look into at some point.

And the issue of nationalism, Chinese nationalism. I noticed in Australia, the local Chinese community is fine with cooperating and being good citizens and so forth until it comes to the South China Sea sovereignty issues. And they're now demanding the Australians start paying more careful attention as to what they say about the South China Sea, you know, directly to the leaders.

So I'm all over the place here. I'm sorry. My colleagues might be able to get more focused than I was.

COMMISSIONER TOBIN: We just have a few minutes. Thank you, Mr. Southerland.

Anything on the garden on what can do or should do?

MS. KALATHIL: Well, I would just say maybe not specifically to the garden, but to all of these types of initiatives, you know, they really all fall under this broad level of mutual understanding. That's what they're supposed to foster, right.

And I support mutual understanding, better mutual understanding, and people-to-people connections and that sort of thing, but I think whether it's a garden or whether it's a movie, it's important to understand who is speaking, who is shaping the narrative and why, who gets to tell that, and that's where I think we collectively have not really paid enough attention because I think we're just now realizing the extent to which China and other authoritarian countries are really seeking to in some ways undermine our democratic discourse.

And so now that we have become more aware to this issue, aware of this issue, I think we can start to think through how to address those issues, and part of it, as I've said, is simply through raising that and making these issues quite transparent and prominent.

MS. COOK: Again, I'm not so sure on the garden, but I think, in general, figuring out

better ways--and this might be more for private donors than the U.S. government--of providing civil society opportunities, investigative journalism opportunities, to, not to counter the narrative but to provide a more level playing field.

In some cases, that's a market issue. In some cases, it's more the market of ideas. So maybe you have the garden, the Arboretum invite a Chinese environmental activist on one of the days and do a big event, and some Tibetans because environmental issues are a growing problem in Tibet.

And for all, again, walking through a Chinese garden is an amazing experience. You know, I think it's great for Americans, American children, and that might get a kid actually interested in learning Chinese, and I think that can be really important. But, again, in terms of how do you supplement this partial view, and the same thing goes say for Confucius Institutes or for Chinese students studying here, a more systematic effort to give them a broader perspective, I think could go a long way because what the CCP fears most is that it knows in a fair level market of ideas, it's not going to be able to win.

But I think in terms of countering just the efforts to marginalize some of these different perspectives, finding ways, whether it's in terms of funding or thinking of opportunities to invite particular individuals becomes really, really important and is something that could be done regularly.

COMMISSIONER TOBIN: I think that's well said and I just want to say--

HEARING CO-CHAIR WORTZEL: Senator Goodwin. We're really over.

COMMISSIONER GOODWIN: I will jump in here. And, again, my appreciation to the panel for your time here today.

Let me in an effort to push the panel a little bit and flesh out some of these issues, let me play a bit of the devil's advocate. I would suspect that ever since the ability to mass distribute and publish artistic works of literature and music and film, there's been ongoing tension between the artistic expression and commerce, and decisions are made of those that distribute those products trying to find the appropriate balance between the two.

But it occurs to me that when works are self-censored, and not simply from an editing standpoint or during the editing stage, but from conception, it seems a little more troubling, especially when that editing or self-censorship is done not with the Chinese market in mind but with the Chinese censors in mind.

But then it occurs to me that those sorts of considerations come into play for the domestic market as well. Some studios will certainly look from conception at trying to achieve a certain rating because it has an effect on the box office draw of individual films.

So I want to hear from you all how is that qualitatively different? How is it pernicious to self-censor with Chinese censors and the market in mind? And does that complicate our efforts to try to address it and shine light on it, especially since in an instance like that, it seems far beyond the reach of CFIUS or the FCC to regulate?

MS. KALATHIL: Okay. Well, I'm going to take a very careful stab at that question. It is, you know, I think you're absolutely correct to observe that there's always a balance there, and certainly that is nothing new.

For me, I would, the way that I analyze it is that in this instance, it's the first time that a foreign country that's seeking to exert strategic influence over the United States has been able to

do so through such a prominent and influential way as through the U.S. film industry, and that's to me where I think the dividing line is, is there's always, there are always going to be issues around artistic expression and commercial success, but this is actually a sovereign government that is trying to use these things to achieve its own aims, and for me that's a distinction.

MS. COOK: I guess I would just add to that, the point you made, that this isn't about necessarily even appealing to the Chinese market in terms of how these decisions are being made but to Chinese censors. There have been lots of movies or products that Hollywood could make that might be very popular in China but that the censors might not like.

We've seen more in television where a program like Big Bang Theory is super-popular in China, and suddenly they'll go just shut down. They shut down a few years ago the streaming. So you have situations where American cultural products are very popular in China. So, then, again, it's not maybe market strategy as much as it is this question of how do you appease a foreign government body when you're considering how you're going to design a film in the United States, and then otherwise I guess I would second Shanthi's point.

I think then, just going to back to my other point, is I think that's perhaps a fund could be created—-by a non-profit or through the National Endowment of the Arts—that could fund a high profile movie starring Richard Gere about Tibet because there was just a big interview about him that he can't get roles in Hollywood now, you know, I mean that's Richard Gere.

So that's where people who care about this issue, who may or may not be the U.S. government, who are concerned about this, you know, it doesn't take a lot of money. You know, there's a documentary about Confucius Institutes that just came out. There are some other very good films--there's an award-winning movie Ten Years in Hong Kong that couldn't get even on screens in Hong Kong. So I think that would be, again, just supplementing. A little money could go a long way. A few million dollars of a fund like that could, again, demarginalize the voices they're trying to marginalize.

HEARING CO-CHAIR WORTZEL: Dan, you?

MR. SOUTHERLAND: No, I can't match that.

[Laughter.]

HEARING CO-CHAIR WORTZEL: It's been--it's a really great panel. I want to thank the three of you for taking the time to be here and your excellent and thoughtful responses.

We're going to break now until 1:45.

[Whereupon, at 12:45 p.m., the hearing recessed, to reconvene at 1:47 p.m., this same day.]

PANEL III: INTRODUCTION BY CHAIRMAN CAROLYN BARTHOLOMEW

CHAIRMAN BARTHOLOMEW: Okay, folks, we're going to begin. Panel three will begin with Dr. Chris Demchak--Demchak?

DR. DEMCHAK: Yes.

CHAIRMAN BARTHOLOMEW: Demchak--is the Grace M. Hopper Professor of Cyber Security and Director of the Center for Cyber Conflict Studies at the U.S. Naval War College.

She has degrees in engineering, economics and political science with a focus on comparative complex organization theory. Her research and many publications address global cyberspace as a globally shared, complex, insecure "substrate" penetrating throughout the critical organizations of digitized society.

HEARING CO-CHAIR WORTZEL: I'm glad you're reading that.

CHAIRMAN BARTHOLOMEW: I should have had Larry read this.

A former user of the LISP programming language, as well as a former military officer, she has taught international security studies and management, comparative organization theory, enterprise information systems, and cybersecurity.

Her recent works include Designing Resilience and Wars of Disruption and Resilience. She is now working on a manuscript tentatively entitled Cyber Westphalia: Redrawing International Economics, Conflict, and Global Structures.

Thank you for being here today, Dr. Demchak.

Next we'll hear from Dr. James Lewis. Dr. Lewis is a Senior Vice President at the Center for Strategic and International Studies. Before joining CSIS, he worked at the Departments of State and Commerce as a Foreign Service Officer and as a member of the Senior Executive Service.

His government experience includes a broad range of assignments, including developing policies on arms transfers, satellites, encryption, and securing and commercializing the Internet.

Dr. Lewis was the Rapporteur for the U.N.'s Group of Government Experts on Information Security for the successful 2010, 2013, and 2015 sessions.

He has led long-running Track 1.5 discussions on cybersecurity with the China Institutes of Contemporary International Relations. He has served on several Federal Advisory Committees, including as the Chair of the Committee on Commercial Remote Sensing and as a member of the Committees on Spectrum Management and International Communications Policy.

Dr. Lewis received his Ph.D. from the University of Chicago. We have very smart witnesses here today. Welcome back, Dr. Lewis.

Once again, we'll ask you to go ahead and limit your remarks to seven minutes. Dr. Demchak, we'll start with you.

OPENING STATEMENT CHRIS DEMCHAK, PH.D., GRACE M. HOPPER PROFESSOR OF CYBER SECURITY AND DIRECTOR, CENTER FOR CYBER CONFLICT STUDIES (C3S), U.S. NAVAL WAR COLLEGE

DR. DEMCHAK: Thank you very much for inviting me this afternoon. I need to emphasize my comments are my own and not the views of any department of the U.S. government.

Over the coming century, consolidated democratic civil societies will be a numerical minority in a deeply cybered and conflictual world dominated by non-western autocratic states.

China is now well into its rise as the huge coherent actor at the demographic and economic center of this emerging post-Western international system. It will have an enormous advantage in scale and market resources.

It has rising momentum internationally as an alternative model of success and is becoming the large new ally for existing and rising authoritarian leaders globally.

In this new world, with no counterbalancing democratic weight, China will particularly be able to influence--if not dictate--the rules in practice across the international system using its deeply embedded regional, economic and cybered bonds.

With that as background, I'd like to make four points:

First, the Internet itself grew up too fast, too cheap and too shoddy in response to Western utopian visions and libertarian IT capital goods business models to be fixed by bolting on security.

It is a substrate--not a domain--whose insecurities created a new form of system-versus-system "cybered conflict." It changed fundamental constraints on offensive campaigns in modern interstate struggles. It doubled the layers of costly complex system surprises that modern nations face.

It must be transformed to embed security as well as freedom of speech and generativity at its most basic layers.

Second, continuing Western democratic opposition to the rise of national borders in cyberspace has proven both damaging and futile. China has used the open Western Internet to massively exploit the intellectual property, IP, of Western states for upending corporate advantages in open markets.

It uses those resources to bribe or bully other actors to comply with its preferences. But its determined defense of its cyber sovereignty, in particular, accelerated into a long-term campaign to change the global cyberspace narrative into one emphasizing China as a model combining economic success and domestic Internet control.

Furthermore, Western states themselves appear a bit hypocritical because we are domestically installing defenses and national cyber policies and creating in bits and pieces our own national borders.

Thus, a global Cyber Westphalia is emerging despite our Western refusal to agree. But its technological and narrative tendencies are now being led by China and other authoritarian states opposed to civil society preferences.

Third, in this world, there will be robust, weak, and wavering cyber powers, but with the consolidated civil societies at roughly ten percent of the world's population, demographic scale actually threatens the survival of individual democracies in a more authoritarian world.

Only by combining the democratically cultural like-minded states and their private sectors into a coherent, functionally integrated and operationally systemic cyber-resilience alliance will this minority community have the weight of a coherent single actor sufficient to extract peer power accommodation from especially China in the future.

For Chinese leaders, their "rightful place" in the world has always been due to their demographic size as a nation. Acting alone in their cyber and economic defense, individual democratic civil societies will not have the scale across all of their socio-technical-economic systems to enforce restraint on China and its allies.

Or they will also not have the ability to create their own robust cyber power as needed in a systemic resilience and effective forward-targeted disruption manner.

Only an operational cyber alliance can protect these civil societies and their private sector actors from eventually having to concede to the Chinese-led dominant practices of this emerging more authoritarian international economic system.

Fourth, only such an alliance can create the crucially needed transformation of the cyberspace substrate. Together, consolidated democratic civil societies have about 900 million educated citizens that gives them the economic market weight and technological talent pool to face China as a peer power able to sustain robust cyber power, independence and defense in a conflictual cybered world.

Such a unified systemic cyber resilience alliance is feasible. It has the joint market size to engage the private sectors as participants, citizens and defenders of the civil society system on which their collective national economic well-being and their own corporate return on investment defense depends now and in the future.

The alliance can be a large technology innovation engine creating technological transformation of the underlying very shoddy cyber substrate with products built on civil society standards for the like-minded states and the rest of the world.

In conclusion, only in this way can the now global cyberspace substrate be made less hollowing for the democratic civil society: fundamentally secure, fair, transparent, open to global trade, and not so easily remotely exploited for economic advantage and for conflict, and yet still widely generative.

Only this cyber resilience alliance can ensure the jointly sustained robust cyber power at the scale and coherence to be needed to negotiate with the rising authoritarian world, and China, and to ensure equitable rules and acceptable societal well-being in the emerging highly conflictual authoritarian and post-Western cybered age.

Thank you very much.

CHAIRMAN BARTHOLOMEW: Dr. Lewis. It's a tough act to follow.

PREPARED STATEMENT OF CHRIS C. DEMCHAK, PH.D., GRACE M. HOPPER PROFESSOR OF CYBER SECURITY AND DIRECTOR, CENTER FOR CYBER CONFLICT STUDIES (C3S), U.S. NAVAL WAR COLLEGE

Asia Hearing on "Information Controls, Global Media Influence, and Cyber Warfare Strategy"

Testimony before
The U.S.-China Economic and Security Review Commission

May 04, 2017

Over the coming century, consolidated[1] democratic civil societies will be a numerical minority in a deeply cybered and conflictual world dominated by non-western autocratic states.[2] Now well into its rise as the center of economic and demographic power in the emerging post-western world, China has the advantage of an enormous scale in market and resources, as well as a rising momentum internationally as an alternative model and large new ally for existing and rising authoritarian leaders globally. Since the bulk of the world tends toward authoritarian political cultures and structures, China will by all measures be particularly able to channel – if not dictate - the rules in practice across the international system using its deeply embedded regional, economic, and cybered bonds.

While this rise of the 'rest of the world' (ROW) was inevitable, westernized democracies have lost their leadership role in the international system faster and more pervasively than might otherwise have occurred if there had been no – or a different form of – cyberspace. Today's cyberspace is a global societal 'substrate', not a 'commons' or an administratively convenient 'domain'. As such, it critically connects societally essential functions domestically and globally. However, it was built on insecurely coded foundational architectures, widespread utopian misperceptions of the internet, a libertarian corporate commercial fixation that prioritized market access over national or systemic security, and an overarching complacency across western states about the inevitable domination of their vision of democratic civil society and international rule of law. In reality, cyberspace has accelerated intra – and inter-state massive economic exploitation, and reinforced the wealth extraction and societal control of personalized political control across the non-westernized majority of the globe.

---

[1] The term 'consolidated' is used to distinguish a stable, functioning, modernized, democratic civil society from a developing nation recently civilianized, highly corrupt, prone to military coups, or ruled by a single party or strongman, yet which occasionally has what are generously called open elections and thus is labeled a democracy. (Diamond, 1994)

[2] Much of this discussion draws upon a previous 2016 publication. See (Demchak, 2016)

The shoddily built cyberspace, in particular, created and spread a new form of system-vs-system 'cybered conflict'[3] China's scale and its ever growing skill in this form of conflict challenge democratic societies' influence over the interstate system and would do so in any case. However, the democratic civil societies have themselves equally to blame for much of the cyber threats emergent today due to their own blinders and failure to act early and collectively. Today, western states experience between 1 to 2 percent annual GDP loss due to cyber insecurity affecting societal rules, economic resources, and national security capabilities. (PWC, 2014) (Hathaway, 2013) This "greatest transfer of wealth in human history" constitutes the hollowing of the future assets needed for the long-term, agile and effective defense of democratic states. (Paganini, 2013)

This testimony will argue four points about the sources of – and solutions to – these trends now threatening a tsunami of offense and extractive campaigns, to which open democratic civil societies remain especially vulnerable.

Summary Points

> The internet grew up too fast, too cheap, and too shoddy, and now must be transformed with security as equally embedded as freedom speech is assured, and generativity is encouraged. Western utopianism and libertarian IT capital goods industry security-blindness laid the foundation for today's unprecedented system-vs-system "cybered conflict" by changing five fundamental constraints on offensive campaigns in modern conflict: scale, proximity, precision, deception in tools, and opaqueness in origins. Cybered conflict then blended with the routine systemic surprises routine found in all largescale complex systems to jointly impose four layers of complex system surprise unique to the cybered era (single firm, critical infrastructure, huge bad actor community, and small deeply skilled advanced threat groups). With such a poorly secured substrate, a modern state is now a deeply interdependent huge socio-technical-economic system (STES) whose economic vitality and societal stability are exquisitely vulnerable to predators and adversarial states. Only transformation of the underlying

[3] 'Cybered conflict' is a term adopted to indicate the conflict is systemic and so likely to be deeply integrated into conflict in the future that the term 'cyber' should eventually be discarded as redundant. For the moment, however, it is necessary to retain the adjective to keep the fundamental trend in view and in discussion. For its first use and explanation, see (Demchak, 2010)

architecture will change the dynamics to something more manageable and less hollowing for democratic civil societies.

Borders are rising in cyberspace across authoritarian and democratic states, and this trend must be accommodated, rather than resisted by democratic states. While China has adamantly maintained a right to its cyber sovereignty, it has also massively exploited the open borders of wealthier western societies, bringing the intellectual property (IP) advantages in technologies to market and future wealth inside its own more controlled systems. In the face of this reality, western states are domestically installing defenses and controls while denying this reality in public policies and international statements. Western libertarian IT capital goods industry leaders are loudly arguing for zero regulation of their activities in democracies while quietly complying with the technology transfer, privacy denying, or other demands of authoritarian government elsewhere. Our western refusal to recognize rising national jurisdictions in cyberspace for our peculiar utopian and libertarian economic reasons appears hypocritical and has more rapidly reduced the influence of western civil society values. In being so distracted by this losing battle, we encouraged the rise of a Chinese narrative as an alternative story path combining economic success and domestic internet control. We also ignored our own urgent need for a collective resilience narrative – a cyber economic 'stateness' story. Without it, we are unable to coalesce public and private efforts aimed at the protection of our openness and economic vitality in a cybered age. In the interim, the rise of a Cyber Westphalia is changing the topology of the international economic system to reflect more authoritarian internet preferences.

The demographic scale is the major Achilles heel of the consolidated democratic societies in a deeply connected world facing a single coherent and cyber aggressive actor the size of China. Only by presenting a competing, competent, and size equivalent alternate cyber power can these states defend their collective cyberspace and future wellbeing. For China's leaders, this scale is their main argument for their "rightful place' in the world. Consolidated democratic societies are a minority community - relatively few (perhaps 40 at best in a world of 196 countries) and small to medium in average size. As trends stand, China's economic weight, rules demands on smaller partners, and sheer presence will majorly define the preferences of the emerging, highly connected, post-western world. As trends stand today with no coherent counterbalancing democratic weight, the international system will increasingly reflect Chinese business and organizational memes: low transparency, hierarchy of big over smaller, self-censored communication, and highly personalized business practices. (Tan & Tan, 2012) That situation will be reinforced with the rise of a more authoritarian rest of the world connected by Chinese technologies and paid for, run, maintained, operated, and updated by Chinese firms, especially in telecommunications.

Western civil societies operating independently in their own cyber defense of their vulnerable STESs will individually eventually have to concede to the dominant practices of this emerging nonwestern world. Only by creating a coherent functionally integrated and operationally systemic 'cyber resilience alliance' will the minority community of consolidated democracies be able to extract restraint and peer power accommodation on the part of China and the larger number of its fellow authoritarian states. Otherwise, the exchange preferences requiring transparency and impersonal relations of the liberal economic international system will be reduced to mere formalities, if that.

Such an alliance is feasible because a community of at least 900 million citizens will have the economic market weight and the technological talent pool to face China as a peer in a conflictual cybered world. Such a unified systemic cyber resilience alliance can orchestrate its own shared adaptive sensor and mitigation systems, massive R&D programs to both universities and firms, and the economic and technological talent to transform the collective cyberspace. [4] The shoddy substrate can be reformulated to be fundamentally secure, fair, open to global trade, but not so easily remotely exploited for economic advantage and cybered conflict.[5] Such a collectively integrated, coherent 'actor' can provide the framework and urgency to build the necessary civil society stateness needed. Its structure and mission to maintain a unified all sector response actively engages the private IT capital goods sector in the defense of the democratic economic system as team players, citizens, and still globally vigorous competitors. The inclusive responsibility for defense and generativity of all sectors across the alliance is critical. The scale of the authoritarian rise and their national jurisdictions will dismantle the civil society values embedded in the currently liberal international economic system, leaving only remnants of the open internet along with the fair market rules of today. China already speaks of eventually displacing the shoddily built westernized technologies with those said to be less exploitable and destabilizing, including for security pervasive surveillance and content and access controls. Chinese technology companies are globally routinely now in the top three ranks across a host of critical components of the cyberspace substrate. When their preferences in design and production dominate cyber-related markets globally, democratic societies will individually not have the means to secure their own cyber substrate supporting democracy and the transparent, free exchange of accurate, unmanipulated information over the long term. Only with such an alliance can democratic societies afford the necessary

[4] John Mallery of MIT has spoken wide and long on the need for this fundamental transformation as the only real long term survival path open to consolidated democratic civil societies. (Mallery, 2011 (2009))

[5] A number of authors have more recently been speaking out on the need for this kind of 'like-minded' alliance, but few have gone further to give it structure and, importantly, a mission distinct from saving the entire world's internet as this piece argues. For recent works that move in the direction of needing such an alliance, , see (Nye, 2014) and especially the latter chapters of (Segal, 2016).

> large push combining in talent and investment to keep healthy markets with alternative technologies able to transform the basic internet technology at the proper scale to defend the economic well-being of their nations in the future. With these nations capable of acting in unity, they will be to no small extent more cyber autarkic and resilient. In so doing, the consolidated democratic world will create the robust cyber power jointly needed to negotiate with the rising authoritarian world – and China – for equitable rules and acceptable societal wellbeing in the emerging highly conflictual cybered age.

Built Poorly on Utopianism, Security-Blind IT Capital Goods Libertarianism, and Hubris[6]

Cyberspace is widely misunderstood and has been from its outset. It is now a deeply intertwined 'substrate' connecting all the critical components of every nation's domestic 'socio-technical-economic system' (STES), built with fault-tolerant programming and insecure hardware routinely sent too quickly to market with overblown promises of fast returns. Three interrelated cognitive blinders in western approaches to the spread of cyberspace hindered accurate assessments of the emerging reality. These were unrealistic optimism in early utopian cyber visions blended with security-blind IT capital goods business models, and endured far longer than reason would suggest due to deeply institutionalized Western societies' hubris about the permanency and moral superiority of their Cold War legacy control of the international system despite the overwhelming demographic and eventual economic scale of the rest of the non-western world. The 'winners' of the Cold War ignored the reality of their cultural uniqueness. The result was insufficient security concerns for the national wealth in their own IT capital goods manufacturing, and of the possibility that the international system they created could be contested and bested by the scale of dedicated, rising adversaries.

Built Fast, Cheap, and Shoddy

From its commercial outset, cyberspace was built fast and cheap in order to create a widely overpromised prosperity as quickly as possible. In the early 1990s after almost three decades of development built in and for universities by public funding, cyberspace emerged for public and commercial use as the "internet". (Hafner, 1999) It was already embedded with the ideology of a public good thereby meant to be free and benignly useful. Sharing the technological developments and access openly across universities became a social presumption embedded as intrinsic and inevitable for the generation of new ideas, languages and software.

---

[6] This section largely draws upon (Demchak, 2016)

Security was an afterthought, The time-consuming, fault-intolerant coding languages used by academics were hard to hack in any case and the early networks connected to relatively few and well known small communities.[7] Furthermore, concerns were limited because early cyberspace did not uniformly connect everything important as it would grow to do twenty years later. Its challenges were unreliable transmission, some cybercrime, and possibly sociopathic organizing. (Rochlin, 1997) The bigger concern was just getting the sharing of the electronic 1's and 0's to be reliably transmitted across often poor electric lines. (Kinnersley, 2015)

Despite its reality as a man -made, -owned, -maintained, -updated, and -monitored, the internet spread with this presumption of being intrinsically an open, unfettered portal to access freely shared, objectively true data called 'information.' Even though the 'world wide web' spread commercially by 'Internet Service Provider' (ISP) firms as a 'peer or pay'[8] system of access, it acquired a new name – "cyberspace", and was promoted with acquired almost mystical properties.[9] Barlow's 1996 "Declaration of Independence for Cyberspace" declared all networked individuals to be 'netizens' beyond the reach of governments. Not by declaration or any necessary act by those individuals, but by simply entering into this connected world of such complexity and connectedness that no bureaucracy could succeed in controlling it, netizens thus freed themselves of any legacy societal constraints. (Barlow, 1996) Other and academically credible scholars said this new cyberspace would produce a world in which laws emerge from the collective consciousness without governments or national boundaries. That vision of no government presence in cyberspace became deeply embedded and continues to be subconsciously endorsed today as a basic framing — that this new digitized world village would be inevitably a universally benign, freely shared, implicitly democratic and government-free global space for good, uplifting all who connected into it.[10] (Norris & Jones, 1998)

---

[7] In 1995 and 1996 access to sites were shut down in Germany due to German laws on pornography and Nazi sympathizer materials. (Hughes, 1996)

[8] Peer or pay means that ISPs or other nodes will only pass through another node's internet traffic on contractual terms, either freely as a peer or with agreements about how the transiting node is to be paid to move the traffic along. For a truly enlightening explanation of how this otherwise ignored reality of the internet operations, see (Blum, 2013).

[9] The problem of not knowing the basics about the global web continues, even among those charged with making highly consequential national policies. In 2011, at a senior level cyber policy conference, several senior US individuals offered deeply felt suggestions about governance of cyberspace. Later in the same conference, they confided to me that they did not know how the internet was actually constructed. (author personal observation) See also Singer and Friedman's 2014 book intended to try to compensate for this appalling ignorance. (Singer & Friedman, 2014) The difficulty is that this and similar books are emerging now – twenty years on – after the developments outlined in this paper are already well advanced due in large measure to the early and widespread levels of ignorance about cyberspace as a socio-technical-economic system.

[10] Arguments for access to Wi-Fi broadband as a basic human right equivalent to the right to existence are highly normative. (Tully, 2014) (Oyedemi, 2014) A variant argument is that access to ICTs is an 'instrumental' human right. (Barry, 2014) See Cerf's cogent rebuttal.(Cerf, 2012)

As the computer industry fed the emerging internet frenzy through the 1990s, however, commercial interests were -- unlike their academic colleagues -- both impatient and proprietary. (McCarthy, 1978) (Mathur & Singh, 2013) By the early 1990s, the demand from the private sector to fund and therefore use these network tools for commercial purposes was overwhelming. The National Science Foundation -- the last official guardian of the otherwise publicly sponsored internet -- opened it up to private carriers fully by 1994. (Frischmann, 2001) From then on, the influence of commercialization on the dominant design of the web was profound. Those more secure established (1960s on) academic languages such as LISP – lengthy to code and intolerant of faults - were seen to take too long and consume too many resources for commercial revenue returns. (Trickey, 1988) Funding flowed to those computer scientists migrating from the earlier less hackable languages to those that could tolerate mistakes in code and yet perform their intended tasks, such as C+ (1990s on). (Wexelblat, 2014) With the rise of commercial interests, entrepreneurs such as Bill Gates wanted to a healthy return on his investment in software. He did not want to make sure programs were perfect before selling them -- DOS stands for 'Dirty Operating System' -- nor to have code shared widely before a return on investment could be achieved. (Rosenzweig, 1998)

The result was a commercialization tsunami with an IT capital goods business model that emphasized the rapid factory-like production[11] of standardized, fault-tolerant (more easily hacked) software getting to the market as quickly as possible.[12] (Houidi and Pouyllau 2012) Beyond login passwords to keep account ownership clear, security concerns were still chiefly reliability of performance, safety of transmission of bytes, and design efficiencies in production for the emerging markets across the US and Europe. (Anderson, 1994)

The utopian vision of a new free world of ideas and collective virtual freedom flowed readily into the commercial world of university graduates and self-taught talent, but the emerging IT capital goods industry was not particularly concerned with the imputed democratization-spreading aspect of cyberspace, only with the aspects that promised freedom from government regulation of their activities, markets, and products. Their libertarian IT capital goods industry business model was widely promoted as benign, efficient, and uniformly economically advancing for everyone. Building on a general ignorance of the techniques and physical realities

[11] The phenomenon of employing a large number of young programmers to whisk out standardized code as fast as possible – with the plan to fix 'bugs' later -- was particularly attributed to Gates' Microsoft with its factory like cubicles and tasks of young programmers called 'Microserfs". (Coupland, 2004)

[12] Often overlooked is the role of globalized mass production in enabling cyber predations in particular. The standardization so essential to the business model of major IT capital goods corporations such as Microsoft played a significant and role in the exceptional broad number of targets and elevated levels of economic losses to nations today. (Geer et al., 2003)

underpinning cyberspace, the technically skilled in the IT world argued repeatedly that only they alone could produce the global prosperity promised in the new internet age – and only if government in particular never – ever – regulated their industry. The view blended with the utopian view that governments would wither in any case with the rising democratization to inevitably follow as people joined the internet. Quickly enough as e-commerce was promoted and enthusiasm to modernize spread, that view became taken for granted across the digitizing western civil societies' public and private communities.

For the next twenty years and until reality could no longer be ignored, western political and economic elites would determinedly argue that the Internet and all its technological designs and development were to be completely open and unfettered by regulation – in particular, something that governments and borders should never touch. (Rosenzweig 1998) The threat was that, if the regulators were allowed to inhibit the freedom of the web, its prosperity – even its generativity -- would be lost.[13] Westernized communities came to view the open internet's economic benefits as explicitly tied to a lack of government controls for any reason. As a result and irrespectively of the opposition – to include a rising China, western public and business elites vigorously argued against erecting national jurisdictions across cyberspace as economically daft as well as morally unacceptable in this new cybered world.[14] (Lessig, 2004(1998 original)) Until as recently as 2011, those in the open internet community still dismissed evidence of bits and pieces of cyber national borders emerging unstoppably across cyberspace.[15] (Betz & Stevens, 2011) This devout fixation on keeping the internet globally universally open and operating along idealized democratic civil society values, however, began over time to founder on the reality that, even for unrealistic utopian visions or libertarian commercial interests, the Internet itself was simply built badly.

---

13 The embedded nature of this threat – the loss of economic innovation if the internet's libertarian path is disrupted – continues today, especially among the more technical thinkers and practitioners. For example, ""if ISPs, diverge from the Internet tradition of the open neutral platform .... It might reduce the rate of innovation, reduce the supply of content and applications, and stall the internet's overall growth." (Clark, 2010) For an interesting nuanced concern, Zittrain cautions against the loss of human gatekeepers able to balance both generativity and security, and the potential for the rise of regulators to dampen both in the name of meeting consumer calls for security. (Shema, 2010)

14 Buried in the thinking of even the more libertarian scholars is the notion that, while one must be left alone to use cyberspace as one likes, that use must nonetheless be standardized under open internet western rules. Clark for example argues for understanding of the developing world's "different governments with different cultures and rules and regulation, different users with different skills, … onto which we will try to impose uniform Internet standards." (Clark, 2010)

15 It is interesting to speculate whether, had this new world been content to stay under the regimes for which its legal and value presumptions were appropriate, the web might have remained within these states as a communally shared resource subject to reciprocal laws, conveyances, and mutually agreed upon limits to surveillance for privacy reason.. (Langheinrich, 2001)

Rather than democracy and ubiquitous prosperity, the rapidly coded, more easily hacked programming languages creating the globally open cybered substrate offered five distinct advantages in offense that had historically only been available to emperors or close neighbors. With nearly free access to the web, predators en masse and large or small could without fear of punishment create large scale in attacking organizations (or botnets), get globally close in proximity for intelligence or reach purposes, and choose among unprecedented ranges and levels of precision in their remote operations – all for any reason including whimsy.[16] A massive underground global cybercrime market then developed with specialized submarkets, warranties, and tools including services to further enable these bad actors – and to employ them in servicing other predators. (Glenny, 2011) Two more cyber-related advantages emerged: deception in tools and opaqueness in origins. Now malicious actors could both obscure their tools – thereby using them again in a variety of other choices while avoiding the quick development of counter tools – but they could also hide themselves across nations, buried in the flood of the global web and avoid having their own local systems hacked back in punishment.

Soon enough, the underground cyber criminal community also hosted governments and transnational criminal organizations that joined into the global hacking for information, money, and political or economic leverage.[17] Over the course of the first twenty years of the global cyberspace, a dizzying variety of predators and adversaries for a wide range of reasons emerged to threaten any open and digitally advanced nation's entire inventory of critical largescale 'socio-technical-economic systems' (STESs) and – in the process – the nation's long-term economic vitality.[18]

Over this frontier era of cyberspace, hacking has risen to such scale that digitally connected nations now face four layers of complex systems surprise. In the precyber era, states had to deal with systemic failures in two layers: first, surprises disrupting in very large, single enterprises critical to the nation, and second, rippling failures across connected sets of critical infrastructure enterprises. For thirty years, scholars in the largescale technical systems (LTS) field studies those complex surprises and even developed a set of standard responses. (Comfort,

---

16 For a longer discussion of these systemic advantages, see (Demchak, 2012)

17 The global underground cybercrime black market is about 80% mid and low skilled actors who ticker with or use someone else's software program. The last 10-15% are the truly skilled coders – the 'wicked actors' – employed by states or transnational organizations and so good that they will get through most defenses. This group includes the so-called "Advanced Persistent Threats" (APTs) generally associated with espionage, but the wicked actor group is larger because of the transnational sources can be both focused on crime as well as espionage. (Demchak, 2012) (Juuso, Takanen, & Kittilä, 2013) (Singer & Friedman, 2014)

18 It is important to note how very recent is the realistic possibility of connecting every process to the internet and, thus, how disrupting to existing social systems. (Kopetz, 2011)

Boin, & Demchak, 2010) These challenges were large enough, but at least they were bounded by national borders. With the advent of the globally open, easily hacked cyberspace substrate, however, two more and much more poorly understood or studies major sources of national systemic surprise erupted into national systems. Now the STES digitally connecting a whole nation faces a third layer of surprise in the continuing tsunami of cyber assaults by large masses of middling skilled bad actors from across the world exploiting the five advantages of scale, proximity, precision, deception in tools, and opaqueness in origins from around the world. A fourth layer of systemic surprise developed from that huge community of malicious actors to produce a much smaller number of exquisitely skilled 'wicked' actors.[19] Their coding and hunting skills and dedication are so elevated that they are usually called 'talent' or 'advanced persistent threats' and almost always employed by criminal organizations and governments. (Demchak, 2012) (Juuso et al., 2013) (Baskerville, 2006)

Together these four layers of complex system nasty surprises and the five offense advantages helped hasten the decline of their hosting democratic civil societies. Although not recognized clearly as such, they have helped derail the promised prosperity and benign tolerance promised by the early utopians and imposed an enormous large societal cost to securing the economic wellbeing of the western states who originated cyberspace. Even what was once the dominant superpower – the United States – has found it does not have the resources to simply absorb or repel the daily onslaught of attacks by state and non-state actors.[20] Major corporations began recognizing – and finally admitting – major information losses. Some, such as Canada's Nortel, went bankrupt after theft of their critical intellectual property.[21] After only two years in office as the Director of the National Security Agency, General Keith Alexander in 2012 called the losses in intellectual property and future market returns "the greatest transfer of wealth in human history." (Paganini, 2013) The Netherlands discovered in 2012 that its 2010 GDP growth had been halved by the costs of cybersecurity and the market losses associated with the massive intrusions.[22] According to a 2014 PWC report for 2014, given the World Bank's estimate that

[19] Often called APTs or Advanced Persistent Threats because they are usually working for a transnational criminal organization or a government. See for example (Mandiant, 2013).

[20] (Richmond, 2011; Schrage, 2011) (Goodin, 2010) (Brian, 2010; Liff & Erickson, 2013)

[21] The Nortel Corporations bankruptcy is a major and clear case of this kind of slow roll of national knowledge stocks. Nortel went bankrupt in 2009, having been exploited by the Chinese firm Huawei in 2006-2007 due to cyber extractions of critical data, and then beat to the broadband wifi market for which Nortel was preparing its major and existential launch. In 2010, the CTO of the former Nortel was publicly listed as working for Huawei and seeking small technology startups for Huawei 'investment'. (Rogers & Ruppersberger, 2012) (McGregor, 2012) Hacking is increasingly so sophisticated that, despite the massive growth of the commercial cybersecurity industry, on average nearly a third of attacks penetrating into an organization are unstoppable. (Lumension, 2015)

[22] Melissa Hathaway, talk prepared for and delivered remotely to cyber expert workshop, at the US Naval War College, September 2015, Newport, RI.

the entire globe's GDP totaled $75 trillion in 2013, then the losses of trade secrets and therefore future earnings could range as high as $2.2 trillion. The effects are concentrated so far in westernized nations, shaving as much at 1% to 3% off a nation's annual GDP. (PWC, 2014)

Western Hubris Delays Recognition of Changing Reality

That the reality of this shoddy construction and mounting economic losses could be ignored for almost twenty years is due to as much to an enduring western hubris fixated on the inevitability of entire world evolving along the western model, as it was to the strong utopian-libertarian blended vision of cyberspace. The peculiarly western presumption that the end state of all societies would be a democratic civil society carried on in the development of cyberspace, allowing major actors to dismiss as mere cybercrime the economic costs of unprotected resources being hacked or manipulated by organized and government-paid foreign bad and wicked actors. A disinterest in economic statecraft prevailed as well, due to an equally firm presumption that the liberal western international economic system was now so firmly ensconced that no one – no rising power of any size – could significantly overturn it. (Mastanduno, 2012) (Blanchard & Ripsman, 2008) (Demchak, 2013)

So strong was this presumption of both immortality and dominance of western governance preferences that international institutions such as the World Trade Organization (WTO, formerly GATT) became - over the western dominated era of the Cold War and aftermath - the forum in which states misbehaving economically were to be corrected. No longer would victim states need to individually engage in their own economic statecraft to change another state's bad behavior according to collectively agreed upon rules for membership. For example, while it was known that China did not meet the basic requirements to enter the WTO in 2000, the nation was nonetheless admitted to membership with this underlying presumption that even a nation the size of China must as a matter of course eventually submit to the western economic rules. (Blancher & Rumbaugh, 2004) The presumption prevails today even though the reality says otherwise. To date, China has not met its own promises to fulfill requirements, and yet there is no discussion of ejecting the state. (R. D. Atkinson & Ezell, 2015)

This underlying western complacency about democracy has served to reinforce the utopian-libertarian conflation of conflating democracy and a lack of any government intervention in cyberspace. The three parts of this combined logic is that democracy is the inevitable end-state of all nations, an open internet inevitably democratizes any using state as long as governments leave it unfettered completely, and that any government enforced rules on IT

capital goods industries will 'balkanize' their internet (i.e., IT markets), destroying thereby its democratizing effects along with a nation's prosperity in a digital age. (Wrobel, 2013) This deeply ensconced logic has for twenty years, in particular, strongly reinforced western communities' collective opposition to legitimizing any national borders in cyberspace. (Kroker & Kroker, 1996)

With the utopian vision, libertarian IT capital goods business model, and the embedded western hubris as a trifecta, democratic governmental responses to cybered threats have been weak, derailed onto ineffective international institutions, and particularly vigorously opposed to having separate national cyber jurisdictions. The latter in particular has been held up for derision and rejection across multiple fora. (R. Atkinson & Brake, 2015) In response to data on massive cyber extractions and rising defenses, many internet governance-related forums -- GFCE, IGF, Global Commission on Internet Governance, NETmundial Initiative, WSIS, WCIT, and the GCCS 'London Process'– have nonetheless redoubled western pressures for nations to be more open to the global internet and more law-abiding, for example, applying international liberal rules internally in cyberspace. A major example is the strong push for Chinese acquiescence to United Nations (UN) human rights applied to cyberspace internally as part of the future cybered world system – a demand that China vigorously rejects as intrusion on its national sovereignty.[23]

This consistent and seemingly immutable opposition to the internal governance concerns of the authoritarian leadersenergized a major rising actor of enormous relative scale, China, to work actively internationally and economically to counter western presumptions about democracy, economic international rules, and – especially – national cyber jurisdictions. The reality is nonwestern, authoritarian actors are rapidly moving onto center stage led by China accelerated the trends in economic and international influence losses. That rise was inevitable over time, but the West lost purchase more rapidly over the international liberal economic system it built and enforced because of its own invention – the internet. Fighting the rise of national control of jurisdictions in cyberspace has distracted civil society governments and – especially -major western economic actors. They failed to recognize the indicators of a waning era of western dominance and its liberal international economic system with universal enforcement of fairness, transparency, impersonalization, and legal recourse in economic exchanges. In short, the western nations built the internet badly, viewed it inaccurately, and have proven slow to defend it – or their own long-term economic lifeblood – for over twenty years.

[23] These are, respectively, the Global Forum on Cyber Expertise, the Internet Governance Forum, World Summit on the Information Society, World Conference on International Telecommunications, Global Conference on Cyberspace, among many others.

Cyber Westphalia Rises amidst Resurgent Authoritarianism for a post-western International System[24]

Cyber borders are rising globally nonetheless. The forms are varied, some in the form of tightening technological, ISP, or policy controls on traffic transiting existing national borders, others in the form of increasing monitoring and removing or rejecting of suspicious traffic that has passed into national servers, and yet others in the form of indirect access and content controls executed through controlled browsers, subscriptions, or identification tagging and logging. (R. J. Deibert & Crete-Nishihata, 2012) However much the western states have fought for an open and unfettered cyberspace, consolidated civil societies are also now creating – if discordantly – domestic filters, gateways, and policies for the cyberprotection of their citizen whose lives depend on the poorly secured cyber substrate.(P. J. Dombrowski & Demchak, 2014) Along with other authoritarian states,China never gave up its control on internal communications systemsand is now reinforcing its national cyber borders with newer technologies. Quite often these newer systems are built through the purchased compliance – some might say 'hypocrisy' – of many western IT capital goods firms captivated by the size of the Chinese market to which, ironically, they are never given the free access they expected in return.

China's scale, presence internationally and ability to offer technological benefits have developed a new persuasive – and nonwestern – narrative about national cyber sovereignty as possible with economic prosperity. That is, as demonstrably shown by the Chinese rise, adding borders does not 'break' the internet and destroy its generativity as western policymakers and technology private sector leaders warned. Overt and latent authoritarian national leaders have been emboldened as a result, and the Cyber Westphalian world is emerging rapidly.

Dismissing China's Cyber Sovereignty Accelerated Trend

Since connecting to the global Internet in the mid-1990s, China's spokespersons have consistently made its sovereignty expectation explicit – including across the internet. (Whiting, 1996) Other authoritarian leaders during the 1990s often conceded to demands for internet openness in return for the promised big economic payoffs, but China was among the earliest of the authoritarian states to clearly want both the economic benefits of an internet and a controlled internal communication system. (Kalathil & Boas, 2010) Most importantly, it was clear to

[24] Much of this discussion is drawn from (Demchak, 2016)

Chinese leaders that avoiding any democratizing effects of the internet would require central Chinese control of its own – sovereign – web. (Qiu, 1999) (Gresh, 2008)

Even before cyberspace, this kind of pushback against the unacknowledged western hubris has never been easy. (Goldstein, 2015) From the Chinese point of view, western governments and civil society promoters consistently have refused to consider – let alone accommodate - the Chinese sovereignty demands on a host of issues for at least a hundred years, expecting democracy to break out at any moment. [25] (Bradley, 2015) For cyberspace, western political and economic leaders regarded the Chinese position as hopelessly out of date, inefficient (libertarian demand for no government control), morally wrong (access to the internet approximates a human right), and contrary to the path of history leading to a world of democracies. (Skepys, 2012) (Kalathil & Boas, 2010)

Chinese frustration at the western opposition was understandable. Given the Cold War's history with the UN in particular, the leaders of China, Russia and many other non-westernized leader could reasonably have expected that sovereign rights of a nation would be upheld for cyberspace. (Duara, 1997) Unlike space, for example, it is completely a man-made underlying substrate relying mostly on undersea cables connecting one nation's sovereign soil to another's equally sovereign territory.[26] (Blum, 2013) No one questioned the right of a nation's government to demand that transnational corporations entering that nation adhere to the local national laws in terms of taxes, environmental rules, or even human relations in hiring and firing. Indeed, linear feet upon linear feet of shelves in western book stores hold many volumes on international management and business describing how western businesses seeking to operate abroad must abide by the other sovereign nation's laws. In no other industry not directly involved in war (such as nuclear weapons) was a nation's demand for sovereignty so simply dismissed. After all, the UN – a foundation of the post-WWII liberal international system and its basic multilateral character – has routinely upheld national sovereignty. (DeNardis, 2014) If one was not taken with the optimism visions, swayed by the economic libertarianism, or imbued with western

[25] Western hubris is deeply embedded in scholars regularly declare Chinese resistance to western preferences as transitory. (Peerenboom, 2006) They have for over a century interpreted a wide variety of phenomena as indicators of progress towards the inevitable civil society model. (Bradley, 2015)

[26] Many cyberspace policymakers, pundits, and civil society promoters do not really know the structural and contractual basics about the global web. Such folks are often resistant to discussing the physical aspects of technology, as though it did not matter for a largescale socio-technical-economic system such as cyberspace. Singer and Friedman's 2014 book was intended to try to compensate for this appalling ignorance. (Singer & Friedman, 2014) The difficulty is that this and similar books are emerging now – twenty years on – after critical early perceptions and policy paths were already well advanced.

hubris, expecting sovereignty to be more or less automatic is a reasonable opening position, even for cyberspace. (Qiu, 1999)

By 2005, after roughly ten years of requests for sovereignty repeatedly rebuffed, the Chinese response was to strengthen its international campaign to alter the global narrative to accept national sovereignty in cyberspace. By this time, China's leaders had relatively better reasons to expect their campaign would be successful. For the first time since the 1990s, China was developing the economic weight to muster forces internationally and bilaterally against this western dismissal of their demand for cyber sovereignty. This campaign focused on using the influence and visibility of particular major institutions in the current international system, such as the ITU (International Telecommunications Union, hosted by the UN).[27] (Yong & Pauly, 2013) By 2011, China's leaders had positioned themselves and some allies in key influential positions in international technical organizations, and across critical IT and related markets.

Nonetheless, after another ten years, by 2015, an international endorsement of China's cyber sovereignty – let alone any other state's – by the international community still has not formally emerged. The prestigious 2011 GCCS 'London Process' international internet governance meeting, for example, once again endorsed open Internet as a human right inside every nation. For the Chinese, these western internet governance blind spots do seem to reflect a cybered form of the deafness of imperialists.[28] "America spreads the ideas of democracy widely across the world, but in cyberspace, it's the opposite," [Hao YeLi, former PLA senior official 2015l] said. "The United States continuously maintains a system to monitor the rest of the world but asks other countries to strictly control themselves and remain within bounds. This unsymmetrical line of thinking continues." (Mozur, 2015) The 2016 statement by the UN's Group of Governmental Experts (GGE) for cyberspace has come the closest, but it is far from what is needed to internationally recognize a nation's cyber jurisdiction as a state's territorial sovereignty is accepted.[29] To add to the frustration, the civil society utopian promoters have since moved the terms of the debate in fighting a rearguard battle to build another obstacle. Internet governance conferences – not sponsored by China, close allies, or the UN -- now elevate the moral and efficacy value of 'multi-stakeholder' meetings -- involving states, commercial

---

[27] The campaign includes exploiting the grey areas in western rules of law to benefit Chinese corporations or avoid punishment for infractions, a variant 'lawfare'. (Dunlap Jr, 2001) (Brink, 2013)

[28] This inability to accommodate the concerns of developing – read 'lesser' – nations is of very long standing, not only in cyber issues. (Hill, 2014) (Bhuiyan, 2014)

[29] See for example "New International Cyber Rules Likely Off the Table for UN Experts Group" at http://www.nextgov.com/cybersecurity/2017/02/new-international-cyber-rules-likely-table-un-experts-group/135193/

interests, and civil society groups in governance – as equal to or better than the 'multilateral' state level meetings traditionally held by the UN.[30]

As of now, the Chinese narrative has hardened publicly against the combination of cyber utopian vision, libertarian economics, and westernized concepts of civil society. (Zheng & Lye, 2015) Not only are they determined that China will have its own cyber sovereign borders, but so will other states to the extent that China's economic and international political power can ensure. China's pragmatists have expected and planned for conflicts with the US on economic, information, institutional, and cultural fronts, seen as an inevitable outcome when a current hegemon resists being displaced. (M. Liu, 2015) (Zhao, 2015) Accordingly, in the past, they muted the public challenge to western disrespect of China's rightful place. In the last few years, however, Chinese senior political and corporate leaders have escalated their aggressive use of rising economic power in cyber and other arenas. Along the way, China's political and economic leaders have learned to exploit the impunity benefits and "Teflon" legitimacy of a near superpower with a very large attractive internal market. (Rowley, 2010) For example, Chinese leaders see the 2015 Obama-Xi agreement regarding cyber-espionage as support for China's Rising Great Power narrative. Without any enforcement mechanism, the largely symbolic agreement depends on the decisions at any given moment by each party to do – or not do – as they promised. In the Chinese view, its general tolerance of poor behavior internationally constitutes the kind of accommodations made between peer great powers, (Hao, 2015)

The wider, more assertive narrative relentlessly uses the rise of China as a future great or super power to rationalize its right to question the current international system's governors. (X. Li & Shaw, 2014) The apparent objective is to influence changes in cyberspace producing a structure more convenient – or at least less threatening – to Chinese national preferences. (DeNardis, 2014) With the new narrative and its clear demonstration of an authoritarian state controlling its internet and yet rising dramatically, China's public and commercial leaders and thinkers now see an opportunity to advance more quickly and are moving to seize the opening, and bring a good portion of the nonwestern world along with them. (Kallio, 2015)

---

[30] The term 'multistakeholderism' is a term becoming widespread, emerging first during the ICT driven globalization surge from the 1980s- mid2000s. (Lund 2013) A strict read of democratic theory would find it odd that civil society activists would demand non-elected leaders of large corporations be given a seat in deciding the rules of interstate commerce, politics, cyberspace, and by extension, the tools of conflict. However, the key characteristic of the cyber utopian vision is its blending of individual freedoms with economic libertarian freedom and the presumption that a cybered world's prosperity depends on both of them absolutely. (Calandro et al. 2013) Ironically, however, for the IT capital goods industry, these borders and values issues are not linked. The business models only require no governmental restrictions in markets, not universal freedom of speech, and that is also fungible. Many major IT corporate leaders concede to Chinese requirements for technology transfer or surveillance compliance. (Tan and Tan 2012) (Jiang 2012) (Shih, 2014)

Rising Cyber Westphalia to be led by Authoritarian States

As China's narrative gains prominence and adherents, its influence rises globally. . While western states' foreign policy circles continue to fight the Chinese narrative on cyber borders, by 2017 cyber borders in praxis are being grudgingly and indirectly accepted. A wide variety of Western documents -- including the widespread rise of national cyber security strategies – recognize a government's obligation to protect their own national cyber jurisdictions. For example, when developing nations' leaders allow the Chinese firm Huawei –to build and operate their national telecommunications public agency's critical national 4G networks for nearly no upfront costs, western states are fighting a battle that they have already effectively lost. (Gagliardone, 2015) (Chung & Mascitelli, 2014) As the Chinese have argued, each bilateral agreement that acknowledges the responsibilities of another state in the parts of cyberspace connecting within their established national territory is one that in effect acknowledges the existence of national cyber jurisdictions. (J. Liu & Deng, 2010; Rowley, 2010)

Furthermore, the Chinese model of societal information control and their wider neo-capitalist business practices have a powerful resonance with the rest of the non-westernized world. (Chen, 2001) Authoritarian leaders were never enthusiastic about unfettered communications access for their citizens, yet the past twenty-five years have been difficult in terms of their national cyber sovereignty. Initially to maintain their control of societal behavior, these leaders would centralize and manage national communication networks and content, such as telephone, telegraph, and postal services, as well as radio and television. Although it would have been natural for these leaders to simply refuse the openness of the western internet, the western model of economic advancement seemed to be the only alternative to staying poor and exploited. The post-Cold War era had brought with it an international movement for to rapid economically advancement. One heavily promoted path was through the 'information revolution, especially the modernization of their aging telecommunications systems in accordance with the dominant memes of an international system guided by the economic and military dominance of the western democracies. (V. Schneider, Fink, & Tenbucken, 2005)

The nonwestern and many westernized nations accepted the orthodoxy the early internet narrative – that if they removed government controls and privatized their centralized, government owned telephone-telegraph-post agency, money would flow into their economies. (Baran, 1996) Many countries gave their agency a more commercial name with reduced formal government control, and opened up to westernized models of internet and then cell phone service. (Frischmann, 2001) Authoritarianism is the norm in political structures throughout

history, especially if societies grew large and concentrated enough to requiring organizing many unwilling denizens against environmental and political challenges likely to destroy the society or, more often, its ruling classes. The approach seemed to have worked over centuries despite the lack of a civil society or human rights sensibility. As a result, many nonwestern cultures with deeply embedded authoritarian roots are better seen as finding more security in their own – rather than western civil society – political structures. (Swyngedouw, 2000) However, in the democratizing fervor of the early internet years, these nations and their leaders were not offered much of a middle ground in the western vision of the universally democratizing global cyberspace, not even the option to be sovereign within their own networks.

Although the last twenty years have been filled with noble echoes of the western views of the open internet –largely in the UN speeches -from China, its desire for surveillance and control of its citizens on the web has received support among non-western states. (R Deibert & Villeneuve, 2004) What the westernized societies interpreted as acquiescence to their democratized world view during the 1990s was really authoritarian leaders waiting to see how and when it would be safe to return to controlling their internal communications systems as they chose, without sacrificing economic gains. For example of this holding pattern, while declaring itself a democracy in the 1990s, Russia never dismantled SORM, its central communications monitoring system.(Soldatov & Borogan, 2013) Other states only superficially disengaged their governments from control of the underlying cables or telephones running the new cyberspace.

China has provided an alternate model of success to the one advanced by the western countries, a strong voice against western domination in international institutions, and alternative sources of technology and capital more suited to the desires for surveillance and interception of leaders with authoritarian tendencies. With Chinese support, they have the option of operating more aggressively on their internal internet, confident of relatively strong similarly-inclined allies outside the western dominated institutions and norms. China now routinely promotes itself in a ‘globally noble’’ argument to collect allies -- that the whole of the internet does not serve the equity and rights of all nations.(Bhuiyan, 2014) In response to the publicly stated western expectations that cyberspace will democratize a using society, the Chinese narrative accentuates the instability and greater dissent that can accrue with a border-spanning open internet. (Cui & Wu, 2016) It is clear unfettered public dissent can prove unhealthy for authoritarian or semi-governed states and their leaders, and this common security argument can produce allies despite apparent geostrategic differences. In 2011, Russia joined China in proposing an “International Code of Conduct for Information Security”. Despite the document’s resounding rejection by the

West, its language formally expresses the basic desire for absolute sovereignty to be the governing principle of the international cybered system. (Farnsworth, 2011)

China's narrative also includes as legitimate sovereign cyber actions a wide range of national online societal controls online from internet surveillance to the shutdown of the domestic web as needed. Known for cutting off neighborhoods, bars, websites, and services, China prominently cut off a province in 2009 for six months in response to unrest. Its narrative clearly considers this policy to be within the sovereign right of a nation to do so. (MacKinnon, 2011) While many developing authoritarian or unstable nations duly privatized their main telecommunications agency in the 1990s, they are now rediscovering that they may nonetheless use the central position of these telecommunications firms for online censorship, access control, surveillance, throttling of traffic, or outright cut offs of whole population segments .(Ronald Deibert, Palfrey, Rohozinski, & Zittrain, 2012) Sometimes it only takes phone calls as happened in Egypt in the Arab Spring. [31] (Shin, 2015) Increasingly, however, national leaders are acquiring the technological means to selectively target whole regions to isolate from the internet. (West, 2016) In 2017 between January and April, Cameroon cut two regions from the internet for 94 days to quell dissent by the English speaking 20 percent of its population against the imposition of the French language in schools and courts.[32]

This pattern – inconceivable when the global web was solely a western reserve – is growing especially among nations more inclined to authoritarian rule and cyber sovereignty. Afrinic (one of five global IP address block allocators) has tabled a proposal to punish governments with no new IP addresses if governments execute a shut down. The measure has little chance of being adopted in the next Afrinic meeting in June 2017 in Kenya.[33] China, India, Russia, Kenya, and others nations are opposed. With the Chinese telecommunications giant Huawei building much of the critical cellular communication structures of Africa and bringing a Chinese perspective on the extent of technological sovereignty these nations should enjoy, few of the continent's governments need choose in advance to give up the right to use that technological lever if they see the need.[34] Huawei – as well as not a few 'flexible' western IT capital goods firms – will build these options into the communications backbone of a nation if so desired. In

[31] It is a mistake to underestimate the negative demonstration effects on authoritarian or beleaguered political leaders when they consider the longer term consequences of a cyberspace-enabled Arab Spring–like dissent movement. (Stewart, 2013)
[32] For a set of articles on Cameroon, see https://techpoint.ng/2017/04/24/cameroon-government-restores-internet/) and (http://www.pewglobal.org/2015/04/15/cell-phones-in-africa-communication-lifeline/.
[33] See https://www.theregister.co.uk/2017/04/12/no_ip_addresses_for_countries/
[34] See http://www.cnn.com/2012/10/04/tech/mobile/africa-mobile-opinion/ and http://www.thisisafricaonline.com/News/Huawei-looks-to-Africa-to-cut-network-deals?ct=true

addition and at the moment, allying oneself as a closer friend to China – as opposed to the United States in particular – tends to reward a national leader with Chinese promises of infrastructure investment in large amounts – as the leader of the Philippines has recently demonstrated.[35] (Duanmu, 2014)

At the end of the day, borders ARE rising as defended cyber jurisdictions across authoritarian and nonauthoritarian states, with even the formally opposed western democratic civil societies building their own cyber borders in bits and pieces. Despite the formal foreign policy language of western states still strongly calling for a globally free and open borderless internet, the domestic policy language of concern by westernized government is now riddled with references to defending their domestic cyberspace, rising from highlighting solely cybercrime, to more broadly critical infrastructure protection, and now to losses to the entire economy over time. Among most major western states, cyber security is now labeled a tier 1 or national threat.[36] Even nations known for their civil society—Sweden for example – have taken steps domestically to monitor[37] what enters or leaves their national territories networks – i.e., to defend their domestic cyber jurisdiction.[38]

However, the reality of an emerging global cyber Westphalia is not being framed in values or conflict potential by the bits and pieces of cyber jurisdictions being constructed in these democratic societies. Rather, due to the western states being distracted, obdurate, complacent, and arrogant for the first twenty years of cyberspace, Chinese technology companies, economic tradecraft, authoritarian sovereignty narrative, and international institutional successes are constructing the emerging world of cyber-bordered states that will create a new topology distributing power across the globe.

---

[35] See http://www.straitstimes.com/asia/se-asia/duterte-plans-to-diversify-economy-with-heavy-china-aid

[36] The United Kingdom is arguably the first major westernized state to declare cyberspace threats to be in the top tier of national security threats. (Norton-Taylor, 2010) The tier language has become a cross-Atlantic term of art indicating the level of importance a state attaches to defending itself in cyberspace.

[37] It is important to note that filtering is not the same as monitoring. The former removes data access; the latter notes the data's movements and possibly the content. Another way to view the difference is to note that NSA has been accused of monitoring, while China is shown empirically to filter. (Greer, 2010) (Xu, Mao, & Halderman, 2011)

[38] The law assigning this mission and authority to the Swedish Federal Police passed in 2008. (Irion, 2009)

Defense in Scale through Cyber Resilience Alliance[39]

Scale in demographics and markets is the Achilles heel of consolidated democratic civil societies, especially in today's cybered conflict and particularly since they are so doggedly unable to recognize it. The post-Cold War legacy inability to recognize the power of scale in system-vs-system conflict is particularly dangerous for the future wellbeing and global influence of modern democratic civil societies. As the borders of cyber jurisdictions rise in a Cyber Westphalian world structure, these societies will be - in demographic and eventually market terms – a minority. Depending on where one places nations with corruption and increasingly authoritarian politics, the democracies that are truly consolidated into stable, rule of law-bound, civil society cultures in practice as well as name across their national STES are few, totally between 30 – 40 [40] This small number compared to the 190-odd recognized nations of the world will not be able to enforce or maintain the liberal international economic system over time when the other ninety percent of the globe's population are likely to be led by the practices, preferences, and products of China and Asia for most of the rest of this century.

In any case, it will be increasingly tough for westernized civil societies to obtain and maintain allies since they are already seen to be in decline. In the 1980s, the former leader of China Deng Xiaoping predicted China would equal the US as a global great power over a period of roughly 70 years because of its demographic and economic weight in the global system. (J. Liu & Deng, 2010) By most measures, the rise of China was inevitable but has occurred faster than anticipated. Analyses, such as the 2007 Goldman Sachs estimate, predicted parity would occur by 2025, with China doubling that of the US by 2050. As of this writing, various authors argue that China has been roughly at parity for several years (at least since 2014). (M. Liu, 2015) (Fujita & Thisse, 2013) (Scott & Sam, 2016). With its poorly secured global pathways across poor and wealthy national STESs, cyberspace and its own form of "hidden hand of economic coercion" shortened that anticipated transition dramatically – to fifteen to twenty years. (Drezner, 2003) (Weede, 2015) This Internet governance challenge to civil society presumptions is only the beginning of a host of looming multi-domain contests. If these democracies – and their economic sectors – refuse to recognize their loss of dominance[41] and to face the implications of

[39] This section draws heavily from a previous publication. See (P. Dombrowski & Demchak, 2015).

[40] The role of India as a largescale nonwestern democracy likely to be critical in improving the odds for the long-term survival of democracies globally is woefully understudied. It is not included in this eleven percent figure. (Stuenkel, 2013)

[41] Increasing the sense of surprise that could feed outrage and poorly considered policies in the future democratic societies is a largely American international relations literature largely silent on adapting to the serious possibility of US decline. (Friedman, 2010)

the rise of an authoritarian much larger world – especially the need to be as systemically resilient in the face of cyber coercive peace as one used to be prepared for destructive wars, then these contests are more likely to be lost in the future.[42]

Being a billion plus population that is centrally led and nationally self-identified as 'Han' is a major advantage in scale for China across the global cyberspace substrate along the entire spectrum of cybered conflict from peace to war. China's Middle Kingdom rulers are fully mindful that their "rightful place" in the world rests fundamentally on their demographic weight as a coherent state actor in a world of many smaller nations. For China, a true peer power for the longer term must be able to coherently wield the power of a similar demographic weight. India has the demography but by far not the coherence. The US and each of its allies taken alone are by no stretch peer powers. Rather, the more they concern themselves entirely with their own cyber security and economic protection, the more they are simply opponents to eventually be over taken as China rises to its 'proper position' globally. Irrespective of what the individual democratic societies prefer, China's state economic champions have the scale and the national support necessary to build the future global internet with Chinese influence embedded across all the future population and economic concentrations of the world – and without western sensibilities, values, and eventually markets. (Khanna, 2009)

If the current trends are not altered, then China's preferences will majorly frame how this new nonwestern world will be governed; however, China has not given details of what, ideally, its leaders would like to see in place. For a state the size of China, the current and future potential to directly influence the cyber and economic preferences of the developing world – and thereby the bulk of the globe's states and populations – is enormous, and this gap in stated vision or intentions is unsettling. The Chinese narrative in speeches and publications connects this essential element -- state cyber sovereignty -- with a world where China rises to its proper place (defined by its demographic scale) as the first great cybered power that is benignly 'nonhegemonic'. The term is used to mean no state including China as rising world power will tell any other state how to operate internally. Thus, one thing is clear – this envisioned new world neatly eliminates the US as the old style global internet hegemon -- and its civil society preferences -- from the center of the global international system's governance. (Kivimäki, 2014)

[42] For a particularly in-depth and instructive comparison of how 'cyber ready' many states are, see the Cyber Readiness Index created by Melissa Hathaway. www.potomacinstitute.org/academic-centers/cyber-readiness-index

Beyond that, one must look to both recent history and long cultural tendencies for indicators of how a China-dominated international system might operate. In Chinese society, its organizations, and its business practices, hierarchy is preferred uniformly, size makes right – the big are entitled to compel the small, and history trumps law unless the law's verdict suits the preferences of the one at the top of the hierarchy, i.e., China.[43] (Kardon, 2017) How China conducts business and politics inside China is how its firms and political leaders will feel comfortable conducting business and politics when China occupies the center of demographic and economic circles globally. In the past few years, China's new leader Xi Jinping and official media outlets have increasingly openly rejected civil society "western" values – chief among them freedom of speech -- and more aggressively asserted the downsides of continuing US dominance of the web. (Kemp, 2015)

In other indicators, as the economic weight of the Chinese market has grown, so has Chinese willingness to use its size in economic statecraft (and blatantly violate the WTO norms) to alternate between bribing and bullying those who do not comply with Chinese preferences, including publicity. (Kennedy, 2006) In direct and many indirect forms, Chinese leaders have successfully curtailed the libertarian demands of western IT capital goods industrial leaders over time. Threatening access to the large Chinese market has the practical effect of inducing compliance from major western corporate and political actors. Both are rewarded for accommodating behaviors explicitly from trade promises to easing of policies – at least for as long as their technology transfer or political influence is needed. (Emmott & Blanchard, 2017) For example, in 2008 Apple's founder, Steve Jobs, conceded to the Chinese demand that a heavily encrypted WAPI Wi-Fi chip of Chinese design and making be inserted in all Apple iPhones if any were to be sold in China itself. Since Jobs did not want to make two world phones, by 2009 he accepted the Chinese explanation that the chip could only be turned on and access inside Chinese borders, though it is not publicly knowable if that restriction is actually accurate. (H.-W. Liu, 2017) (M. Li, Liu, & Reimers, 2011) While aggressively demanding freedom from government controls in western states lest the commercial generativity be destroyed, many IT industrial leaders have nonetheless abandoned their oft stated (in western settings) concerns for either democracy or non-interference from governments in order to preserve their firm's access to markets in China and other authoritarian states.

One need not be the actual offending actor to catch the wrath. Non-accommodating national policies, public statements, or even unflattering news reports are punished by

[43] There is considerable speculation on what happens in the post-western world. See for example (Jacques, 2012).

"difficulties" imposed on other members of the offending community within Chinese reach, whether it is the actual actor who caused offense or just other prominent members. (Reilly, 2013) Foreign companies that are seen to embarrass China are compelled to apologize, even if the actors causing the harm were Chinese employees in China far from the senior leaders, as the CEO of the toy company Mattel was obliged to do. (Story, 2007) Those who do not comply – such as Google – have been forced to withdraw (for some time) from Chinese markets and subjected to intense competitive pressures directly and indirectly. (Helft & Barboza, 2010) For example, recently major South Korean firms have suddenly experienced 'difficulties' in their Chinese operations when South Korea and China relations hit a downturn. (Jin, 2017)

What is to be done? None of this global topological change was anticipated by early internet promoters, nor desired today by leaders and citizens of consolidated democratic civil societies. Put more colloquially, how will these nations in the demographic and coming economic minority individually avoid being vassals over time in a conflictual, largely authoritarian, cybered world. Scale needs to be met by scale, or the challenger needs to change the conditions of key aspects of the competition. In this case, changing the conditions will take longer and is less certain than the one feasible alternative available to these societies – creating the necessary scale in an institutionally and technologically integrated cyber systemic resilience alliance. It must be one that accepts the rise of cyber sovereignty among nations which will not in the foreseeable future be civil societies – if ever. Yet this alternative must preserve some remnant of the free and open cyberspace created by the West for its own tolerant cultural preferences, transparent legal regimes, and comparative well-being. And it must succeed eventually in re-making the underlying substrate properly – transforming it technologically, societally, and economically as it was intended, and defending it, even if only for themselves. The alternative is to eventually concede to a global version of China's "info-web" internet. (F. Schneider, 2015)

Conclusion: Creating this Alliance requires Essential Recognitions

First, a major part of the necessary response is to alter the cognitive framing created in the early frontier era of cyberspace and explicitly accept the rise of Cyber Westphalia. It has been costly for the western democracies to be so distracted into pushing for a future fully democratized, borderless, and civil society-led world that had nearly no chance of emerging. Chances to slow this rise of cybered conflict have been squandered across a range of missed technological transformation, societal resilience, markets reform, and informed policy

opportunities. That doggedly western civil society narrative now has a major counter-narrative – well funded, covertly reinforced, and overtly widely promoted from a rising and confident large authoritarian actor, China – about changing the realities governing the future cybered world. Cyber jurisdictions are emerging whether or not the westernized world desires them, and opposing the process accelerates the likely affiliation of the rest of the world with the Chinese model.

Recognizing a national cyber jurisdiction – the essence of cyber sovereignty – is the first step to developing a consensus of society much like a cooperative enterprise worthy of defending in terms of its STESs' viability and political freedoms. Without this recognition, democratic leaders cannot use "stateness" [44] – a sense of collective willingness to act – in order to create and sustain systemic resilience. While cyber sovereignty has been repeatedly rejected by western corporations and political leaders for commercial and optimistic reasons, a wide array of autocratic leaders - led by China as the rising center of economic and demographic power – argue strongly in favor of internet sovereignty.[45] Those nations will – to the extent possible – have the internal coherence in power, infrastructure, and citizen/commercial entity controls to create resilience as they interpret it,[46] leaving the democratic societies with no examples of success in doing so unless – as improbably as it sounds – these nations regain control of the entire global web and its use policies.

Second, this cyber resilience alliance will need this "stateness" as a shared identity across consolidated democracies. Rather than seeing the rest of the world as moving inexorably to becoming democratic civil societies, recognizing the cultural peculiarity – and consequent numerical fragility – of the democratic experiment in comparison to the more normal, authoritarian, and affective speaking cultures of the rest of the world will be essential. The alliance will need a common perception that it matters to each of us and each nation to defend the democratic civil societies against the economic losses and political intrusions of the rising and much larger authoritarian world. This unusual community of nations empowered by the United States grew to dominate the world when China and Russia (and allies) so helpfully self-isolated during the Cold War. They were helped by the way Russia's communism provided a

[44] Put differently, stateness is the ability to persuade the leaders of a state to act together to resist external coercion. See (Blanchard & Ripsman, 2008)

[45] Kissinger observed that, in his long experience, most Asian states in particular have not ever been willing to concede local sovereignty unless forced to do so. (Kissinger, 2015) p.179. See also (Chang, 2014).

[46] Nationally controlled radio stations and telephone exchanges have long been prime points of societal control in non-western states, with the internet quite unlikely to be regarded much differently in the view of national leaders – if the means to control in the same way were available. (Glanz & Markoff, 2011) (Gumede, 2016)

discernible and distinct face of authoritarianism against which they could unite, unlike the generalized rise of authoritarianism emergent today. After the Cold War, however, these states still expected their global dominance to continue and never recognized it as both shallow and culturally incompatible with most of the world. Led by American hubris in particular, the western powers thought – and continue to think – of themselves as the universal exemplar of normal humans, not as what they are: the product of a highly and narrowly unique blend of historical trends involving Catholic transnationalism, Protestant leveling ethics, and the Enlightenment. (Goldstein, 2015; Tilly & Ardant, 1975)

Third, the alliance requires recognition of the power of demographic scale as the only measure recognized by China to merit peer status. China is unlikely to daunted, deterred, or deflected over time by this ten-eleven percent of the world's population found in democratic societies if they stand disunited, individually small in demographic and eventually market comparisons, and attempt to individually defend their own national cyber jurisdictions. They have little chance of independently gathering the necessary levels of investment and domestic talent needed to be a robust cyber power. The maintenance of secured national STESs will be unsustainable systemically if every state alone is to afford and orchestrate advanced technologies, resilience budgets,[47] and collective intelligent choices as a minority democracy in a much larger, deeply cybered, and overwhelmingly authoritarian world system.

Fourth, the alliance is feasible. The community estimated at 30-40 states has collectively about 800-900 million people in well-educated modern communities, sufficient to be relatively economic autarkic if need be and certainly capable of developing the talent and technology to compete as a peer cyber power with China if they – like China – were a unified community. The collective scale of these cultural and trade allies can be turned in their advantage in a cybered world if these minority states create a coherent entity able to defend these cybered STESs jointly. There is nothing magical about the authoritarian turn to the telecommunications agencies in those nations in order to deepen authoritarian controls. Consolidated democratic civil societies also have central telecommunications firms to be enlisted into the resilience of their community. But democracies also have the large private sector likely to lose both their access to large markets in the future and their own viability as borders close and internal national policies extract technologies and concessions for access. It is not always recognized that the private

[47] Constrained budgets easily sideline advanced technologies today, even before the era of system-wide national IT R&D and transformational deployment budgets has fully emerged. See (Cava, 2017)

sector and their talent in democracies have as much to lose with the loss of the international liberal economic system as have the nations they call home.

Furthermore, that one has yet not seen this kind of cross-border, culturally like-minded, operationally active, public and private joint resilience structure is not an argument against the alliance. One had never seen a NATO, an EU or even the anti-Confiker private sector group formed in 2009 before these structures – large and small, military, economic, and technological – were created as the need arose. One has seen remarkable organizational efforts in short periods of time if the urgency is both clearly communicated and a program to solve it collectively funded. At the end of the 1970s, miniaturization went from a strong interest of the western militaries, especially the US, to a critical major push when the Soviet military conventional buildup was seen as an overwhelming scale advantage over Western Europe. The result is a technological transformation found all around us in smart phones and other advanced technologies. The same kind of transformation is needed now, but we do not have the stability of the basic competition present between NATO vs Warsaw Pact to buy time. The alliance is needed in the near term to create the jointly defended resilience buffering the democratic societies while their collective talent innovate a new more secure and yet democratic cyber substrate and their leaders learn how to maneuver, trade, and defend in an overwhelmingly authoritarian world.

At the end of the day, the likeminded have the economic, technological, and demographic resources to stand up to the much larger scale of an authoritarian world led by China over the coming century – IF they create this skillfully integrated and operational alliance of mutual systemic cyber resilience recognizing the existential long term trends and competently defending the interlinked STESs. Alone, none of these nations will do well over time. Together, these consolidated democratic civil societies – including all the major public and private actors – can jointly muster the resources and talent to defend their entire community and values across the full range of cybered conflict. In changing the current trends, they have the chance to survive collectively as robust cyber powers adequately prosperous in trade and wellbeing, and still be consolidated democracies over the long term.

Bibliography

Anderson, R. J. (1994). Liability and computer security: Nine principles *Computer Security—ESORICS 94* (pp. 231-245): Springer.

Atkinson, R., & Brake, D. (2015). Net Gains: A Pro-Growth Digital Agenda. *Democracy*(36), 9.

Atkinson, R. D., & Ezell, S. (2015). False Promises: The Yawning Gap Between China's WTO Commitments and Practices. Washington DC: Information Technology and Innovation Foundation.

Baran, N. (1996). Privatization of telecommunications. *Monthly Review, 48*(3), 59.

Barlow, J. (1996). A Declaration of the Independence of Cyberspace. *Humanist - Buffalo, 56*(3), 18-19.

Barry, J. J. (2014). *Don't Be Evil: Should Access to the Internet Be Conceptualized as an Instrumental Human Right?* Paper presented at the American Political Science Association 2014 Annual Meeting Paper.

Baskerville. (2006). Hacker Wars: E-Collaboration by Vandals and Warriors. *International Journal of e-Collaboration, 2*(1), 16.

Betz, D. J., & Stevens, T. (2011). Chapter two: Cyberspace and sovereignty. *Adelphi Series, 51*(424), 55-74.

Bhuiyan, A. (2014). *Internet governance and the global south: demand for a new framework*: Palgrave Macmillan.

Blanchard, J.-M. F., & Ripsman, N. M. (2008). A political theory of economic statecraft. *Foreign Policy Analysis, 4*(4), 371-398.

Blancher, M. N. R., & Rumbaugh, M. T. (2004). IMF: China - international trade and WTO accession: International Monetary Fund.

Blum, A. (2013). *Tubes: A Journey to the Center of the Internet*: HarperCollins Publishers.

Bradley, J. (2015). *The China mirage: The hidden history of American disaster in Asia*: Hachette UK.

Brian, A. (2010). *Seven deadliest USB Attacks*. Burlington, MA: Syngress Media Inc.

Brink, G. F. (2013). Anti-dumping and China: three major Chinese victories in dispute resolution.

Cava, C. P. (2017, February 6). Grounded: Nearly two-thirds of US Navy's strike fighters can't fly, *Defense News*

Cerf, V. G. (2012). Internet access is not a human right. *New York Times, 4*, 25-26.

Chang, A. (2014). Warring State: China's Cybersecurity Strategy http://www.cnas.org/chinas-cybersecurity-strategy#.VeHZlM5REns: Center for New America Security.

Chen, M.-J. (2001). *Inside Chinese business: A guide for managers worldwide*. Cambridge, MA: Harvard Business Press.

Chung, M., & Mascitelli, B. (2014). Huawei's Battle: Cold War or Commercial War? *Asian Business and Management Practices: Trends and Global Considerations: Trends and Global Considerations*, 107.

Clark, D. (2010). Fighting over the Future of the Internet. *IEEE Internet Computing, 10*, 22-23.

Comfort, L., Boin, A., & Demchak, C. (Eds.). (2010). *Designing Resilience: Preparing for Extreme Events*. Pittsburgh: University of Pittsburgh Press.

Coupland, D. (2004). *Microserfs*: HarperCollins UK.

Cui, D., & Wu, F. (2016). Moral goodness and social orderliness: An analysis of the official media discourse about Internet governance in China. *Telecommunications Policy, 40*(2-3), 265-276.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2012). *Access contested: security, identity, and resistance in Asian cyberspace*: The MIT Press.

Deibert, R., & Villeneuve, N. (2004). Firewalls and power: An overview of global state censorship of the Internet. *Human rights in the digital age. London: GlassHouse*.

Deibert, R. J., & Crete-Nishihata, M. (2012). Global Governance and the Spread of Cyberspace Controls. *Global Governance: A Review of Multilateralism and International Organizations, 18*(3), 339-361.

Demchak, C. C. (2010). Conflicting Policy Presumptions about Cybersecurity: Cyber–Prophets, –Priests, –Detectives, and –Designers, and Strategies for a Cybered World". *Atlantic Council Issue Brief*.

Demchak, C. C. (2012). Resilience, Disruption, and a 'Cyber Westphalia': Options for National Security in a Cybered Conflict World. In N. B. a. J. Price (Ed.), *Securing Cyberspace: A New Domain for National Security*. Washington, DC: The Aspen Institute.

Demchak, C. C. (2013). Economic and Political Coercion and a Rising Cyber Westphalia. In K. Ziolkowski (Ed.), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (pp. 595-620). Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence.

Demchak, C. C. (2016). Uncivil and Post-Western Cyber Westphalia: Changing Interstate Power Relations of the Cybered Age. *The Cyber Defense Review, 1*(1).

DeNardis, L. (2014). *The global war for internet governance*: Yale University Press.

Diamond, L. J. (1994). Toward democratic consolidation. *Journal of Democracy, 5*(3), 4-17.

Dombrowski, P., & Demchak, C. C. (2015). Thinking Systemically about Security and Resilience in an Era of Cybered Conflict. *Cybersecurity Policies and Strategies for Cyberwarfare Prevention*, 367.

Dombrowski, P. J., & Demchak, C. C. (2014). Cyber Westphalia: Asserting State Prerogatives in Cyberspace. *Georgetown Journal of International Affairs, special issue on cyber*.

Drezner, D. W. (2003). The hidden hand of economic coercion. *International Organization*, 643-659.

Duanmu, J.-L. (2014). State-owned MNCs and host country expropriation risk: The role of home state soft power and economic gunboat diplomacy. *Journal of International Business Studies, 45*(8), 1044-1060.

Duara, P. (1997). Transnationalism and the predicament of sovereignty: China, 1900-1945. *The American Historical Review*, 1030-1051.

Dunlap Jr, C. J. (2001). *Law and military interventions: preserving humanitarian values in 21st century conflicts*. Paper presented at the Humanitarian Challenges in Military Intervention Conference, Washington, DC.

Emmott, R., & Blanchard, B. (2017, March 28). Wary of Trump, China launches EU charm offensive: diplomats, *Reuters*, pp. http://www.reuters.com/article/us-eu-china-idUSKBN16Z22S.

Farnsworth, T. (2011). China and Russia Submit Cyber Proposal ["International code of conduct for information security"]. *Arms Control Today*, 35-36.

Friedman, G. (2010). *The next 100 years: a forecast for the 21st century*: Anchor.

Frischmann, B. (2001). Privatization and Commercialization of the Internet Infrastructure. *Columbia Science and Technology Law Review, 2*(1), 1-70.

Fujita, M., & Thisse, J.-F. (2013). *Economics of agglomeration: cities, industrial location, and globalization*: Cambridge university press.

Gagliardone, I. (2015). China and the Shaping of African Information Societies. *Africa and China: How Africans and Their Governments are Shaping Relations with China*, 45.

Geer, D., Bace, R., Gutmann, P., Metzger, P., Pfleeger, C. P., Quarterman, J. S., & Schneier, B. (2003). CyberInsecurity: The cost of monopoly *CyberInsecurity Reports*. http://www.totse2.net/totse/en/technology/computer_technology/cyberinsecurit171812.html (original http://www.ccianet.org/papers/cyberinsecurity.pdf): Computer and Communications Industry Association (CCIA).

Glanz, J., & Markoff, J. (2011, February 15). Egypt Leaders Found 'Off'Switch for Internet, *The New York Times,* p. online.

Glenny, M. (2011). *Dark Market*. New York: Random House.

Goldstein, L. J. (2015). *Meeting China halfway: How to defuse the emerging US-China rivalry*: Georgetown University Press.

Goodin, D. (2010, January 14). IE zero-day used in Chinese cyber assault on 34 firms: Operation Aurora unveiled, *El Register*. Retrieved from http://www.theregister.co.uk/2010/01/14/cyber_assault_followup/

Greer, J. N. (2010). Square legal pegs in round cyber holes: The NSA, lawfulness, and the protection of privacy rights and civil liberties in cyberspace. *J. Nat'l Sec. L. & Pol'y, 4*, 139-154.

Gresh, A. (2008). Understanding the Beijing consensus. *Translated by Stephanie Irvine. Le Monde Diplomatique English Edition*.

Gumede, W. (2016). Rise in Censorship of the Internet and Social Media in Africa. *Journal of African Media Studies, 8*(3), 413-421.

Hafner, K. (1999). *Where Wizards Stay Up Late: The Origins of the Internet*: Simon and Schuster.

Hao, Q. (2015). China Debates the 'New Type of Great Power Relations'. *The Chinese Journal of International Politics, 8*(4), 349-370.

Hathaway, M. (2013). Cyber readiness index 1.0. *Great Falls, VA: Hathaway Global Strategies LLC*.

Helft, M., & Barboza, D. (2010). Google shuts China site in dispute over censorship. *NY TIMES, Mar, 22*.

Hill, R. (2014). *Internet governance: the last gasp of colonialism, or imperialism by other means?* : Springer.

Hughes, K. A. (1996). Copyright in Cyberspace: A Survey of National Policy Proposals for On-line Service Provider Copyright Liability and an Argument for International Harmonization. *Am. UJ Int'l L. & Pol'y, 11*, 1027.

Irion, K. (2009). Privacy and security International communications surveillance. *Communications of the ACM, 52*(2), 26-28.

Jacques, M. (2012). *When China rules the world: The rise of the middle kingdom and the end of the western world [Greatly updated and expanded]*: Penguin UK.

Jin, H. (2017, April 3). Hyundai flags weaker China sales after missile row; Kia's March China sales halved: source, *Reuters,* pp. http://www.reuters.com/article/us-southkorea-autos-china-idUSKBN17511C.

Juuso, A. M., Takanen, A., & Kittilä, K. (2013). *Proactive cyber defense: Understanding and testing for advanced persistent threats (APTs).* Paper presented at the Proceedings of the 12th European Conference on Information Warfare and Security: ECIW 2013.

Kalathil, S., & Boas, T. C. (2010). *Open networks, closed regimes: The impact of the Internet on authoritarian rule*. Washington DC: Carnegie Endowment.

Kallio, J. (2015). Dreaming of the great rejuvenation of the Chinese nation. *Fudan Journal of the Humanities and Social Sciences, 8*(4), 521-532.

Kardon, I. B. (2017). *Rising Power, Creeping Jurisdiction: China's Law of the Sea (dissertation manuscript)*. Ithaca, NY.: Cornell University.

Kemp, T. (2015, July 6). China leaders oppose 'universal values,' but it may not matter: interview with Prof Steinfeld Brown University, *CNBC.com*.

Kennedy, S. (2006). The political economy of standards coalitions: Explaining China's involvement in high-tech standards wars. *Asia Policy, 2*(1), 41-62.

Khanna, T. (2009). Billions of entrepreneurs: How China and India are reshaping their futures and yours. *Strategic Direction, 25*(10).

Kinnersley, B. (2015). A Chronology of Influential [computer] Languages, The [Computer] Language List: Collected Information On About 2500 Computer Languages, Past and Present. Retrieved 2015 August 21, from University of Kansas

Kissinger, H. (2015). *World order*: Penguin Books.

Kivimäki, T. (2014). Soft power and global governance with Chinese characteristics. *The Chinese Journal of International Politics, 7*(4), 421-447.

Kopetz, H. (2011). Internet of things. In H. Kopetz (Ed.), *Real-time Systems* (pp. 307-323): Springer.

Kroker, A., & Kroker, M. (1996). Code Warriors. *CTheory.net*, 2-7.

Langheinrich, M. (2001). Privacy by Design-Principles of Privacy-Aware Ubiquitous Systems. *LECTURE NOTES IN COMPUTER SCIENCE*, 273-291.

Lessig, L. (2004(1998 original)). The laws of cyberspace. In R. A. Spinello & H. T. Tavani (Eds.), *Readings in Cyberethics* (pp. 134-145). Sudbury, MA: Jones and Bartlett Learning.

Li, M., Liu, X., & Reimers, K. (2011). *Emerging mobile platform competition in China's 3G era and beyond.* Paper presented at the Service Systems and Service Management (ICSSSM), 2011 8th International Conference, June 25-27, 2011, Tianjin, China.

Li, X., & Shaw, T. M. (2014). “Same Bed, Different Dreams” and “Riding Tiger” Dilemmas: China’s Rise and International Relations/Political Economy. *Journal of Chinese Political Science, 19*(1), 69-93.

Liff, A. P., & Erickson, A. S. (2013). Demystifying China's Defence Spending: Less Mysterious in the Aggregate. *The China Quarterly, 216*, 805-830.

Liu, H.-W. (2017). Inside the Black Box: Political Economy of the Trans-Pacific Partnership’s Encryption Clause. *Journal of World Trade, 51*(2), 309-333.

Liu, J., & Deng, B. (2010). America Hegemony: Is It To Decline or To Continue. *Pacific Journal, 1*, 1-8.

Liu, M. (2015). *The China Dream: Great Power Thinking & Strategic Posture in the Post-American Era*.

Lumension. (2015). 2015 Sixth Annual State of the Endpoint Cybersecurity Survey *Annual State of the Endpoint Cybersecurity Survey*. https://www.lumension.com/Lumension/media/graphics/Resources/2015-state-of-the-endpoint/2015-State-of-the-Endpoint-Whitepaper-Lumension.pdf: Ponemon.

MacKinnon, R. (2011). China's" networked authoritarianism". *Journal of Democracy*, *22*(2), 32-46.

Mallery, J. C. (2011 (2009)). *A Strategy for Cyber Defense (earlier title: Multi-spectrum Evaluation Frameworks and Metrics for Cyber Security and Information Assurance)*. Paper presented at the MIT/Harvard Cyber Policy Seminar,, Cambridge, MA.

Mandiant. (2013). APT1: Exposing One of China’s Cyber Espionage Units. In M. I. Center (Ed.). New York: Mandiant.

Mastanduno, M. (2012). Economic statecraft. *Foreign Policy: Theories, Actors, Cases*, 204.

Mathur, A., & Singh, K. (2013). Foreign direct investment, corruption and democracy. *Applied Economics, 45*(8), 991-1002.

McCarthy, J. (1978). History of LISP. *History of programming languages I*, 173-185.

McGregor, J. (2012). No Ancient Wisdom, No Followers‖: Prospecta Press, Westport.

Mozur, P. (2015, September 29). Chinese Official Faults U.S. Internet Security Policy [Ms. Hao YeLi], *New York Times*.

Norris, P., & Jones, D. (1998). Virtual democracy. *Harvard International Journal of Press Politics, 3*, 1-4.

Norton-Taylor, R. (2010, October 18). The UK is under threat of cyber attack, the national security strategy says- Home secretary outlines priority threats facing Britain ahead of the publication of the national security strategy today, *Guardian Online*.

Nye, J. S. (2014). *The Regime Complex for Managing Global Cyber Activities*. http://www.cigionline.org/publications/regime-complex-managingglobal-cyber-activities: Ourinternet.org Retrieved from http://www.cigionline.org/publications/regime-complex-managingglobal-cyber-activities.

Oyedemi, T. (2014). Internet access as citizen's right? Citizenship in the digital age. *Citizenship Studies*, 1-15.

Paganini, P. (2013). Cyber-espionage: The greatest transfer of wealth in history. *H+ Magazine online*.

Peerenboom, R. (2006). Law and development of constitutional democracy: Is China a problem case? *The ANNALS of the American Academy of Political and Social Science, 603*(1), 192-199.

PWC. (2014). Global State of Information Security® Survey 2015 *Annual State of Information Security Survey*. http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml: Price Waterhouse Cooper.

Qiu, J. L. (1999). Virtual censorship in China: Keeping the gate between the cyberspaces. *International Journal of Communications Law and Policy, 4*(Winter), 1-25.

Reilly, J. (2013). China's economic statecraft: turning wealth into power. *Lowy Institute for International Policy*.

Richmond, R. (2011, April 2). The RSA Hack: How They Did It, *New York Times*.

Rochlin, G. (1997). *Trapped in the Net: The Unanticipated Consequences of Compute rization*. Princeton Princeton University Press.

Rogers, M., & Ruppersberger, C. D. (2012). *Investigative report on the US national security issues posed by Chinese telecommunications companies Huawei and ZTE: A report*. Washington DC: US Government Press.

Rosenzweig, R. (1998). Wizards, bureaucrats, warriors, and hackers: Writing the history of the Internet. *American Historical Review*, 1530-1552.

Rowley, C. (2010). Commentary: China's chimera: miracle or mirage in the 'Middle Kingdom'? *Asia Pacific Business Review 16*(3), 269-271.

Schneider, F. (2015). China's 'info-web': How Beijing governs online political communication about Japan. *New Media & Society*, 1-21.

Schneider, V., Fink, S., & Tenbucken, M. (2005). Buying Out the State: A Comparative Perspective on the Privatization of Infrastructures. *Comparative Political Studies, 38*(6), 704-727.

Schrage, M. (2011, May 6). How Amazon or Apple Could Cause a War with China: Networked and cloud-based digital businesses are vulnerable targets for cross-border mischief that could cause international conflict, says Michael Schrage *Harvard Business Review*.

Scott, M., & Sam, C. (2016, May 12). China and the United States -Tale of Two Giant Economies, *Bloomberg.com*. Retrieved from https://www.bloomberg.com/graphics/2016-us-vs-china-economy/

Segal, A. (2016). *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*: PublicAffairs.

Shema, M. (2010). *Seven deadliest web application attacks*. Burlington, MA: Syngress Media Inc.

Shih, G. (2014, December 8). Chinese Internet regulator welcomed at Facebook campus., *Reuters*. Retrieved from http://www.reuters.com/article/us-china-facebook-visit-idUSKBN0JM0O820141208.

Shin, H. (2015). The Relationship between the Arab Spring Revolutions and Entrepreneurial Inhibitors, Enablers, and Activity in North Africa. In J. Ofori-Dankwa & K. Ormani-Antwi (Eds.), *Comparative Case Studies on Entrepreneurship in Developed and Developing Countries* (pp. 82-98). Hershey, PA: IGI Global.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What Everyone Needs to Know*: Oxford University Press.
Skepys, B. (2012). Is There a Human Right to the Internet. *J. Pol. & L., 5*, 15.
Soldatov, A., & Borogan, I. (2013). Russia's surveillance state. *World Policy Journal, 30*(3), 23-30.
Stewart, S. (2013). Epilogue–From the 'colour revolutions' to the 'Arab spring': Implications for democracy promotion. In S. Stewart (Ed.), *Democracy Promotion and the 'Colour Revolutions'* (pp. 181). London: Routledge.
Story, L. (2007, September 22). Mattel Official Delivers an Apology in China *New York Times*. Retrieved from http://www.nytimes.com/2007/09/22/business/worldbusiness/22toys.html?_r=1&oref=slogin
Stuenkel, O. (2013). Rising Powers and the Future of Democracy Promotion: the case of Brazil and India. *Third World Quarterly, 34*(2), 339-355.
Swyngedouw, E. (2000). Authoritarian governance, power, and the politics of rescaling. *Environment and Planning D, 18*(1), 63-76.
Tan, J., & Tan, A. E. (2012). Business under threat, technology under attack, ethics under fire: The experience of Google in China. *Journal of Business Ethics, 110*(4), 469-479.
Tilly, C., & Ardant, G. (1975). *The formation of national states in Western Europe* (Vol. 8): Princeton Univ Pr.
Trickey, H. (1988). C++ versus Lisp: a case study. *ACM Sigplan Notices, 23*(2), 9-18.
Tully, S. (2014). A Human Right to Access the Internet? Problems and Prospects. *Human Rights Law Review*, ngu011.
Weede, E. (2015). Future Hegemonic Rivalry Between China and the West? *Journal of World-Systems Research, 1*(1), 639-658.
West, D. M. (2016). Internet shutdowns cost countries $2.4 billion last year Washington DC: Brookings Institution Center for Technology Innovation.
Wexelblat, R. L. (2014). *History of programming languages*: Academic Press.
Whiting, A. S. (1996). The PLA and China′ s Threat Perceptions. *The China Quarterly, 146*, 596-615.
Wrobel, D. M. (2013). *Global West, American Frontier: Travel, Empire, and Exceptionalism from Manifest Destiny to the Great Depression*: UNM Press.
Xu, X., Mao, Z. M., & Halderman, J. A. (2011, May 20-21). *Internet censorship in China: Where does the filtering occur?* Paper presented at the 12th Passive and Active Measurement Conference, Atlanta, GA.
Yong, W., & Pauly, L. (2013). Chinese IPE debates on (American) hegemony. *Review of International Political Economy, 20*(6), 1165-1188.
Zhao, S. (2015). Rethinking the Chinese World Order: the imperial cycle and the rise of China. *Journal of contemporary China, 24*(96), 961-982.
Zheng, Y., & Lye, L. F. (2015). China's Foreign Policy: The Unveiling of President Xi Jinping's Grand Strategy. *East Asian Policy, 7*(01), 62-82.

OPENING STATEMENT JAMES A. LEWIS PH.D., SENIOR VICE PRESIDENT, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

DR. LEWIS: I was going to say. And I agree with everything she said even if it wasn't official U.S. policy.

Thanks again for having me here to speak. It's a good opportunity to have a good discussion on China. What I look at is a little different. I'm looking at the significant changes that have occurred in Chinese policies since President Xi took office, and Xi confronted some major problems. You have the erosion of Party legitimacy, and you have the ongoing economic fragility that afflicts China. So his goal has been to strengthen the regime, the Party's control, strengthen the ability of the Party to continue to dominate Chinese politics.

If you look, there's been, I think, a number of efforts that contribute to this goal. You're all familiar, of course, with the anti-corruption campaign, which serves the dual purpose of both helping President Xi gain control of the Party and yet also appeal--the hope is it will appeal to a larger public audience by showing that corruption is being tackled.

You have PLA modernization, which you've talked about. This is something that the Chinese take very seriously. To some extent, it's modeled on our own activities, but it's ongoing, and I think it will create challenges for us.

There's been less discussion of intelligence reform by President Xi, but since taking office, he has centralized tasking and collection by the Chinese intelligence services.

I thought that was really interesting that one of the first things he did was order review of ongoing collection programs, and what that suggested to me at the time was that meant Beijing did not know what their agents were up to.

Finally, and perhaps most importantly for the Chinese, Xi has sought to expand control of cyberspace, and like the other authoritarian regimes, there's a deep and abiding fear that something like Arab Spring will happen in China, and so finding ways to reduce the political effect of the Internet is a crucial part of his strategy, and he actually oversees the effort in an unusual way. He is personally involved in this.

When I look at China's cyber strategy, the keys are sovereignty and political stability. It is largely focused on the domestic. It's a domestic focus for the Chinese. The good news is we're opponent number two. Their greatest concern is their own population. There's a tremendous emphasis on content control, and if you look at the Chinese social media, you'll see many complaints that the space for remarks is being greatly constrained.

Finally, and a bit more telling for the U.S., both mercantilists and security motives have prompted China to adopt new policies on technology. We're all familiar, I think, with the emphasis on developing Chinese semiconductor industry. This has been a longstanding goal of the Chinese. This is their third or fourth effort. The previous efforts didn't work.

This one is a little different because instead of trying to acquire technology licitly or illicitly or to build their own plants, they seem to have moved to simply buying Western entities, which solves a lot of the human capital and knowledge problems they have.

You see this in other areas as well, and in some ways, the Chinese believe that they can use these policies to create national champions who by being able to operate in a protected domestic market will be able to displace their foreign competitors.

So for me this is a significant threat, and you see it in AI, in robotics, in cloud services,

and in semiconductors.

The Chinese position in international negotiation is largely defensive. They seek to block anything that would create risk for China's own national positions; right. Their emphasis in international negotiation is on sovereignty and on asserting the right, as Dr. Demchak mentioned, for nations to control their internal networks. They find the application of international law contentious. This is troubling in some ways, and my view is that if we put the Universal Declaration of Human Rights up for a vote today, it would not get a majority of nations, but China is certainly among them.

In particular, the Chinese are opposed to anything that would appear to legitimize U.S. attack or U.S. retaliation upon them, and I've heard this directly from senior Chinese diplomats. We do not agree with the Law of Countermeasures or the application of the laws of armed conflict because it would legitimatize your attack, your retaliation.

Their own military use of cyber, as you know, the Chinese goal is regional dominance and resisting--that would be their term--or challenging the U.S. I believe their planning is scenario-specific. So they have plans for how to operate in the South China Sea, how to operate in the Sea of Japan, but that they don't have a larger general strategy or doctrine yet. This is one of the goals of the PLA reform.

Their targets are command and control and weapon systems. We know they have penetrated U.S. systems and will seek in the opening phase of any conflict to disrupt command and control and the operation of weapons.

It's interesting to watch what happened with efforts probably by the North Koreans, but perhaps by the Chinese, to probe the recently deployed THAAD system in South Korea.

The U.S. needs to respond to this, and in some ways we have fallen a little bit behind. In 2008, a Chinese diplomat told me that they had assumed that the U.S. was withdrawing from Asia. In the first Obama administration, they said, well, it looks like you're coming back to Asia. That was the pivot. But now I think they believe we're again not as emphatic in what we want to do in Asia.

So I believe the goals for any administration would be sustained senior level engagement and a more assertive, but not confrontational, policy. I think this is possible, and I look forward to your questions.

Thank you.

PREPARED STATEMENT OF JAMES A. LEWIS, PH.D., SENIOR VICE PRESIDENT, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

Asia Hearing on "Information Controls, Global Media Influence, and Cyber Warfare Strategy"

Testimony before
The U.S.-China Economic and Security Review Commission

May 04, 2017

China finds itself in a remarkably fortunate position. The United States, its chief strategic competitor, has been weakened by intractable wars in the Middle East and political turmoil at home. Russia, which could be a strategic competitor, has chosen instead to partner with China against the U.S., and in any case, is in decline as a great power. No other country in the region or outside poses a significant challenge to China.

It would be an overstatement to say that Xi Jinping inherited a crisis, but the trends for China and, more importantly, for continued Party rule, were not positive when he arrived. China faces serious political, economic and environmental problems, but the Xi government has worked energetically to reduce political risk. Xi's efforts to reduce corruption, centralize intelligence tasking, and reform and modernize the PLA have the added benefit of reinforcing Xi's authority.

Controlling the internet and information play an important part in this effort. China's information policy has four goals. They are to reduce risks to political stability and continued Party rule; promote Chinese content and technology; reshape global rules to favor China's interests; and defend against perceived U.S. hegemony. China, in the last few years, has created policies, regulations and to make the information environment in China more controllable, most recently with the "National Cyberspace Security Strategy" released late last year.

China, along with Russia, promotes a reassertion of national sovereignty. This reflects in part an erosion of western and American influence and in part recovery from the collapse of communism. We could call this reassertion the "authoritarian alternative," an effort to replace the U.S.-led international order and to rebalance the relationship between sovereignty and "universal" values. Russia and China reject the idea of universal values, saying these are in fact 'western values" that are inappropriate for non-western nations. This line of reasoning has some appeal with some non-aligned nations, and China has benefited from the Russian campaign to exploit the Snowden leaks and other purloined materials to attack the idea of democratic institutions and universal values.

Before 1945, sovereignty was absolute within a nation's borders. Non-interference in internal affairs was the norm for state behavior. Since 1945, the predominant view is that there are

issues, such as human rights, that transcend borders. The UN Charter, the Universal Declaration of Human Rights, and the agreements establishing the World Trade Organization, are all examples where nations including China, have voluntarily surrendered some of their sovereign authorities. Fundamentally, Russia, China and other authoritarian regimes seek to reclaim sovereign authority. The goal is to give national sovereignty greater influence, legitimizing government control of national networks, and to restore older concepts of inviolable sovereignty.

In the last few years, China has articulated a new and coherent view of cyberspace that places sovereign control at the center of national and international policy. China's new National Cyberspace Security Strategy assert that "National sovereignty extends to cyberspace, and cyberspace sovereignty has become an important part of national sovereignty." The concept of cyber sovereignty is part of this reassertion. President Xi defined the elements of cyber sovereignty at the 2016 Wuzhen conference as "respecting each country's right to choose its own internet development path, its own internet management model, its own public policies on the internet, and to participate on an equal basis in the governance of international cyberspace—avoiding cyber-hegemony, and avoiding interference in the internal affairs of other countries."[1] *China's views on sovereignty seeks to reassert the dominant role of states within the context of an approach to globalization that seeks to amend rules, institutions and, standards in ways favorable to its own interests and more consistent with its own political views.*

This vision has been accompanied by a substantial reorganization of the State and Party apparatus for dealing with cyberspace, including the creation in 2014 of a Central Leading Group for Internet Security and Informatization, chaired by President Xi, and a new Agency, the Cyberspace Administration of China (CAC). Other actions to reinforce domestic control include restrictions on Virtual Private Networks and disruptions to the service they offer, and new limits on social media by deleting posts and closing accounts. The Leading Group sets policy and the CAC implements, improving China's control over domestic networks and internet users. These changes are the result of a deep interest by President Xi in extending control over cyberspace, which he has identified (along with corruption) as a key threat to political stability and continued party rule.

China has been successful in extending sovereign control to the internet. As the internet is based on physical infrastructure located within national territory, it is easy to control many functions. Beijing blocks access to and traffic from foreign sites of which it does not approve. This does not come without economic costs, as Chinese researchers and businesses cannot access useful information and services, but this is a price that Beijing is willing to accept. China the only country to impose national control over the internet and other countries are moving toward greater localization of data and apply national laws to the internet. The is not the borderless one-world that American technologists so confidently expected, but neither is it the dreaded "fragmentation" of the internet. What is interesting is that while many countries are asserting control over the internet, here is very little effort in China or elsewhere to coordinate or

[1] http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml

multilateralize these controls, reflecting widely disparate views on privacy and the treatment of data.

The impetus for greater control and reducing risk motivates a parallel effort at industrial policy. China's motives in expanding its information technology sector are both commercial and political. Since the 1980s, China has sought to build a strong information industry and we have seen repeated efforts, such as the push for indigenous innovation, to achieve this. China has not hesitated to extract concessions or block foreign competition in the IT sector in pursuit of this goal. China employs various strategies to displace western companies, using non-tariff barriers, security regulations, procurement mandates, the acquisition (both licit and illicit) of foreign technology, and through strategic investments and the acquisition of western firms.

China is driven by the same supply chain security concerns heard in the U.S. and there is a long-standing belief in China that western technology is inherently untrustworthy. It is troubling that this most likely reflects China's own intentions rather than the actual behavior of western companies. China legitimate desire for economic development is complicated by powerful commercial motives to use national investment produce globally dominant national champions in many different industry sectors.

The Chinese are aware of these limitations and have developed a new approach: to buy western companies rather than create a Chinese counterpart (China uses a similar strategy in its latest effort to create a domestic semiconductor industry, with a well-financed strategy to create a domestic industry intended to displace foreign suppliers). Creating a counterpart company and blocking western services (such as Weibo instead of Twitter) was an effective policy for controlling social media use by a domestic audience, but it is not effective overseas. It is too early to assess the effect of China's media purchases, [2] but when Alibaba bought the South China Morning Post it was with the explicit goal of creating more positive coverage of China.[3]

China's informational campaign seeks to use western media formats to shape foreign views of both China and the U.S. in ways favorable to it (Russia uses RT in a similar fashion). The Global Times, the effort by Peoples Daily to cooperate in shaping overseas opinion, is only slightly more persuasive than RT. It is more likely that the Chinese government will encourage new owners to ensure that favorable views of China are presented in films or the media - a kind of soft propaganda - rather than to win support for specific Chinese positions.

Russia has used its long experience, dating back to the Czars, in what we would now call information operations. These operations to produce cognitive effect and shape the thinking of opponents and neutrals are a central element of Russian military doctrine and what Russia calls "New Generation Warfare." In contrast, the Chinese do not have similar military doctrine on opinion shaping.

---

[2] China and Russia may wish to recall the words of Lu Xun: "Lies written in ink can never disguise facts written in blood"
[3] According to Alibaba's vice Chair.https://www.nytimes.com/2015/12/12/business/dealbook/alibaba-scmp-south-china-morning-post.html?_r=0

China's own information operations suffer from a lack of subtlety and attractiveness. Chinese propaganda is effective in shaping the views of a domestic Chinese audience, but has far less traction in other countries. While these information operations are very effective in influencing the views of a Chinese audience, they are much less successful in other cultural and linguistic arenas. The opportunity to play the role of supernumerary in the "China Dream" does not attract many adherents.

China and International Cooperation in Cybersecurity

Multilateralizing China's online restrictions plays a tertiary part in this effort. China's primary focus is domestic. It's primary negotiating goal is to avoid agreements that could increase political or military risk - Chinese interlocutors have expressed concern, for example, that a specific reference to the inherent right of self-defense[4] could legitimatize U.S. cyber actions against China. Promoting Chinese view on sovereignty, internet governance, or cyberwar come second to these domestic goals.

China has found a willing partner in Russia for its international efforts, but this is a marriage of convenience, not love. The Russians distrust the Chinese and the Chinese do not hold the Russians in high esteem. But both are united in this uneasy partnership by their desire to push back against the U.S. and the international order it created. They seek multilateral assent to norms that reduce the chances of events similar to the "Arab Spring" in their countries, to what they see as internet-inspired domestic unrest, something that both China and Russia fear.[5] Chinese interlocutors say that Social media and "Color Revolutions" are a threat, but that the party is in the process of learning how to deal with and use them for its own purposes, such as by using government employees (the Chinese equivalent of Russian media trolls) to plant millions of positive messages about the party and Chinese policies on social media sites[6].

China has a consistent approach to multilateral cybersecurity negotiations, to promote sovereign control and to safeguard its security and commercial interests. China's new National Cyberspace Security Strategy talks about "increasingly fierce competition" to "seize the right to develop rules." China has increased its involvement in international standards-making (previously the domain of western companies) for information technology both to garner commercial advantage and to revise standards, protocols, and architectures to improve government ability to control cyberspace. China is *as yet unskilled in wielding its new power and influence, and while it is adept in pursuing its economic interests overseas, it is less effective in advancing its political agenda.*

---

4 Article 51 of the UN Charter

5 Chinese commentators expressed a degree of schadenfreude over the news of Russian interference in the U.S. elections. There sense was that the Russians had only done to the U.S. what the U.S. had been doing for years to governments it opposes.

6 https://www.washingtonpost.com/news/monkey-cage/wp/2016/05/19/the-chinese-government-fakes-nearly-450-million-social-media-comments-a-year-this-is-why/?utm_term=.9d718382c7fd

These multilateral activities include the Shanghai Cooperation Organization (SCO), discussions among "BRIC nations," efforts to promote their "International Code of Conduct for Information Security, and Chinese positions in the negotiations in the UN Group of Government Experts on information security (GGE). China has also tried to use its first World Internet Conference in 2014 to gain support for its ideas of "cyber sovereignty" and a multilateral approach to internet governance. (which would give governments a dominant role, in contrast to the current multi-stakeholder model). In each of these efforts, however, Russia and China have met with only mixed success. On internet governance, the Chinese appear to have accepted the IANA transition, where the U.S. government ended its contractual relationship with ICANN, as a legitimate change in internet governance that had made the issue less salient. This may also reflect greater Chinese confidence in their ability to manage the internet, to extend sovereign control over their own networks, and to reduce political risk.

Russia and China introduced their Code of Conduct[7] to challenge the international status quo and shift the terms of the global debate over cybersecurity and online freedoms in their favor. The Code essentially redrafts international commitments to increase the rights of the state vis-à-vis the rights of citizens. The chief problem with the Code is that many of its provisions are obviously intended to redefine and limit other international commitments, and in particular the Universal Declaration of Human Rights. Most Western observers believe it is an effort to amend international agreements in ways that strengthen sovereign authority at the expense of existing international commitments. Russia and China revised the Code in 2014 to soften these provisions, but even with these changes, it has attracted only limited support. U.S. opposition to the Code has been unwavering.

Similarly, the SCO has not met expectations for global influence. SCO is the poor man's NATO. It lacks the deep cultural affinity and shared historical experience that shapes the transatlantic alliance. While it reached agreement in 2009 on information security, its one major achievement has been to provide a multilateral veneer to the Code of Conduct. SCO has held one cybersecurity exercise, in 2015, focused not on a defense of critical infrastructure but on preventing Arab Springs by coordinating the removal of "terrorist" content on websites and social media.[8] This is a very different approach to cybersecurity, inward looking and focused on stifling dissenting views.

While Russia and China signed a cybersecurity pact in 2015, this was done largely for show, with intention of annoying the Americans. The pact was a Russian diplomatic maneuver to which China acceded. Some call it a "nonaggression pact," which should give the Russian pause, and to date there is no evidence of tangible cooperation between the two nations on cybersecurity.

---

[7] https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf

[8] First network anti-terrorism exercise successfully held in Xiamen, Xinhua, October 2015, Peter Wood, http://news.mod.gov.cn/action/2015-10/14/content_4624236.htm; Peter Wood, China Conducts Anti-Terror Cyber Operations With SCO Partners, Jamestown, October 2015, https://jamestown.org/program/china-conducts-anti-terror-cyber-operations-with-sco-partners/

Russia and China have made efforts to use the BRIC nations as a multilateral counterweight to the western alliance, with various initiatives, funds, and agreements that are announced at every BRIC meeting. These are also largely for show and noticeable for absence of any meaningful commitment of resources. The idea of the BRICs as a political alliance faces fundamental problems. It is worth bearing in mind that the term "BRICS" was coined by a business consultancy to describe economic trends and it suggests a certain poverty of imagination that Russia and China have embraced it as a political vehicle. To the extent the BRIC's share a goal, is it discontent with the current order of international relations rather than any deep cultural affinity or shared values, but China has so far been unable to capitalize on this diffuse discontent.

Attitudes towards fundamental rights create an immediate challenge for cooperation among the BRICs. India and Brazil are democracies with a strong commitment to free speech. However much they distrust the U.S., they are unlikely to abandon this commitment. Nor are China and India likely to forge a strategic partnership. If anything, they are strategic competitors. In simple terms, while India and Brazil may enjoy playing Russia and China against the U.S. and its allies, they are not going to move into the authoritarian camp. The NetMundial Conference, organized by Brazil in response the Snowden revelation of U.S. surveillance, ended by producing a powerful endorsement of democratic freedoms online that only Russia, Cuba and India opposed (somewhat sourly) and in retrospect, Indian officials say that they regret this opposition.

This is a somewhat threadbare tapestry of diplomatic accomplishment in international agreement in cybersecurity, orchestrated by Russia and tolerated by the Chinese, with little tangible effect other than to create concern among gullible western observers and impose obstacles to any agreement on western terms. However important these maneuvers are to Russia in its effort to restore its international position, they are of secondary importance to China. The authoritarian alternative is simply not that attractive for most people. China's rulers, however, do not care. There is still a degree of insularity in China's views, reinforced by the belief that its vast population and growing wealth allow it to set its own course.

Cybersecurity Negotiations

Chinese (and Russian) views on international negotiations on cybersecurity are shaped by defensive requirements, to protect themselves from what they see as a hostile and technologically superior U.S. whose actions are largely untrammeled by international law and are motivated by plans to disrupt Chinese (and Russian) society and replace the current regimes with ones more in its own image. China, if anything, takes a more intransigent position that Russia in international cybersecurity negotiations. This may in part reflect the greater confidence Russia has in being able to control these negotiations, given its long history and experience in arms control. The Russians are the masters of this game and the Chinese, while increasingly skilled, remain more cautious and less flexible.

The focal point for international cybersecurity negotiations are the meetings of the UN GGE.

The Report of the 2013 GGE reshaped the international discussion of cybersecurity. It recognized the requirement for nations to observe their international commitments in cyberspace, including the centrality and applicability of the UN Charter, International Law (including both International Humanitarian Law and the Universal Declaration of Human Rights), and national sovereignty. This report, later endorsed by the General Assembly embedded state practices in cyberspace in the existing framework of international relations and law. The 2013 Report and the consequent 2015 Report also identified a set of initial norms and CBMs, also endorsed by the General Assembly.

China was the nation that most strongly opposed these commitments, particularly to the applicability of international law, and by the end of the negotiations, it was the only nation that opposed them. It is likely that China finally agreed only because Presidents Xi and Obama were to meet at Sunnylands the day following the GGE's conclusion, and the Chinese did not want to place their leader in the position of explaining why China was the only country to oppose international agreement on cybersecurity. While China has grudgingly accepted the applicability of international law, it continues to show ambivalence over the treatment of cyber warfare, and it supports Russian proposals that existing international law is insufficient for cyber conflict and must be amended and expanded.

China promotes a very different vison of international order that reasserts the primacy of national sovereignty and devalues international agreements that constrain sovereignty, particularly the Universal Declaration of Human Rights. China is not alone in this and receive significant support from some nonaligned nations, notably Pakistan, Egypt and Malaysia, and from Russia.

China pursues international agreements that would reduce political risk and move in the direction of more traditional views of national sovereignty (increasing governmental authority over the internet. At the same time, it takes a defensive position in the international discussion of cybersecurity norms., seeking to block agreement on norms that could potentially be used to justify action against China for its *cyber activities, such as a norm reinforcing the right to use Counter-Measures (e.g. retaliatory action that do not involve the use of force, such as sanctions or indictments).*

China, along with Russia and some Non-Aligned Movement nations have called for a ban on cyberattacks and cyber "weapons." China has said that cyberspace should be a "zone of peace," while western nations say that we should recognize the widespread adoption of cyberattack for military purposes (including by Russia and China) and that its use should be regulated by international humanitarian law, as is the case with other military activities. These fundamental disputes over the extent to which sovereignty applies and the legitimacy of cyberwar shape international discussion of norms Chinese negotiating positions on cyber war reflect more than anything else the disconnect between the positions China's Foreign Ministry takes in international negotiations and China's actual military policies – the most salient example being the Foreign Ministry' steadfast calls for the demilitarization of space that continued until the day after China's 2009 ASAT test. The Chinese do not find it anomalous to call for banning

weapons in cyberspace at the same time they actively pursue the development of such weapons and plan for their use.

Cyber Operations

Chinese negotiating positions do not reflect the actual capabilities of the PLA, which the Chinese believe are still significantly inferior to those of the U.S. Those familiar with China will not be surprised to learn that there is something of a disconnect between the military and foreign policy establishments. Paradoxically, PLA modernization and the public admission that China has something similar to the U.S. Cyber Command could make it easier to hold bilateral military talks with the Chinese.

"Winning informationized local wars" has been a theme in Chinese strategy for years. Recent organizational changes make this a more achievable goal, but in the long term. China's 2015 Military White Paper acknowledged China's plans to build capabilities for offensive cyber operations and to organize them in the new Strategic Support Force. The White Paper identified outer space and cyberspace as the "new commanding heights in strategic competition."[9] Chinese interlocutors do not see cyber as a weapon of mass destruction. Chinese military doctrine for cyber operations appears to be scenario based and limited, although some PLA representatives say this may changes when the Strategic Support force reorganization is complete in 2018 and develop broad doctrine and strategy (noting that it took the U.S. years after the creation of Cyber Command to develop doctrine for offensive cyber operations).

The most interesting thing about Chinese planning for cyber operations is that it seems to be specific to a few scenarios, part of a larger package of weapons and attacks intended to defeat American carrier battle groups in the South China Seas and the Sea of Japan. Cyberattacks would be combined with electronic warfare, high-speed anti-ship missile strikes, and anti-satellite activities to defeat deployed U.S. forces. Chinese planning and doctrine for cyber operations do not appear to have the general applicability found in U.S. cyber doctrine and planning. This may reflect limitations in Chinese current military planning and organization, or China's larger strategic orientation, and this could change as the new Strategic Support Force matures. We may be guilty of "mirror-imaging" when it comes to explain Chinese planning for cyber operations, attributing to it strategic and global considerations similar to those that guide that guide U.S. thinking but not necessarily China's.

These differences in doctrine, strategy and capability, create a divide in Chinese and American views of cybersecurity that complicate negotiating efforts but also helps us to identify where agreement may be possible and where it is not. China's primary concern is internet content and its domestic political effect. America's primary concern has been espionage and the risk of attack on its domestic critical infrastructure, something that does not appear to be a central part

[9] **China's Military Strategy: The State Council Information Office of the People's Republic of China, May 2015, Beijing,** http://www.chinadaily.com.cn/china/2015-05/26/content_20820628.htm

of Chinese planning for cyber operations (nor is there any indication that China has mounted a campaign to subject the U.S. to a "death by 1,000 hacks").

This means that the space for agreement will be found in a discussion of international security that take into account China's fears about domestic political stability. The U.S. has some leverage in discussing cybersecurity with the Chinese. The Chinese fear Cyber Command; this means they will discuss restraints on cyber war. Some Chinese worry that a "techno-nationalist" approach to information technology will create economic damage, and China worries about its own vulnerabilities to hacking and cybercrime.

China and the U.S. will never approach human rights in the same way, *but while there will be constant sparring over freedom of expression in any negotiation, and while it is essential to hold China accountable to the international community for its* UN commitments to protect human rights, the areas of potential agreement involve avoiding miscalculation and misunderstanding in military operations, limits on espionage, and cooperation in cybercrime, subjects where both sides share common interest in avoiding miscalculation, controlling the potential for escalation, and cooperating to prosecute actions in cyberspace that are illegal in both countries.

In private, PLA representatives accept the U.S. ability to accurately authenticate the source of an attack. This does not yet appear to have greatly affected PLA planning for cyber operations. In the event of conflict, both sides intend to attack each other's command and control networks, weapons systems and reconnaissance assets. This is unavoidable, nor is it in the U.S. interest to agree to constraints that we would observe and others would not, or that do not fit with state practice in conflict. There would be benefit, however, from establishing formal mil-to-mil exchanges on cyber operations, the adoption of bilateral and regional confidence building measures, and the creation of mechanisms to reduce the chances of miscalculation or misinterpretation.

The Chinese say they are open to improved communication to manage the risk of cyber conflict and to increase stability. One obstacle is that the Chinese do not always seem confident of their own cyber capabilities when compared to the U.S., making them hesitant to pursue formal discussion. They believe that the disparity between U.S. and Chinese military cyber capabilities is so great that it could be awkward for them to meet. One pre-condition for expand mil-to-mil discussion may be the need to wait for PLA reform to complete, but it may be possible in the next few years to have serious discussions of cyber operations through flag-rank exchanges, conferences, and other vehicles. The U.S. would need to carefully consider in pursuing bilateral exchanges the risk that it could unintentionally instruct China in how better to organize and plan military cyber operations.

Espionage is no longer the most salient topic. China appears to be living up to its commitments under the Obama-Xi agreement. The language of this agreement was carefully crafted by the U.S. to allow both sides to continue to engage in political-military espionage. It is not an agreement to end cyber espionage. China's reasons for agreeing to this owe as much to

President's Xi's own agenda as to U.S. pressure. The agreement supports PLA modernization and reorganization by ending PLA units' cyber espionage moonlighting to augment their incomes. It advances Xi's goal of centralizing control of intelligence collection and assets under his control. The outcome of the agreement is likely to be a more effective and focused Chinese intelligence system, an unexpected consequence, but so far, Chinese commercial espionage against U.S. companies appears to have has decreased.

The Obama-Xi agreement showed that China's behavior and policy can still be influenced through engagement at senior levels, through realistic proposals, and with the threat, implicit or otherwise, of penalties, but it is far more difficult to do this than it was twenty years ago. U.S. policies need to adjust to a more assertive and independent China to identify where there is room for mutual understanding and where it will be necessary to build coalitions with like-minded nations to oppose further encroachments on universal values and the rule of law.

U.S. policy itself needs to be more assertive. Ultimately, the Chinese are pragmatic and will accommodate American concerns if persuaded it is best to do so. The West has a better hand to play (even if we do not always play it well), the Party's rule is fragile, and China's economy, despite its size, cannot grow without access to the West. A good first step, one where the U.S. might be able to persuade Europe to join us, is to insist on reciprocity in the treatment of foreign and Chinese companies. Reciprocity should be the catchphrase of China policy. The first step requires an honest assessment of how American views of the international relations will need to change from expectations in the 1990s of perpetual American predominance to fit a more world of greater conflict and competition.

PANEL III QUESTION AND ANSWER

CHAIRMAN BARTHOLOMEW: Thank you. Very sobering testimony from both of you. We'll start with Dr. Wortzel.

HEARING CO-CHAIR WORTZEL: I have a couple of questions related to the whole concept of a Cyber Westphalia. I mean it flies in the face of what has been established U.S. policy, that there's kind of a global commons.

DR. DEMCHAK: Correct.

HEARING CO-CHAIR WORTZEL: And if we go down the route you suggest, it seems to me that we begin to--first of all, we're going to accept cyber sovereignty and each country is going to control its own Internet space. But creating this alliance would then for me mean we're going to be talking about even new programming languages, creating secure and resilient supply chains inside the alliance, which may or may not solve some of our supply chain problems.

And a large part of what I see as the industry would probably be appalled by the fact that they might lose access to what they hoped would be a huge market because they couldn't turn this stuff over. So I mean, I don't mean to challenge your concept. It's a challenging concept, but I'd like to hear your response to that.

Jim, what you describe is a suite of campaign plans. You talk about a scenario-specific use of instruments in cyber. Then what you're talking about is a suite of campaign plans, which the Chinese already have, with annexes that would dictate strategic operational theater level and tactical cyber attacks, and penetration at least of probably U.S., Japanese and Taiwanese systems prior to that.

How do you form the kind of resilient alliances among the targets to counter those plans? I guess--

CHAIRMAN BARTHOLOMEW: We have plenty of time so take your time in responding.

DR. DEMCHAK: Thank you for the questions. I'm going to take them as I wrote them down. Number one, cyberspace was never a commons.

CHAIRMAN BARTHOLOMEW: Never what?

DR. DEMCHAK: It was never a commons.

DR. LEWIS: Commons.

CHAIRMAN BARTHOLOMEW: Thank you.

DR. DEMCHAK: It was always paid for, built by, operated by firms who operated on a peer or pay basis. So either I as a network accepted you as a peer network or you paid me.

Secondly, it never was a commons because it didn't matter where it went, it always came up on somebody's sovereign territory, and somebody always had something to say about what that meant in that sovereign territory.

Side note. A lot of folks have said one can't parse cyberspace. That is objectively wrong. Most of the IT capital goods companies who say one can't break up operations do it also operate globally with HP France, MS Germany, HP this, Apple Italy, etc for every country. The firms have to comply with all the other laws in these countries. That's why all those countries who make their own cyber rules will make these firms comply in any case.

So, number one, it never was a commons. Number two, it never was going to be our

choice to keep it open. The argument in my various works and also in the testimony is that it has actually harmed us to refuse to recognize the cyber sovereignty of some states. It energized the Chinese to go and change the international debate because we wouldn't leave them alone on the topic.

We not only said that you had to not close off your Internet, but it's an automatic democratizing element, and we want you to include it as we mean for you to use it. And that, needless to say, was not a pleasant thing to hear, and they weren't pleased.

Thirdly, for most of the time in which we've called it a commons, it comes from a peculiar part of the United States where we have these folks that grew up in universities working on this thing called the Internet, and that Internet was funded largely by U.S. government funds, and those U.S. government funds made that a public good.

So if you're a student, it's a public good. It's free; it must be so. And it must always be so. And it came from the '90s from these folks with this narrative that says it's free, it's a commons, and governments have to stay out.

Now, at the same time, you see the build of the IT capital goods industry using this very shoddy failure-prone language, or at least fault tolerant language, and they didn't care about democracy, but they sure as heck cared about that government out of my, out of my activities, and so by the time you get to our foreign policy, we have people who don't know how it's built. I'm serious. In 2011, I was at a workshop where senior people came to me privately, and they were making policy statements, but they did not know how the fundamental Internet was built. Frightening.

And they said, oh, that sounds good. It's a commons. It's democratizing. Isn't that wonderful? And along comes the IT capital goods industry, and see that's why us alone of all industries in the world can never be regulated because, you know what, we'll die. No you won't. No one does.

And you are a part of regulated industries, and furthermore we've seen the movement of ISPs onto telecommunications agencies, who are intrinsically regulated as phone, post-telegraph companies and have been throughout the world. In fact, most of the world, outside of this little weird little ten percent have moved their telecommunications agencies into putatively commercial phone systems, but they own the same infrastructure.

It doesn't take very much to go back and go, you know, on a side note, can you, can you cut off this neighborhood, half of that province, because they're used to it. So it never was our choice. We just told ourselves that.

And, finally, at the end of the day, there was never going to be a future in which China didn't rise to a center. It was simply going to happen. The only question is how fast it happened. And what we see is that in unprecedented rates, the Chinese have acquired resources to come back out and buy critical technology companies.

Legally or illegally they get these resources, and now they compete with us in our markets, and our folks say no, no, no, you can't regulate us because we want to have access to the Chinese markets, and how well is that working out for you? Seriously, how well is that working out for you?

Do you get the access? You get the access for the time that you still have something that a mercantilist power doesn't have. And I only tell you one other thing. For 11 years, I taught

international management, not business. That's accounting. International management. And Chinese business managers for their own survival--by the way, I say this with sympathy--for their own survival in their affective, high-powered, distance, clan-based society, they have to operate this way, very Weberian. For their own survival, that's how they operate.

And you go and watch those internal business practices, and imagine your world operating on those business practices, and that's why I'm saying we need to start thinking about how we survive, not on whether we convert them to us at this time.

I hope that answered your question. Thank you.

CHAIRMAN BARTHOLOMEW: Jim.

DR. LEWIS: Sure. Thank you. So you said suite of campaign plans and how we might get around it. It's worth noting that when, in that suite of campaign plans the Chinese look for ways to combine hypersonic missiles, electronic warfare, anti-satellite weapons, as well as cyber. So we're looking not only at a suite of plans but a suite of attack modes that are intended to I think largely defeat the U.S. in the air and maritime domain, and carrier battle groups are a primary target.

The Chinese weakness is in allies because they really don't have any. I guess you could count North Korea as an ally. I'm not sure if that's good, but they lack both effective diplomacy and they lack the formal alliance structure that the U.S. has, and this is a significant weakness for them.

The Chinese know this. They know their military is not equal to the U.S. They may hope to eventually reach that point, but they would tell you they're at least a decade away from that, and so for now they'll seek to avoid conflict.

They'll seek to do things that fall below the level of the use of force so that they can't--remember their fear is that we will seize upon some excuse to retaliate against them. A Chinese admiral once told me that anything--the U.S. does whatever it wants, and then says it was self-defense.

So I think that's their view, and in some ways we can exploit that, but the way to exploit it is through a more nimble diplomacy, through closer relations with key allies, particularly Japan and Australia, and giving the Chinese the sense not that they're being encircled, but that there is no way they can achieve military dominance in the region.

CHAIRMAN BARTHOLOMEW: Commissioner Stivers.

COMMISSIONER STIVERS: Thank you for your excellent testimonies.

I'd like to ask you a little bit about the U.S.-China cyber agreement last year. I can tell you that even though I was a member of the Obama administration, I was privately very skeptical that this would make any progress. Frankly, I didn't believe that the Chinese would live up to any of the agreement, the promises and commitments it made in that agreement, but it seems to me that there has been some progress in terms of Chinese cyber hacking on the U.S.

FireEye reported an overall decline in China-based intrusion activity against public and private sector organizations. So it seems that, so what this tells me are two things. First of all, that there should be no doubt that the central government in Beijing has power to stop hacking if it wants to on the U.S., and likely it was either government or military entities that were doing that, if they can turn it on and off that easily.

The second thing it tells me is that high level engagement at the very top can really make

a difference on this and frankly on other issues also.

Do you agree with the information that the Chinese have kind of scaled back their hacking since that agreement? And what other conclusions have you drawn from since then?

DR. LEWIS: Well, I followed the negotiating process very closely at the time and met with both, with Chinese officials to discuss it and American officials when they wanted. So I've been interviewing companies like FireEye, and all of them agree that Chinese behavior has changed, that the number of incidents has gone down.

So there's some useful lessons we can draw from that. The first is while the U.S. was surprisingly skillful in its diplomatic efforts in the use of threats of sanctions, and we were fortunate that the Chinese were in a position that we could take advantage of with the Xi visit. They were very, very concerned that he not be embarrassed on his visit so the threat that you would announce sanctions against PLA units the morning of his visit was much more influential than we would have expected.

So there were leaks that supported this view. And so it was a relatively skillful effort to manipulate the Chinese, but that's only half the story. The other half of the story is that the agreement serves Xi's purposes. I was told in April of 2013 that Xi was trying to assess the scope of Chinese espionage activities against the U.S., and he discovered that most of them were not done at his behest.

Most of them were PLA units seeking to make money, and so one thing to remember is the PLA, and this fits into the modernization effort, the PLA is not a Western military yet. It may not be a Western military. It's more like a Southeast Asian military where it's not unusual for senior officers to have business enterprises on the side.

I used to work with one Southeast Asian country where the Air Force Chief of Staff and his fellow generals also owned an airline; right. It's unthinkable in the Western context.

CHAIRMAN BARTHOLOMEW: Not so much.

[Laughter.]

CHAIRMAN BARTHOLOMEW: It might be changing.

DR. LEWIS: I hope not because it tends to distract them from what should be their primary mission. And so Xi was eager, one, to get control of his intelligence resources so that they were doing what he wanted. They were collecting what he wanted and not freelancing.

Two, he wanted to get the PLA to focus on its primary mission, which is military. He wanted to professionalize it.

And three, he wanted to show that he was pushing back against corruption. I mean there's a lot of debate is the anti-corruption campaign for show or is it for real, and it's clearly a mixture of both. So he, he found it beneficial for his own purposes to agree with Obama to end commercial espionage.

Now, it's important to note, and this is maybe the kicker to this, is the language is a little convoluted because the language permits continued espionage. This was at the U.S. request. The U.S. wrote language that was intended to allow us to continue to spy on China for political military purposes. And the U.S. was fairly frank in the negotiations with their Chinese counterparts that we recognized that that meant that they could spy on us, not to help their companies, not to steal White House paint, but for political military purposes.

And so in some ways having an agreement that helps Beijing get better control of its

intelligence apparatus and is better able to target them on collection that serves national purposes may mean that we could see a resurgence of more conventional espionage from the Chinese as they move away from commercial targets.

COMMISSIONER STIVERS: Thank you.

Dr. Demchak.

DR. DEMCHAK: I agree with everything my good colleague has said. One of the things I found interesting was, of course, the lack of enforcements, but nonetheless something happened. But, in particular, as a statement about how you consolidate control, it certainly is consistent with that.

If you look at the reorganization of the PLA, most folks trying to get control would not take something that had four units and turn it into 12 or 15 unless you needed to break it up in order to know what the 12 or 15 were doing in order to control them. So I think this is very consistent with that.

The other thing is in sympathy for the Chinese, speaking as someone who studies large-scale complex systems, they have had an enormous number of people for two to 3,000 years, and they always think first and foremost how do I keep the security of this crowd of folks who could be doing anything to us? And in that regard, when I look at many of the things that they do, I must confess, were I Chinese, I would do exactly the same thing, and I hope you understand my remarks are taken with that note. It's just that I prefer that we survive at the same time.

And I also think the agreement is only part of the story, that these are agreements that can change at any time, and the way the calculations will proceed is depend on who is considered to be in a better power position in cyberspace. By that I mean the resilience of the entire society, not just whether or not you have a cyber command.

In cyberspace, no one is a robust cyber power today, but if the Chinese get the impression that they are more robust than we are, I don't expect these kind of peer power accommodations to go on in practice.

COMMISSIONER STIVERS: Thank you.

CHAIRMAN BARTHOLOMEW: Commissioner Shea.

VICE CHAIRMAN SHEA: Thank you very much for your testimony.

One question for Dr. Demchak and then one question for follow-up on this conversation for Dr. Lewis.

Dr. Demchak, I did not read your written testimony, I confess, but I did listen to you intently, and I intend to read your written testimony afterward.

[Laughter.]

VICE CHAIRMAN SHEA: But I just want to get--you seem to make a lot about demographics.

DR. DEMCHAK: Correct.

VICE CHAIRMAN SHEA: And you say, I did read this sentence: The demographic scale is the major Achilles heel of the consolidated democracies. And you said there are about 900 million. Okay. Then I'm thinking, well, what about India?

CHAIRMAN BARTHOLOMEW: That doesn't include India. Yeah.

VICE CHAIRMAN SHEA: Yeah, India is going to be the largest by population country in the world.

COMMISSIONER STIVERS: Probably is already.

VICE CHAIRMAN SHEA: Chinese demographics are terrible. They're going to get old probably before they get rich. The Indian population is incredibly young while the Chinese population is skewing older. So I don't--I'm just curious about the math and the demographics.

DR. DEMCHAK: One of the points that I make is that, the ones I counted were what I call "consolidated democratic civil societies." India is a democracy. It is a very large democracy. India has not yet succeeded in educating the population in the same extent it would like to do. It has a top 250 million folks in India are very well educated, a lot of them here from us.

And in international management, particularly in communication styles, you have these things called neutral speakers versus affective speakers. When they're educated with us, and they go out as what we call neutral speakers. But the other 800 million or so are affective speakers.

The difference is profound in organizational terms. In the kinds of organizations that we have, we have low-power distance. We tend to have nuclear family, we have nuclear family orientations, and we tend to be impersonalized.

In affective cultures, you have high-power distance, clan-based and highly personalized relationships. That's what they are. That's what we are. And it has nothing to do with anything other than where you were raised and where you're educated. I fully want India to survive as a democracy because we need her, desperately need her. There are struggles for her as the 800 million seek to move up, and India knows it, and it's a difficulty. It's the reason they're not in this number at the moment.

VICE CHAIRMAN SHEA: Where does India stand on this issue of Internet sovereignty or the U.S. global commons?

DR. DEMCHAK: India is quite clear on its own sovereignty.

VICE CHAIRMAN SHEA: So they side currently with China?

DR. DEMCHAK: Yes, they do.

VICE CHAIRMAN SHEA: Okay.

DR. DEMCHAK: In fact, it was the actions of the Indian government that posed a problem for a major telecommunications company that did BlackBerry. As you may recall, BlackBerry had completely secure communications that went up to Canada, and when the Indian government was able to force BlackBerry to give them access, that basically broke BlackBerry's business model.

They are very clear on having their own cyber sovereignty. They straddle this line, and we can't lose her. Part of the reason I'm concerned about us appearing individually weak, hacked, hollowed, is that nations who straddle the line will lean in the direction of someone who can give them something, give them the technologies that have surveillance, give them the money, to show up with the megabucks. And by the way, we'll operate it for you and take care of it for them, and tell them how they can listen in on all their citizens. All the while, the Chinese close down their own internal telecommunications markets to us. This is the long-term concern I have.

VICE CHAIRMAN SHEA: Okay. Thank you.

And just to follow up on a conversation about the MOU of last year, it was pointed out that it relates solely to cyber espionage for commercial exploitation, but the MOU, as I

understood it, prohibited it. So the fact that it's still going on means somebody is violating the MOU.

And I have also heard, you know, I've read the FireEye statements that, you know, there seems to be a reduction but not a cessation, as the MOU requires, that they just may have become more professional, and we just cannot identify the new actors that might be the space exploiting, stealing the information. So could you react to that, Dr. Lewis?

DR. LEWIS: Sure. Those are all good points. When it said commercial exploitation, the language was written in a way so that the classic example is the formula for White House paint, and apparently one of the big U.S. companies has a White House paint that's shinier, brighter, you know, better than any other White House paint, and it was stolen by a PLA unit, given to a Chinese paint company. There's no military benefit to that.

But you can think of technologies that would be useful in a military setting and could legitimately be stolen for military purposes, and we do the same. So I think that you would not see commercial espionage go to zero. I think what you would see is commercial espionage conducted solely for the pecuniary benefit of a particular PLA unit decline.

And that's where you see the decline. That's where you see the confusion. I mean we all know about dual-use technology, and if I swipe dual-use technology that will help a weapons program, that would be allowed under the agreement, but it could be seen as a continuation.

On the more professional note, I'm not so sure that we've seen that yet. It is true that when the U.S. has revealed that it has been able to establish the identity of an attacker, that the people on the other end immediately take severe measures to close the avenues that the U.S. used to gain that information, and you saw that recently with the Russians hauling people off and presumably shooting them. The North Koreans do something similar. Bad to be an IT systems person in North Korea, but they--when we tell them we know something, they seek--the Iranians do it--they seek to close the loopholes, and so there's a disadvantage there.

The Chinese fear U.S. capabilities in cyberspace, and so this is a sort of a dated reference, but when I used to talk to them, it was clear they thought we were the Borg, right, that we were a technologically advanced superpower whose goal was to dominate and assimilate them.

VICE CHAIRMAN SHEA: It's futile, you know.

[Laughter.]

VICE CHAIRMAN SHEA: Resistance is.

DR. LEWIS: It's futile, that's right, and they thought that was our motto, "Resistance is futile." And that still guides to some extent their policy. They--recently PLA officers told me they accept now that--this was in a discussion of Sony and the DNC--they accepted the U.S. has the ability to attribute most cyber-attacks. Whether that's true or not is another matter, but it's useful to have them think that.

So we have not seen or I have not heard of a move to a more--there was a debate after the agreement would MSS take a greater role, would PLA do less, would they reform? I don't think we've seen that yet. I do think you'll see MSS play a greater role, but we have not seen an uptick. I have not seen an uptick in Chinese capabilities.

VICE CHAIRMAN SHEA: Okay. Thank you.

CHAIRMAN BARTHOLOMEW: I think I'll go though it's hard to put all of these things together. First, Dr. Lewis, I actually have heard that after the MOU, incidents went down, but

actually since the inauguration, they've been heading back up again. I can't attribute where I heard that to, so I just, I'm just curious about that. I mean is it indeed a continuing downward trend? Maybe some of it is different definitions.

Dr. Demchak, you know, of course, the promise of access to the free flow of information was the ideal about on which Silicon Valley was based, and I'm just curious. I have a bunch of questions, but I'm just curious how Silicon Valley reacts to what you say? Have you been invited to do a Ted talk, for example?

And, you know, it has been interesting and often quite disillusioning to see how these companies have set aside their own founding values in order to be able to move forward on the commercial front.

I wonder with--all of this is separate-- but with all of this focus on Russia, if there's any evidence of sort of Russia-Chinese cooperation out there in the cyber world? I don't mean necessarily activities but how they think about it. I'm just going to put a bunch of issues out there.

Dr. Demchak, I think you're going to have to revise some of your how they do business and how we do business because now that we have a princeling model here, I think that the Chinese are going to be much more comfortable.

We try not to be political. It's a little difficult for me right now. When you talk about a cyber resilience alliance, I'm in the camp of people who believe that the whole concept of liberal democracy is under attack, and I just wonder how people put together some sort of alliance when we are struggling within our own societies for the very values that this country was based on?

We see it in France. We see it--we see it all around Europe. How, is it even possible to put together some sort of alliance when we have these own trends? You can see I have a real positive view of the world right now.

And then also, just the issue of, you know, exporting the Chinese model. Africa is a perfect example of that. We have countries where people are perfectly happy to, as you said, not--they're perfectly happy to be able to track what their citizens are doing.

Finally--sorry--a lot of issues here. It's just interesting to me as we have been through today and as we think about these issues that we do justifiably express concern about the Chinese government's ability to track what its own citizens are doing. Somebody mentioned the Internet of Things. What is always interesting to me about our society is that we have more concern generally in the public about the government being able to do that than we do about the public sector, I mean the private sector being able to do that.

So information is being gathered. There was just a story that came out that people were tracking people's use, what music they were listening to when they were listening to headphones. Information is being gathered and monetized, and so to me I'm trying to deal with that kind of balance, those kinds of concerns. Is there hypocrisy involved in this?

Again, I don't have a specific question on that, but these are just issues that I've been trying to think through as we talk about all of these things. I'd say pick one, pick two, answer what you want to answer.

DR. LEWIS: Let me start by noting that in 2013, the U.S. agreed in the United Nations in Agreement on Cybersecurity that national sovereignty applied to cyberspace. So in some ways it's a done deal. And there's a couple reasons for that--all the pressures that Chris has

described. We don't want to be King Canute and throwing chains into the sea. And when you look at Turkey or India or Russia or any of the Europeans, a number of countries are moving--it's not that they--to establish sovereign control.

And so we accepted this, and the benefit of accepting sovereign control is that it embeds cyber security in the framework of laws and treaties that govern international relations. And this is something that both the Chinese and the Russians want.

In this, the Russians are more active, and so Navalny, the Russian dissident, just said recently in a Spiegel interview that Vladimer Putin wants to reestablish Russia's position as a global leader by leading an anti-American, anti-Western alliance, and one of his goals is to use informational tactics to degrade democracy.

CHAIRMAN BARTHOLOMEW: And it's working.

DR. LEWIS: It is working, but I wonder if it's run its course. So when you look at the Russian tactics, they're often initially successful and then taper off rapidly. And so now everyone knows this bag of tricks, and the Europeans are very excited about it. They're taking steps to counter it. They may find--the Russians may find that what worked in the DNC will not work as well in other countries.

And so I think the Russians have come to the point where they may need to rethink some of the things they're doing and come up with some new tricks. That will be hard for them.

The Russians and the Chinese do have various agreements, but it's funny when you're actually in negotiations with them because you can see the Russians looking at the Chinese, trying to do like mind control. You will do this; you will do that. And the Chinese, oh, they're reading their papers, duh-da-duh-da. They ignore the Russians.

So it's a very--the body language is interesting, and it suggests that it's a very fragile relationship. The Russians are deeply fearful of the Chinese, as they should be. You have a vibrant growing economy with a huge population, and the Russians, of course, are in steep decline.

The Chinese still have some respect for us, perhaps not as much as they had ten years ago, but they have no respect for the Russians. So you don't see, you have these efforts to create the structure, the appearance of an alliance, but they aren't in any way meaningful.

I have not seen evidence that Russia and China have cooperated in cyber activities the way we would cooperate with our NATO allies or with Australia or Japan. That doesn't seem to have occurred, and part of it is the lack of a formal arrangement, the high level of distrust. When I'm in a bad mood, I tell the Russians I could break their alliance in about three months if we wanted to.

So I don't think, I don't think we see--it's not so much that they're getting stronger, is that we're having troubles exercising our own power, and they need to bear that in mind. Some things I remind my Chinese interlocutors of is in the 1970s, the then Soviets said that the correlation of forces had shifted irrevocably to the socialist camp, and I remind them that ten years later that was completely wrong. Useful to bear in mind. So it was sort of a rambling answer, but it was a rambling question.

CHAIRMAN BARTHOLOMEW: It was a rambling question. Dr. Demchak, any pieces of it? I admit I was rambling.

DR. DEMCHAK: I'm going to take them not in the order that you asked, but in the order

that it pops up. Russian and Chinese cooperation, Jim is certainly absolutely correct. The only thing that I have--all my work is unclassified. And I just have no life and I'm a voracious reader. So one of the things I would say is that the Russians are very interested in copying the Chinese Firewall in cyberspace. They are very clear on this topic that they are going to have their own part of the great substrate.

In turn, the Chinese, according to my deeply embedded colleagues, have learned some of the Russian very covert techniques. Now, in fairness, the entire global underground hacker community has moved to these kinds of techniques. The old and less mature days, when one hacked in, one stole everything one came across. In the new days, they plant a marker, much like organized crime's auto theft business model. The thief just goes in with a list of what they want, and the key is to be able to get back in repeatedly and then get exactly what one wants and obscure its extraction on the way out. So that possible change in technique feeds the concern that one of the reasons we're seeing the drop in exploitation by the Chinese is that we don't know whether they stopped or just gotten really good at being stealthy.

In addition, cyber talent working for authoritarian sides of the house. They all do it. The only time you know that it's from a country in particular is that the attacks come during business hours. And then the ones that come after business hours as they're going home doing whatever they're doing on the other side.

As for the alliance, the one great thing about cyber security right now in the US and I don't see it, there might be some edges, it is so far the most nonpartisan thing I've probably been in in my entire life.

Everyone involved, irrespective of what political position they come from, is just simply tired of being ripped off by whoever is doing it through the cyberspace. Because we were all promised a great open global "holodeck," and they're just tired of finding out that this other firm has gone under. If you lived in the company town that Nortel had in Canada, you'd really be tired of hearing about it.

And so I don't think that you could--I don't think that part, the difficulties, the political difficulties, would, in fact, get in the way of making this kind of alliance. There's a ton of engineers who would love to work together on this.

I think the critical difficulty is getting the public, I mean the private sector actors to realize their long-term viability depends on our long-term viability, that they are not going to survive us, and if we are individual little markets, we're Denmark, we're Estonia, and China has built out the 4G networks across all of Latin America and Asia and the Middle East, including Chinese operating, maintaining, updating, then who are you going to call when Ghana is attacking you, and then the person in Ghana, who is your friend, goes to the person running their 4G network and says what's going on, and they're told, oh, there are no irregularities here.

That will make China quite an extensive cyber hegemon. And our private sector actors have to understand that their chances of getting a fair deal and a honest return on investment, contract protection, currency stability -- all the things we teach in international management -- are going to decline dramatically in this coming world unless we act together.

So my thinking is that this topic is still nonpartisan. It's systemically important, and part of it is making, having the kind of honest conversations with the private sector, especially about how they are going to survive when people who don't play fair make the rules, get to come invest

and get to push you out of your market, but you don't get to do the same to theirs?

CHAIRMAN BARTHOLOMEW: I'm going to just take the prerogative and ask one clarifying question, and then I'll turn it over to Commissioner Tobin. And that is, is it possible that the cyber resilience alliance could be done without government? That their--

DR. DEMCHAK: No.

CHAIRMAN BARTHOLOMEW: Okay. I'm just, I'm just thinking of people I know who are out there.

DR. DEMCHAK: It will be a whole another paper I'd like to write, but the answer is no. Motives and the motivations are quite different. So we have to blend them.

CHAIRMAN BARTHOLOMEW: Commissioner Tobin.

COMMISSIONER TOBIN: Admiral, Dr. Demchak, I want to push further into the territory that Chairman Bartholomew was speaking to, which is this alliance, this cyber resilient alliance. You spoke about it theoretically, and we fully understand because your argument is persuasive why it's important, but can you be concrete?

You just said that government needs to be involved. Can you be specific in--if what you gave us is like the normative reality, can you give us the everyday steps that you would propose? Who's the leader? How do we build that alliance? Through what groups or functions should we do that? That would be what I would ask of you.

And, Dr. Lewis, you had a thought-provoking conversation that included after you said that China is concerned about our regional dominance and challenging the U.S., and then you spoke about THAAD in a way that related to cyber security, and I wanted to hear a lot more because I could tell that there's a story there, and I'd like to hear that.

So Admiral.

DR. DEMCHAK: No. Just professor.

COMMISSIONER TOBIN: It's Rear Admiral. Okay, Professor.

DR. DEMCHAK: Oh, no. I'm a professor. I'm the Rear Admiral Hopper Professor.

COMMISSIONER TOBIN: Ah. Grace Hopper.

HEARING CO-CHAIR WORTZEL: You can explain who Grace Hopper was.

COMMISSIONER TOBIN: No, I know who she is.

HEARING CO-CHAIR WORTZEL: Oh, okay.

COMMISSIONER TOBIN: Very well.

DR. DEMCHAK: My personal hero.

COMMISSIONER TOBIN: You've got her chair.

DR. DEMCHAK: So this is, this suggestion, this proposal, is something like 25 years in the making for me to come to the conclusion that this is the answer. And I am now putting my organization theory head on exactly that task, on how do we do that? There's a number of players involved. This is why I can say it has to be both government and the private sector has to be together, in part because I define cyber power as having two halves.

One is this systemic resilience in a country, and the second one is a more narrow, more narrow element targeted for disruption. And to be a bit of gravitas, in the old days when we used to study sociotechnical systems, you had two layers of complex system surprise. And one was just the enterprise, and the second one was critical infrastructure when you joined them together.

My argument is that cyberspace as a substrate has added two more, and that's the huge

population of bad actors--middling scrip kiddies, beyond--I'd probably be a middling script kiddie--and then there's that tiny group of what we call wicked from the mathematical idea, wicked actors, and these are a small group, but it's so talented that if they get inside, they will simply not be found.

Now, for the first three layers, resilience works. Resilience means transform the underlying substrate, get people together to pick up the pieces as they go along, and be innovative in it. But for that last little group, you have to have forward operating folks that can disrupt the business models of these wicked actors. No country can be a robust cyber power unless they play in both of those.

The first layer, the first three layers, those are massively involved with the private sector and the economic viability of a country. So when you build a resilience alliance, it's going to have such diverse players as the national telecommunications agencies, private or public. It's going to have the certs. It's going to have the producers of technologies, the designers of technologies, and it's going to have the governments because the governments, of course, have the authority to defend the country.

They have all the policies. They can help you with education. They can do all these other things that are going to be necessary. I am fully aware that transforming the underlying substrate is a major endeavor. I simply argue that it is existentially necessary. And no country, even us, can afford to do it on our own, and we will not be taken seriously unless we are considered a vibrant, and not declining, peer power on the part of China and the other folks.

So I don't have an answer on exactly how to build it. I already have a list of who needs to be in it, and then I've been looking at, of course, following very, very closely on the things that are happening in NATO and in the EU, in general, and other places in the world--Five Eyes--well, to the extent we know. And other relationships in the world. And I am, in fact, engaged in thinking that one right now.

COMMISSIONER TOBIN: Thank you.

CHAIRMAN BARTHOLOMEW: Dr. Lewis, I'm curious about just sort of your response to Dr. Demchak. Are you, are you in the same place in terms of thinking that these are the challenges, and that it's existential?

DR. LEWIS: I no longer work for the U.N., which is an advantage. But in the last week I've had conversations with a number of our European allies about this very subject, and you could get some similarities to what Chris has suggested and also some important differences.

So we are at a moment of transition when it comes to international negotiation on these subjects. We had a plan about seven years ago to build norms and confidence building measures. That plan has come to an end, largely because the international community has fractured. The Russians and the Chinese and some others are on one side, and we are on the other.

And when I say "we," the discussion now is can we create a group of like-minded nations that would cooperate? When I worked in the U.N., we used to call them weak-minded nations.

CHAIRMAN BARTHOLOMEW: Say it again.

DR. LEWIS: Weak-minded.

CHAIRMAN BARTHOLOMEW: W-E-A-K?

DR. LEWIS: Yeah. Because they sometimes had difficulty understanding where their own interests lie.

But this turns out to be very difficult to get these countries together. First, the U.S. is not sure if it wants to abandon discussions with Russia and China. That would be a bad idea, but you can pursue both avenues at the same time.

In thinking about what this arrangement would look like, a number of issues have come up. There's difficulty in defining what a collective response to a cyber action would be, and that at core of that difficulty is in how you are convinced of the evidence that someone was responsible for an attack.

So the U.S. has very good attribution capabilities. It doesn't share them with perhaps only one or two of its closest allies. And so if you had say the G20 or NATO, we would not tell you. People would have to accept on faith it was the Russians, it was the North Koreans, it was whoever. And they are willing to accept that on faith as long as they don't have to do anything.

If you say to them it was the Russians and we need to impose additional sanctions, the requirement for evidence goes way up, and they have trouble seeing how that would work. This is something we can work through.

Another issue that comes up is the First Amendment, which is peculiar, but in conversations, particularly with German officials, they would like to see, as Chris has suggested, an Internet where there are many more rules. So Germany has a law under consideration now that would require U.S. companies to have a responsible person in Germany who could be approached to remove objectionable content; right.

And at this moment, the way the law is drafted, any German citizen could make that request. There could be more formal requests from a court, but in these discussions, it's come up that, well, what might be objectionable to Germany would be permitted under the First Amendment.

In the Budapest Convention, we got around this dilemma by creating a hate speech codicil. So there's the Convention on Cyber Crime. It doesn't mention hate speech or content control. But there's a codicil that everyone else signed that says you can criminalize hate speech. We did not because of the First Amendment.

So there's obstacles to reaching agreement, but there are discussions under way on how to do this, how to create a like-minded idea. Some of the ideas that come out of non-governmental sources are not that useful. So people talk about an IAEA for cybersecurity. The IAEA is based on a treaty where everyone has agreed that certain behaviors are objectionable and they won't engage in them.

There is no such agreement in cybersecurity, and there's never going to be one in the near future, probably the mid-term. So you would find a situation--I think it's sort of hilarious to have an independent body attribute the source of an attack. You would depend on government sources. So you would end up asking either the Russians or the Americans was it you? I can tell you what their answer is going to be right now.

CHAIRMAN BARTHOLOMEW: No. We know the--yeah.

DR. DEMCHAK: So can I.

DR. LEWIS: You know, so a bad idea. You have this idea for a cyber Geneva convention. It has some useful elements, but it clearly does not have strong support in the community of nations. You have a group of outside experts who drafted the Tallinn Manual. The Tallinn Manual also does not have widespread support among leading nations. I was in a

meeting in Geneva in the U.N. where the authors said to me that they had gotten the Chinese to agree with the Tallinn Manual.

By fluke, the Chinese ambassador was walking by at that moment, and I know him. So I said Ambassador Fu, come over here. What does China think of the Tallinn Manual, and he said, oh, we hate it, and he just walked away.

[Laughter.]

DR. LEWIS: So we are very far from agreement, and in pursuing the idea of a like-minded agreement, I think what you'd see is the U.S. work with perhaps NATO partners, certainly Five Eye partners, possibly G20 partners, and it would be hard to extend beyond that. Some people say it might just have to be G7; right.

You have a model of the PSI, the Proliferation Security Initiative, which is a cooperative approach between companies and governments. That one hasn't gotten traction for some reason, but it's one of the ideas on the table.

Another idea is you need some sort of overarching set of institutions and agreements, at least on the like-minded. This is a hot topic in negotiation, but as with any serious negotiation, it's very difficult to see a path forward.

The one point that I know we agree on is the U.S. must lead. The Germans have thought about it, and they're not ready to step up to the plate. There is nobody else. It's either us or nothing, and so if we do not lead, and we're confused--we were confused before, we're still confused now. If we don't know what we want and how to get it, nothing will happen. So that's my thoughts.

CHAIRMAN BARTHOLOMEW: Thank you.

Dr. Wortzel, you've got another question. Oops, I'm sorry.

DR. LEWIS: Oh.

DR. DEMCHAK: Can I--

COMMISSIONER TOBIN: There's a piece of my question related to the THAAD.

CHAIRMAN BARTHOLOMEW: Oh, yeah, sorry.

DR. LEWIS: Sure. The THAAD one, as you know, the Chinese have had a neuralgic reaction to the deployment. It's part of--you can hear the conversations--it's part of our evil plan to encircle China and contain it. The Chinese usually say we have a grand strategy. Americans usually laugh when they say that.

But they think we're encircling them, and so they have sought over the last five years to penetrate all of the weapon systems that we have that would be used in a conflict with them to acquire the software. In most cases, the U.S. believes it has been unable to undo the damage that they've done, but that's been costly.

Part of the reason for the F-35s' expense is the need to redo software. They use it to develop their own weapons and their tactics to defeat these things, and THAAD would be a logical target for Chinese espionage. That might be as much as you can say.

COMMISSIONER TOBIN: Thank you. Yes, I appreciate that.

CHAIRMAN BARTHOLOMEW: Dr. Demchak, you had more to say, and then Dr. Wortzel.

DR. DEMCHAK: I just want a quick point on resilience. Resilience doesn't include content, objectionable content control. My background comes from the sociotechnical systems

or large-scale technical systems literature, and when we talk about disruptive surprises, we mean to the operations, to the how things work. We don't mean it in terms of political sense. I think that's the way--and the Budapest Convention, that was a good reminder. You focus on the thing you mean and then you work out that other part, but that's quite different.

CHAIRMAN BARTHOLOMEW: So you're essentially separating content from--content from mechanics?

DR. DEMCHAK: Absolutely. The telecom agencies will undoubtedly be pillars in this alliance. Absolutely.

CHAIRMAN BARTHOLOMEW: Sorry. I think we're--

DR. DEMCHAK: That's where the cables come up. That's where the servers are. That's what's going to happen.

CHAIRMAN BARTHOLOMEW: We're having more of a conversation. I just also keep--

DR. LEWIS: The one thing--the one thing to bear in mind is that we might want to separate out content, but others may not, and so that would be the negotiation.

CHAIRMAN BARTHOLOMEW: Right. And also, to me, the libertarian nature of many of the people who have the technical skills that you're talking about is yet another. When you can talk about bringing the companies to the table, the people I know who are really good at activities on the Internet are people who are suspicious of government, of government activities, how--so that's another issue that I'm just thinking through, how you bring these people into the very kind of thing that you're talking about.

DR. DEMCHAK: One of the major telecommunications companies' vice president gave a talk recently, and, to paraphrase him he said —"My position has been libertarian, but I am simply tired of being ripped off". That's where I got the phrase. He's one of the more surprising people to say that; they are just tired of it. So are we.

CHAIRMAN BARTHOLOMEW: Okay. Larry.

HEARING CO-CHAIR WORTZEL: Both of your descriptions of what any kind of agreement or cyber resilient alliance might begin to look like gives me the impression that as a minimum it would be layered. There would be some really close partners, Five Eyes like where everything is shared and everything, near everything is agreed, and then you expand it out to NATO where you have sort of agreed sets of what constitutes a threat, and then you get these nebulous G7, G20 things. I mean that's what I'm hearing, and I'd like to hear your thoughts on whether that's correct.

And then the one issue, major, one of the major issues that we've heard from the American Chamber of Commerce about, from U.S. business about, is specific to China, are these restrictions on data transfer. But it strikes me that European companies and allied companies are going to have the same problem. So I'd like your responses to how you might handle that.

DR. LEWIS: We'll flip. Okay.

DR. DEMCHAK: We have to invert the question here. Is the argument that we westernized nations should not defend ourselves, whereas China in having a huge internal market may acceptably make those restrictions on data transfer? Is it acceptable that the western corporations fight vigorously with their libertarian arguments at home and comply with the Chinese restrictions abroad, leaving the US and allies open to being exploited and resources

extracted? While I can't predict what kinds of restrictions on data transfer the Europeans will impose, however, one would presume that within an alliance, it wouldn't happen. I also do not imagine this is fortress alliance. But anyone who has that thought, no. This is an open seed market. It's just the substrate itself is being fundamentally transformed to something more secure.

DR. LEWIS: So a couple points. First, the Chinese, at least in the past, and we'll see if this resurfaces, were always intrigued by the idea of a G2, as opposed to a G7, where the U.S. and China would set the rules for the world, and you can see the temptation there. That seems to have subsided recently, but it might come up again.

So one question would be is the U.S. still capable of a diplomatic strategy that would involve engagement with the Chinese bilaterally, with authoritarian regimes, with the non-aligned countries, with like-minded countries? It would have to be a machine with many moving parts, and that was too much for the last administration although they were moving in that direction.

I think the privacy point is important, and we didn't really address it in your earlier question, but it comes up in data transfer. So this is a major problem for the Europeans and the Chinese. They naturally have different solutions. The Europeans want to regulate. The Chinese want to block and create national champions.

And that will be their way of dealing with the fact that most of the big data transfer companies are American, and the issues that come up are what are the terms for access by law enforcement agencies? You have suits now in the European Union dealing with this. You have an effort to revise the MLAT process, the Multilateral Legal Assistance Treaty process, where we exchange information to speed it. That seems to have fallen on hard times.

You have the question of how do you protect data, and when Europeans and Chinese say protect data, they mean protect data from the U.S.; right? And what I usually tell them is don't bother, we'll be able to get it anyhow, you know. I don't need, I don't need some company to cooperate to get your data. That's mainly to annoy them.

[Laughter.]

DR. LEWIS: But they are deeply concerned. And you'll see this come up this year with the debate over the renewal of Section 702 of the Foreign Intelligence and Surveillance Act.

But the issue of privacy was a stumbling block for an agreement. We largely share the views of our like-minded allies. The one area where there are significant differences is in privacy because American companies have not followed what the Europeans would want to when it comes to protect personal data, to using personal data.

And there's a dilemma here that the Europeans, to their credit, now realize, which is you're an American, you don't have any privacy. I hope that's not a shock. The Europeans would like to change that through regulation, but they realize that the business model that the U.S. has come up with, U.S. industry has come up with, where data subsidizes Internet activities, is the only business model that works for the Internet.

And when they killed that model in Europe a decade ago through the privacy regulations, they also killed European industry. So how do you expand privacy protections without killing innovation on the Internet? And no one has a good answer for that.

I can tell you what we thought of in the Clinton administration. None of it worked. So I

won't bother. But I think that's the issue, is data transfer. Data is not the new currency, it's not the new oil, it's not--it is the new cliche, but people have realized its value. There's value if it can move quickly and unimpeded, but we don't have an agreed structure of rules to do this on a global basis. And that might be a good topic for negotiation.

CHAIRMAN BARTHOLOMEW: Do you have closing comments on that?

HEARING CO-CHAIR WORTZEL: No. I just think it was, it was a great panel. I appreciate both of you being here, and you challenged some of the principal architectures that we've been functioning under.

CHAIRMAN BARTHOLOMEW: Yeah, yeah. Certainly stretched our brain and our thinking on all of these things. I hope that you are more successful than those of us who 20 years ago started talking about what was happening to our manufacturing infrastructure, and some of the other issues that--some of the industries that China has focused subsidies on.

I mean I think, I hope, I hope you succeed in some of these things. Before we close, I want to thank our staff who did all the work to put this together, Alexander Bowe and Matt Southerland, and thank you everybody. We certainly have a lot of thinking to do.

Thank you so much.

DR. DEMCHAK: Thank you.

DR. LEWIS: Thank you.

[Whereupon, at 3:05 p.m., the hearing was adjourned.]